Kaspersky
Endpoint Security für Windows

Inhalt

Über Kaspersky Endpoint Security für Windows

Dieser Abschnitt beschreibt die Funktionen, die Komponenten und den Lieferumfang von Kaspersky Endpoint Security und nennt die Hard- und Softwarevoraussetzungen für Kaspersky Endpoint Security.

Neuerungen

Kaspersky Endpoint Security für Windows bietet folgende Neuerungen und Verbesserungen:

1. Integration von Endpoint Sensor, die eine Komponente von Kaspersky Anti Targeted Attack Platform ist:
   - IoC-Scanner (Indikatoren für die Kompromittierung)
   - Tools für die Verarbeitung von Vorfällen
   - Option für die Untersuchung von Vorfällen
2. Unterstützung von Server-Betriebssystemen im Rahmen der Komponenten Verhaltensanalyse, Rollback von schädlichen Aktionen und Exploit-Prävention
3. Funktionalität für den Schutz von gemeinsamen Ordnern vor der externen Verschlüsselung im Rahmen der Komponente Verhaltensanalyse
4. Verbesserungen der Benutzeroberfläche:

- Gruppierung der Schutzkomponenten in folgende Abschnitte:
  - Erweiterter Schutz
  - Basisschutz
- Komponentennamen, die der aktuellen Situation im Bereich der Informationssicherheit entsprechen:
  - Die Komponente Datei-Anti-Virus heißt jetzt Schutz vor bedrohlichen Dateien.
  - Die Komponente Mail-Anti-Virus heißt jetzt Schutz vor E-Mail-Bedrohungen.
  - Die Komponente Web-Anti-Virus heißt jetzt Schutz vor Web-Bedrohungen.
  - Die Komponente Schutz vor Netzwerkangriffen heißt jetzt Schutz vor Netzwerkbedrohungen.
  - Die Komponente Aktivitätsmonitor wurde in folgende Komponenten unterteilt: Verhaltensanalyse, Rollback von schädlichen Aktionen und Exploit-Prävention.
  - Die Komponente Aktivitätskontrolle für Programme heißt jetzt Programm-Überwachung.
  - Die Komponente Kontrolle des Programmstarts heißt jetzt Programmkontrolle.

5. Cloud-Modus für den Schutz vor Bedrohungen: Die eingeschränkte Version der Antiviren-Datenbanken beansprucht bei der Verwendung von Kaspersky Security Network weniger Arbeitsspeicher und Platz auf der Festplatte.

6. Gerätekontrolle:
   - Neu: Funktionalität Anti-Bridging (verbietet die Installation unerlaubter Verbindungen zwischen Netzwerken)
   - Neu: Option für den Import/Export einer Liste mit vertrauenswürdigen Geräten (im XML-Format, das sich einfach lesen und bearbeiten lässt)

7. Programmkontrolle:
   - Aktivierung eines Testmodus für bestimmte Regeln
   - Neue KL-Kategorie "Vertrauenswürdige Zertifikate", die zur KL-Kategorie "Goldene Kategorie" gehört

8. Eine vereinfachte Benutzeroberfläche von Kaspersky Endpoint Security ist verfügbar: In der Taskleiste ist ein Kontextmenü des Programmsymbols verfügbar. Dabei kann das Programmhauptfenster nicht geöffnet werden.

9. Die Prüfsumme (Hash) einer gefundenen Datei wird an den Administrationsserver von Kaspersky Security Center übertragen, in Berichten ausgewiesen und kann verwendet werden, um Ausnahmen festzulegen (Vertrauenswürdige Zone).

10. Unterstützung von Masken (*, ?, **) zum Festlegen von Ausnahmen (Vertrauenswürdige Zone)

11. Indikator des Schutzniveaus für die Richtlinie von Kaspersky Security Center. Der Indikator zeigt gegebenenfalls an, dass sehr wichtige Schutzkomponenten deaktiviert sind.

12. Weitere Verbesserungen zur Erhöhung der Nutzungsfreundlichkeit des Programms:

    - Der Schnellstartassistent des Programms wurde vereinfacht.
    - Optimierte Verwaltung für die Lizenzverwaltung

In Kaspersky Endpoint Security 11 für Windows werden die Funktionalitäten Quarantäne, IM-Anti-Virus und Schwachstellensuche nicht mehr unterstützt.

Lieferumfang

Zum Lieferumfang von Kaspersky Endpoint Security gehören folgende Dateien:

- Dateien, die zur Installation des Programms mit allen verfügbaren Methoden erforderlich sind
- Dateien der Update-Pakete, die bei der Programminstallation verwendet werden
- Datei klcfginst.msi für die Installation des Verwaltungs-Plug-ins für Kaspersky Endpoint Security über Kaspersky Security Center
- Datei ksn_<Sprach-ID>.txt mit den Bedingungen für die Teilnahme an Kaspersky Security Network
- Datei license.txt mit dem Text des Lizenzvertrags und der Datenschutzerklärung
- Datei incompatible.txt mit einer Liste der inkompatiblen Software
- Datei installer.ini mit den internen Parametern des Programmpakets

  Es wird davon abgeraten, die Werte dieser Parameter zu ändern. Falls Sie die Installationseinstellungen ändern möchten, verwenden Sie die Datei setup.ini.

Um Zugriff auf die Dateien zu erhalten, muss das Programmpaket entpackt werden.

Organisation des Computerschutzes

Kaspersky Endpoint Security bietet dem Computer einen komplexen Schutz vor unterschiedlichen Bedrohungsarten, Netzwerkangriffen und Betrugsversuchen.

Jeder Bedrohungstyp wird von einer bestimmten Programmkomponente verarbeitet. Die Komponenten können unabhängig voneinander aktiviert und deaktiviert sowie über ihre Einstellungen angepasst werden.

Zusätzlich zum konstanten Schutz, der anhand der Programmkomponenten realisiert wird, empfiehlt sich die regelmäßige Durchführung einer *Untersuchung* des Computers auf Viren und andere schädliche Programmen. Das ist erforderlich, um die Möglichkeit einer Ausbreitung schädlicher Programme

auszuschließen, die nicht von den Schutzkomponenten erkannt wurden, da beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Um Kaspersky Endpoint Security immer auf dem neuesten Stand zu halten, muss ein *Update* der Datenbanken und Programm-Module, die im Programm verwendet werden, durchgeführt werden. Standardmäßig wird das Programm automatisch aktualisiert. Bei Bedarf können Datenbanken und Programm-Module jedoch jederzeit manuell aktualisiert werden.

Die folgenden Programmkomponenten werden als Kontrollkomponenten bezeichnet:

- **Programmkontrolle**. Diese Komponente verfolgt den Start von Programmen durch den Anwender und reguliert den Programmstart.
- **Gerätekontrolle**. Diese Komponente ermöglicht es, flexible Zugriffsbeschränkungen einzurichten für Geräte, die als Informationsquellen dienen (z. B. Festplatten, Wechseldatenträger, Bandlaufwerke, CD/DVD-Disks), Datenübertragungsgeräte (z. B. Modems), Geräte, mit denen Informationen ausgedruckt werden können (z. B. Drucker), oder Schnittstellen, mit deren Hilfe Geräte mit einem Computer verbunden werden können (z. B. USB, Bluetooth, Infrarot).
- **Web-Kontrolle**. Diese Komponente ermöglicht es, für verschiedene Anwendergruppen flexible Zugriffsbeschränkungen für Webressourcen einzurichten.

Die Funktion der Kontrollkomponenten basiert auf Regeln:

- Die Programmkontrolle verwendet Kontrollregeln für Programme.
- Die Programm-Überwachung verwendet Aktivitätskontrollregeln für Programme.
- Die Gerätekontrolle verwendet Regeln für den Zugriff auf Geräte und Regeln für den Zugriff auf Schnittstellen.
- Die Web-Kontrolle verwendet Regeln für den Zugriff auf Webressourcen.

Die folgenden Programmkomponenten werden als Schutzkomponenten bezeichnet:

- **Verhaltensanalyse**. Diese Komponente erhält Daten über die Aktionen der Programme auf Ihrem Computer und versorgt die anderen Schutzkomponenten mit entsprechenden Informationen, um die Effektivität des Schutzes zu steigern.
- **Exploit-Prävention**. Diese Komponente verfolgt die ausführbaren Dateien, die von verwundbaren Programmen gestartet werden. Wenn der Startversuch einer ausführbaren Datei aus einem verwundbaren Programm nicht vom Benutzer initiiert wurde, blockiert Kaspersky Endpoint Security den Start dieser Datei.
- **Programm-Überwachung**. Diese Komponente registriert die Aktionen, die von Programmen im System ausgeführt werden, und reguliert die Aktivität von Programmen in Abhängigkeit von der Gruppe, zu der ein Programm gehört. Für jede Gruppe von Programmen ist eine Auswahl von Regeln vorgegeben. Diese Regeln regulieren den Zugriff von Programmen auf persönliche Anwenderdaten sowie auf die Ressourcen des Betriebssystems. Zu solchen Daten zählen Benutzerdateien (Verzeichnis "Eigene Dateien", Cookies, Daten zur Aktivität des Anwenders) sowie Dateien, Verzeichnisse und Registrierungsschlüssel, die Arbeitsparameter und wichtige Daten häufig verwendeter Programme beinhalten.

- **Rollback von schädlichen Aktionen**. Mithilfe dieser Komponente kann Kaspersky Endpoint Security Aktionen rückgängig machen,die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

- **Schutz vor bedrohlichen Dateien**. Diese Komponente schützt das Dateisystem des Computers vor einer Infektion. Die Komponente wird beim Start von Kaspersky Endpoint Security gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die auf Ihrem Computer und auf allen angeschlossenen Laufwerken geöffnet, gespeichert und gestartet werden. Diese Komponente fängt jeden Zugriff auf eine Datei ab und untersucht diese Datei auf Viren und andere bedrohliche Programme.

- **Schutz vor Web-Bedrohungen**. Diese Komponente untersucht den Datenverkehr, der über die Protokolle HTTP und FTP auf dem Benutzercomputer empfangen wird. Außerdem überprüft sie, ob Links zu bösartigen Webadressen oder zu Phishing-Webadressen führen.

- **Schutz vor E-Mail-Bedrohungen**. Diese Komponente untersucht, ob in ein- und ausgehenden E-Mail-Nachrichten Viren und andere Schadprogramme enthalten sind.

- **Schutz vor Netzwerkbedrohungen**. Diese Komponente prüft den eingehenden Netzverkehr auf für Netzwerkangriffe charakteristische Aktivitäten. Wenn Kaspersky Endpoint Security einen Angriff auf den Computer erkennt, blockiert das Programm die Netzwerkaktivität des angreifenden Computers.

- **Firewall**. Diese Komponente gewährleistet den Schutz der Daten, die auf dem Benutzercomputer gespeichert sind. Während eine Verbindung zum Internet oder zum lokalen Netzwerk besteht, werden die meisten Bedrohungen blockiert, die das Betriebssystem gefährden können. Die Komponente filtert die gesamte Netzaktivität gemäß den folgenden zwei Regeln: Netzwerkregeln für Programme und Netzwerkregeln für Pakete.

- **Schutz vor modifizierten USB-Geräten**. Diese Komponente verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem Computer verbunden werden.

- **Netzwerkmonitor**. Diese Komponente ermöglicht die Ansicht der Informationen zur Netzwerkaktivität des Computers im Echtzeitmodus.

In Kaspersky Endpoint Security sind die folgenden Aufgaben vorgesehen:

- **Integritätsprüfung**. Kaspersky Endpoint Security überprüft, ob die Programm-Module, die sich im Installationsordner des Programms befinden, Beschädigungen oder Änderungen aufweisen. Besitzt ein Programm-Modul eine inkorrekte digitale Signatur, so gilt das Modul als beschädigt.

- **Vollständige Untersuchung**. Kaspersky Endpoint Security führt eine Untersuchung des Betriebssystems aus und scannt dabei u. a. folgende Elemente: Systemspeicher, Objekte, die beim Hochfahren geladen werden, Sicherungsspeicher des Betriebssystems sowie sämtliche Festplatten und Wechseldatenträger.

- **Benutzerdefinierte Untersuchung**. Kaspersky Endpoint Security untersucht die vom Benutzer ausgewählten Objekte.

- **Untersuchung wichtiger Bereiche**. Kaspersky Endpoint Security prüft Objekte, die beim Start des Betriebssystems geladen werden, den Systemspeicher sowie Objekte, die mit Rootkits infiziert sind.

- **Update-Rollback**. Kaspersky Endpoint Security setzt das letzte Update der Datenbanken und Module zurück.

- **Update**. Kaspersky Endpoint Security lädt aktualisierte Datenbanken und Programm-Module. Dadurch befindet sich der Schutz des Computers vor Viren und anderen Schadprogrammen stets auf dem

neuesten Stand.

Die Dateiverschlüsselungsfunktion ermöglicht das Verschlüsseln von Dateien und Ordnern, die auf den lokalen Computerfestplatten gespeichert sind. Mit der Funktionalität zur vollständigen Festplattenverschlüsselung können Festplatten und Wechseldatenträger verschlüsselt werden.

Remote-Verwaltung über Kaspersky Security Center

Kaspersky Security Center ermöglicht das Starten und Beenden von Kaspersky Endpoint Security auf Client-Computern, die Verwaltung von Aufgaben und die Konfiguration der Programmeinstellungen im Remote-Betrieb.

Verwaltungsfunktionen des Programms

Kaspersky Endpoint Security bietet mehrere Verwaltungsfunktionen. Die Verwaltungsfunktionen dienen dazu, das Programm auf dem neuesten Stand zu halten, die Optionen des Programms zu erweitern und den Benutzer zu unterstützen.

- Berichte. Während der Ausführung des Programms wird für jede Programmkomponente und -aufgabe ein Bericht erstellt. Der Bericht enthält eine Liste mit den Ereignissen, die während der Ausführung von Kaspersky Endpoint Security aufgetreten sind, sowie mit allen vom Programm ausgeführten Operationen. Treten Probleme auf, können Sie die Berichte an Kaspersky Lab senden, um sie von den Experten des Technischen Supports eingehend untersuchen zu lassen.

- Datenverwaltung. Wenn das Programm bei der Untersuchung des Computers auf Viren und andere Schadprogramme infizierte Dateien findet, so werden diese Dateien blockiert. Kaspersky Endpoint Security speichert die Kopien desinfizierter und gelöschter Dateien im *Backup*. Dateien, die bisher nicht verarbeitet wurden, werden von Kaspersky Endpoint Security in die *Liste der aktiven Bedrohungen* verschoben. Sie können Dateien untersuchen, Dateien an ihrem ursprünglichen Speicherort wiederherstellen und die Datenverwaltung leeren.

- Benachrichtigungsdienst. Der Benachrichtigungsdienst informiert den Anwender über den aktuellen Schutz des Computers und über den Betrieb von Kaspersky Endpoint Security. Die Nachrichten können auf dem Desktop eingeblendet oder per E-Mail zugestellt werden.

- Kaspersky Security Network. Durch die Teilnahme des Anwenders an Kaspersky Security Network kann die Effizienz des Computerschutzes gesteigert werden, indem Informationen zur Sicherheit und Zuverlässigkeit von Dateien, Webressourcen und Programmen von allen Teilnehmern weltweit zur Verfügung gestellt werden.

- Lizenz. Durch den Kauf einer Lizenz erhalten Sie eine voll funktionsfähige Programmversion, Zugriff auf Updates für die Datenbanken und Programm-Module, sowie das Recht auf technischen Support bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail.

- Support. Alle registrierten Nutzer von Kaspersky Endpoint Security können sich im Falle eines Problems an unsere Experten vom Technischen Support wenden. Senden Sie eine Anfrage aus "Personal Cabinet" auf der Support-Website oder lassen Sie sich telefonisch von unseren Mitarbeitern beraten.

Wenn im Programm Fehler auftreten oder das Programm "hängen bleibt", kann sich das Programm automatisch neu starten.

Treten bei der Ausführung des Programms wiederholt Fehler auf, aufgrund derer das Programm beendet wird, führt das Programm die folgenden Aktionen aus:

1. Deaktivierung der Schutz- und Überwachungsfunktionen (die Verschlüsselungsfunktion bleibt aktiv).

2. Benachrichtigung des Benutzers über die Deaktivierung der Funktionen.

3. Versuch der Wiederherstellung der Funktionsfähigkeit nach Updates der Antiviren-Datenbanken und der Übernahme von Updates der Programm-Module.

Um Informationen über wiederholte Fehler und Abstürze zu erhalten, nutzt das Programm spezielle Algorithmen, die von den Kaspersky-Lab-Experten erstellt werden.

Hard- und Software-Voraussetzungen

Um die Funktionsfähigkeit von Kaspersky Endpoint Security zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen.

Allgemeine Mindestanforderungen:

- 2 GB freier Speicherplatz auf der Festplatte
- Microsoft Internet Explorer 7.0
- Internetverbindung für die Programmaktivierung und das Update der Datenbanken und Programm-Module
- Intel Pentium 1 GHz (oder kompatibel)
- Arbeitsspeicher:
  - Für das 32-Bit-Betriebssystem - 1 GB
  - Für das 64-Bit-Betriebssystem - 2 GB

Unterstützte Betriebssysteme für Workstations:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1
- Microsoft Windows 8 Professional / Enterprise x86 Edition, Microsoft Windows 8 Professional / Enterprise x64 Edition, Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition

Besonderheiten im Hinblick auf die Unterstützung des Betriebssystems Microsoft Windows 10 finden Sie im Artikel 13036 der Wissensdatenbank des Technischen Supports: http://support.kaspersky.com/de/kes11 .

Unterstützte Betriebssysteme für Dateiserver:

- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1, Microsoft Windows Server 2008 Standard / Enterprise x86 Edition SP2, Microsoft Windows Server 2008 Standard / Enterprise x64 Edition SP2
- Microsoft Windows Small Business Server 2011 Essentials / Standard x64 Edition
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition, Microsoft Windows MultiPoint Server 2012 x64 Edition
- Microsoft Windows Server 2016

Besonderheiten im Hinblick auf die Unterstützung des Betriebssystems Microsoft Windows Server 2016 finden Sie im Artikel 13036 der Wissensdatenbank des Technischen Supports: http://support.kaspersky.com/de/kes11 .

Programm installieren und deinstallieren

Dieser Abschnitt bietet Informationen zu folgenden Vorgängen: Installation von Kaspersky Endpoint Security auf einem Computer, Erstkonfiguration des Programms, Upgrade einer Vorgängerversion, Deinstallation des Programms.

Programm installieren

Dieser Abschnitt enthält Informationen zur Installation und Erstkonfiguration von Kaspersky Endpoint Security.

Methoden der Programminstallation

Kaspersky Endpoint Security für Windows kann entweder lokal (direkt auf dem Benutzercomputer) oder ferngesteuert vom Administrator-Arbeitsplatz aus installiert werden.

Die lokale Installation von Kaspersky Endpoint Security für Windows ist in einem der folgenden Modus möglich:

- Im interaktiven Modus mithilfe des Installationsassistenten des Programms

  Der interaktive Modus erfordert Ihre Beteiligung am Installationsvorgang.

- Im unbeaufsichtigten Modus aus der Befehlszeile

  Nach dem Start der Installation im unbeaufsichtigten Modus ist Ihre Beteiligung am Installationsvorgang nicht mehr erforderlich.

Für die Remote-Installation des Programms auf Netzwerkcomputern können verwendet werden:

- Programmpaket für Kaspersky Security Center (s. *Implementierungshandbuch zu Kaspersky Security Center*)

- Gruppenrichtlinienverwaltungs-Editor von Microsoft Windows (s. Dokumentation für das Betriebssystem)
- System Center Configuration Manager

Es wird empfohlen, vor Beginn der Installation von Kaspersky Endpoint Security (auch vor einer Remote-Installation) alle laufenden Programme zu schließen.

Programm mithilfe des Installationsassistenten installieren

Die Benutzeroberfläche des Installationsassistenten für das Programm besteht aus einer Abfolge von Fenstern, die den einzelnen Installationsschritten entsprechen. Verwenden Sie die Schaltflächen **Zurück** und **Weiter**, um zwischen den Fenstern des Installationsassistenten zu navigieren. Schließen Sie den Installationsassistenten mit der Schaltfläche **Beenden** ab. Der Installationsassistent kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie wie folgt vor, um mithilfe des Installationsassistenten das Programm zu installieren oder eine Vorgängerversion zu aktualisieren:

1. Starten Sie die Datei setup_kes.exe, die im Lieferumfang enthalten ist.

   Der Installationsassistent wird gestartet.

2. Folgen Sie den Anweisungen des Installationsassistenten.

Nach dem Start der Datei setup.exe überprüft Kaspersky Endpoint Security, ob auf dem Computer inkompatible Software vorhanden ist. Wird inkompatible Software gefunden, so wird die Installation standardmäßig abgebrochen und auf dem Bildschirm erscheint eine Liste der gefundenen Programme, die nicht mit Kaspersky Endpoint Security kompatibel sind. Um die Installation fortzusetzen, müssen diese Programme vom Computer gelöscht werden.

Schritt 1. Systemkompatibilität für die Installation überprüfen

Bevor Kaspersky Endpoint Security für Windows auf einem Computer installiert oder eine Vorgängerversion des Programms aktualisiert wird, werden folgende Voraussetzungen überprüft:

- Übereinstimmung des Betriebssystems und des Service Packs mit den Softwarevoraussetzungen für die Installation
- Erfüllung der Hard- und Softwarevoraussetzungen
- Vorhandensein von Rechten für die Programminstallation

Wenn eine der aufgezählten Voraussetzungen nicht erfüllt ist, erscheint eine entsprechende Meldung auf dem Bildschirm.

Erfüllt der Computer die erforderlichen Voraussetzungen, so führt der Installationsassistent eine Suche nach Kaspersky-Lab-Programmen durch, deren gleichzeitige Verwendung zu Konflikten führen kann. Werden solche Programme gefunden, so werden Sie aufgefordert, diese manuell zu entfernen.

Befindet sich eine ältere Version von Kaspersky Endpoint Security unter den gefundenen Programmen, so werden alle Daten, die migriert werden können (z. B. Aktivierungsinformationen und Programmeinstellungen) gespeichert und bei der Installation von Kaspersky Endpoint Security 11 für Windows verwendet. Die ältere Programmversion wird automatisch entfernt. Dies bezieht sich auf folgende Programmversionen:

- Kaspersky Endpoint Security 10 Service Pack 1 für Windows (Version 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 für Windows (Version 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 für Windows (Version 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 für Windows (Version 10.2.5.3201)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 für Windows (Version 10.2.6.3733)
- Kaspersky Endpoint Security 10 Service Pack 2 für Windows (Version 10.3.0.6294)

Schritt 2. Startfenster des Installationsvorgangs

Wenn die Voraussetzungen für die Programminstallation vollständig erfüllt sind, öffnet sich nach dem Start des Installationspakets ein Startfenster. Das Startfenster enthält Informationen über den Beginn der Installation von Kaspersky Endpoint Security auf dem Computer.

Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**.

Schritt 3. Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie anzeigen

Bei diesem Schritt des Installationsassistenten ist es erforderlich, den Endbenutzer-Lizenzvertrag, der zwischen Ihnen und Kaspersky Lab abgeschlossen wird, genau zur Kenntnis zu nehmen.

Lesen Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie sorgfältig. Wenn Sie mit allen Punkten des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie im Block **Ich bestätige, dass ich die folgenden Dokumente vollständig gelesen und verstanden habe und akzeptiere** die Kontrollkästchen:

- **Bedingungen des vorliegenden Endbenutzer-Lizenzvertrags**
- **Datenschutzrichtlinie, welche die Verarbeitung von Daten beschreibt**

Die Programminstallation auf Ihrem Gerät wird fortgesetzt, nachdem diese beiden Kontrollkästchen aktiviert wurden.

Wenn Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie ablehnen, klicken Sie auf das Kontrollkästchen **Abbrechen**.

Schritt 4. Installationstyp wählen

Bei diesem Schritt können Sie den passenden Installationstyp für Kaspersky Endpoint Security wählen:

- **Basisinstallation**: Wenn Sie diesen Installationstyp auswählen, werden unter Ausnahme der Komponente Schutz vor modifizierten USB-Geräten alle Schutzkomponenten auf dem Computer installiert. Dabei werden die von Kaspersky Lab empfohlenen Einstellungen verwendet.

- **Standardinstallation**: Wenn Sie diesen Installationstyp auswählen, werden unter Ausnahme der Komponente Schutz vor modifizierten USB-Geräten alle Schutzkomponenten und Kontrollkomponenten auf dem Computer installiert. Dabei werden die von Kaspersky Lab empfohlenen Einstellungen verwendet.

- **Benutzerdefinierte Installation**: Bei Auswahl dieses Installationstyps können Sie die Installationskomponenten auswählen und den Ordner angeben, in dem das Programm installiert werden soll.

  Mit diesem Installationstyp können Sie Komponenten installieren, die nicht zur Basis- und Standardinstallation gehören.

In der Grundeinstellung ist die Standardinstallation ausgewählt.

Klicken Sie auf **Zurück**, um zum vorherigen Schritt des Installationsassistenten zurückzukehren. Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**. Klicken Sie auf **Abbrechen**, um den Installationsassistenten abzubrechen.

Schritt 5. Programmkomponenten für Installation auswählen

Dieser Schritt wird ausgeführt, wenn Sie die *Benutzerdefinierte Installation* des Programms ausgewählt haben.

Bei diesem Schritt können Sie wählen, welche Komponenten von Kaspersky Endpoint Security installiert werden sollen. Die Komponente Schutz vor bedrohlichen Dateien ist für die Installation obligatorisch. Sie können die Installation dieser Komponente nicht abwählen.

Standardmäßig sind alle Programmkomponenten für die Installation gewählt. Eine Ausnahme bilden folgende Komponenten:

- Schutz vor modifizierten USB-Geräten.

- Dateien verschlüsseln

- Vollständige Festplattenverschlüsselung.

- Verwaltung von BitLocker.

- Endpoint Sensor.

Die *Verwaltung von BitLocker* besitzt folgende Funktionen:

- Verwaltung der BitLocker-Verschlüsselung, die in das Windows-Betriebssystem integriert ist

- Anpassen der Verschlüsselung in den Einstellungen der Richtlinie für Kaspersky Security Center und Überprüfung, ob die Einstellungen auf den verwalteten Computer anwendbar sind
- Start von Verschlüsselungs- und Entschlüsselungsvorgängen
- Überwachung des Verschlüsselungsstatus auf dem verwalteten Computer
- Zentralisierte Speicherung von Wiederherstellungsschlüsseln auf dem Administrationsserver für Kaspersky Security Center

Endpoint Sensor ist eine Komponente von Kaspersky Anti Targeted Attack Platform. Diese Lösung dient der rechtzeitigen Erkennung von Bedrohungen wie beispielsweise gezielten Angriffen. Die Komponente überwacht kontinuierlich Prozesse, offene Netzwerkverbindungen und Dateiänderungen, und leitet diese Informationen an Kaspersky Anti Targeted Attack Platform weiter.

Um eine Komponente für die Installation zu wählen, öffnen Sie mit der linken Maustaste das Kontextmenü des Symbols neben dem Komponentennamen und wählen Sie den Punkt **Die Komponente wird auf der lokalen Festplatte installiert**. Nähere Informationen dazu, welche Aufgaben die gewählte Komponente erfüllt und wie viel Speicherplatz ihre Installation erfordert, sehen Sie im unteren Bereich des Fensters des Installationsassistenten.

Klicken Sie auf **Laufwerk**, um Details über den freien Speicherplatz auf den Festplatten Ihres Computers anzuzeigen. Im folgenden Fenster **Verfügbarer Platz auf den Laufwerken** werden entsprechende Informationen angezeigt.

Wenn eine Komponente nicht installiert werden soll, wählen Sie im Kontextmenü den Punkt **Die Komponente wird nicht verfügbar sein**.

Klicken Sie auf **Zurücksetzen**, um zur Liste der standardmäßig zu installierenden Komponenten zurückzukehren.

Klicken Sie auf **Zurück**, um zum vorherigen Schritt des Installationsassistenten zurückzukehren. Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**. Klicken Sie auf **Abbrechen**, um den Installationsassistenten abzubrechen.

Schritt 6. Installationsordner für das Programm auswählen

Dieser Schritt ist verfügbar, wenn Sie die *Benutzerdefinierte Installation* des Programms gewählt haben.

Bei diesem Schritt können Sie den Pfad des Zielordners angeben, in dem das Programm installiert werden soll. Klicken Sie auf **Durchsuchen**, um den Installationsordner für das Programm auszuwählen.

Klicken Sie auf **Laufwerk**, um Informationen zum freien Speicherplatz auf den Festplatten Ihres Computers anzuzeigen. Die Informationen werden im erscheinenden Fenster **Verfügbarer Platz auf den Laufwerken** angezeigt.

Klicken Sie auf **Zurück**, um zum vorherigen Schritt des Installationsassistenten zurückzukehren. Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**. Klicken Sie auf **Abbrechen**, um den Installationsassistenten abzubrechen.

Schritt 7. Untersuchungsausnahmen hinzufügen

Dieser Schritt ist verfügbar, wenn Sie die *Benutzerdefinierte Installation* des Programms gewählt haben.

Bei diesem Schritt können Sie festlegen, welche Untersuchungsausnahmen zu den Programmeinstellungen hinzugefügt werden sollen.

Das Kontrollkästchen **Die von Microsoft empfohlenen Bereiche von der Untersuchung ausschließen** / **Die von Kaspersky Lab empfohlenen Bereiche von der Untersuchung ausschließen** nimmt Bereiche, die von Microsoft bzw. Kaspersky Lab empfohlen werden, in die vertrauenswürdige Zone auf oder schließt sie aus dieser Zone aus.

Ist das Kontrollkästchen aktiviert, schließt Kaspersky Endpoint Security die von Microsoft / Kaspersky Lab empfohlenen Bereiche in die vertrauenswürdige Zone ein. Diese Bereiche werden von Kaspersky Endpoint Security nicht auf Viren und andere Schadprogramme untersucht.

Das Kontrollkästchen **Die von Microsoft empfohlenen Bereiche von der Untersuchung ausschließen** ist nur dann verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Microsoft Windows für Dateiserver installiert ist.

Klicken Sie auf **Zurück**, um zum vorherigen Schritt des Installationsassistenten zurückzukehren. Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**. Klicken Sie auf **Abbrechen**, um den Installationsassistenten abzubrechen.

Schritt 8. Programminstallation vorbereiten

Es wird empfohlen, den Installationsprozess zu schützen, da sich auf dem Computer schädliche Programme befinden können, welche die Installation von Kaspersky Endpoint Security für Windows stören kann.

Der Schutz für den Installationsvorgang ist standardmäßig aktiviert.

Es wird empfohlen, den Schutz für den Installationsvorgang zu deaktivieren, falls die Programminstallation andernfalls nicht möglich ist (Dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein). Brechen Sie in einem solchen Fall die Installation ab und starten Sie den Installationsassistenten für das Programm erneut. Deaktivieren Sie beim Schritt "Programminstallation vorbereiten" das Kontrollkästchen **Installationsprozess schützen**.

Das Kontrollkästchen **Kompatibilität mit Citrix PVS gewährleisten** aktiviert/deaktiviert eine Funktion, welche die Installation von Treibern im Citrix-PVS-Kompatibilitätsmodus ausführt.

Aktivieren Sie dieses Kontrollkästchen nur, wenn Sie Citrix Provisioning Services verwenden.

Das Kontrollkästchen **Pfad der Datei avp.com zur Systemvariablen %PATH% hinzufügen** aktiviert / deaktiviert das Hinzufügen des Pfades zur Datei avp.com zur Systemvariablen %PATH%.

Wenn dieses Kontrollkästchen aktiviert ist, muss der Pfad zur ausführbaren Datei nicht angegeben werden, um Kaspersky Endpoint Security oder beliebige Aufgaben des Programms aus der Befehlszeile zu starten. Es ist ausreichend, den Namen der ausführbaren Datei und den Startbefehl für die entsprechende Aufgabe einzugeben.

Klicken Sie auf **Zurück**, um zum vorherigen Schritt des Installationsassistenten zurückzukehren. Klicken Sie auf **Installieren**, um dieInstallation zu starten. Klicken Sie auf **Abbrechen**, um den Installationsassistenten abzubrechen.

Während das Programm auf einen Computer installiert wird, kann es vorkommen, dass bestehende Netzwerkverbindungen getrennt werden. Die meisten getrennten Netzwerkverbindungen wird nach dem Abschluss der Programminstallation wiederhergestellt.

Schritt 9. Programminstallation

Die Installation des Programms nimmt einige Zeit in Anspruch. Warten Sie die Fertigstellung ab.

Wenn Sie ältere Programmversionen aktualisieren, werden bei diesem Schritt auch die Einstellungen übertragen und die Vorgängerversion wird entfernt.

Nach Abschluss der Installation von Kaspersky Endpoint Security wird der Schnellstartassistent für das Programm gestartet.

Programm über die Befehlszeile installieren

Die Programminstallation kann aus der Befehlszeile entweder im interaktiven oder im unbeaufsichtigten Modus ausführen.

Außerdem können Sie bei der Programminstallation aus der Befehlszeile den Benutzernamen und das Kennwort für den Zugriff auf das Programm anpassen. Das Programm fragt den Benutzernamen und das Kennwort ab, wenn der Benutzer versucht, das Programm zu löschen, zu beenden oder die Programmeinstellungen zu ändern.

Um den Installationsassistenten per Befehlszeile zu starten,

geben Sie in der Befehlszeile `setup.exe` oder `msiexec /i <Name des Programmpakets>` ein.

Um im unbeaufsichtigten Modus (ohne den Installationsassistenten zu starten) das Programm zu installieren oder ein Programm-Upgrade auszuführen,

geben Sie in der Befehlszeile ein: `setup.exe /pEULA=1 / PRIVACYPOLICY=1 /pKSN=1|0 /pINSTALLLEVEL=<Wert> /pALLOWREBOOT=1|0 /pSKIPPRODUCTCHECK=1|0 /pSKIPPRODUCTUNINSTALL=1|0 /s`

oder

```
msiexec /i <Name des Programmpakets> EULA=1 PRIVACYPOLICY=1 KSN=1|0 INSTALLLEVEL=
<Wert> ALLOWREBOOT=1|0 ADDLOCAL=<Wert> SKIPPRODUCTCHECK=1|0 SKIPPRODUCTUNINSTALL=1|0
```

`/qn`,

wobei:

- `EULA=1` bedeutet, dass Sie die Bedingungen des Lizenzvertrags annehmen. Der Text des Lizenzvertrags ist im Lieferumfang von Kaspersky Endpoint Security enthalten. Die Bedingungen des Lizenzvertrags müssen akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann. Ist bei der Installation im unbeaufsichtigten Modus kein Wert für diesen Parameter angegeben, so wird das Programm nicht installiert.

- `PRIVACYPOLICY=1` bedeutet, dass Sie die Bedingungen der Datenschutzerklärung annehmen. Der Text der Datenschutzerklärung ist im Lieferumfang von Kaspersky Endpoint Security enthalten. Die Bedingungen der Datenschutzerklärung müssen akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann. Ist bei der Installation im unbeaufsichtigten Modus kein Wert für diesen Parameter angegeben, so wird das Programm nicht installiert.

- `KSN=1|0` bedeutet, dass die Teilnahme am Programm Kaspersky Security Network (im Folgenden auch "KSN" genannt) akzeptiert (1) oder abgelehnt (0) wird. Der Text der Erklärung zu Kaspersky Security Network ist im Lieferumfang von Kaspersky Endpoint Security enthalten. Die Angabe dieses Parameterwerts ist optional. Ist im Befehl kein Wert für den Parameter `KSN` angegeben, so wird beim ersten Start von Kaspersky Endpoint Security ein Abfragefenster zur Teilnahme am Programm KSN geöffnet.

  Das Programmpaket für Kaspersky Endpoint Security ist für die Nutzung von Kaspersky Security Network optimiert. Falls Sie die Teilnahme an Kaspersky Security Network abgelehnt haben, aktualisieren Sie Kaspersky Endpoint Security sofort nach dem Abschluss der Installation.

- `INSTALLLEVEL=<Wert>` gibt den Installationstyp für Kaspersky Endpoint Security an. Die Angabe dieses Parameterwerts ist optional. Wenn im Befehl kein Wert für `INSTALLLEVEL` angegeben ist, wird in der Grundeinstellung die Standardinstallation des Programms ausgeführt.

  Als `<Wert>` können folgende Werte für `INSTALLLEVEL` stehen:

  - `100`. Die Basis-Programminstallation wird ausgeführt.
  - `200`. Die Standard-Programminstallation wird ausgeführt.
  - `300`. Alle Programmkomponenten werden installiert.

- `ALLOWREBOOT=1|0` bedeutet die Erlaubnis (1) oder das Verbot (0) für einen automatischen Neustart des Computers, falls dieser nach der Installation oder dem Programm-Upgrade erforderlich ist. Die Angabe dieses Parameterwerts ist optional. Ist im Befehl kein Wert für den Parameter `ALLOWREBOOT` angegeben, so ist ein automatischer Neustart des Computers nach der Installation oder dem Programm-Upgrade standardmäßig verboten.

  Ein Neustart des Computers kann erforderlich sein, wenn ein Programm-Upgrade ausgeführt wurde oder während der Installation von Kaspersky Endpoint Security Antiviren-Software von Drittherstellern gefunden und entfernt wurde.

Ein automatischer Neustart des Computers kann nur im Silent-Installationsmodus (mit dem Parameter /qn) ausgeführt werden.

- `ADDLOCAL=<Wert>` gibt an, welche Komponenten zusätzlich zu den Komponenten installiert werden sollen, die im standardmäßigen Installationsmodus gewählt sind. Die Angabe dieses Parameterwerts ist optional.

  Für `<Wert>` sind folgende Werte für den Parameter `INSTALLLEVEL` möglich:

  - `MSBitLockerFeature`. Die Komponente Microsoft BitLocker Manager wird installiert.
  - `AntiAPTFeature`. Die Komponente Endpoint Sensor wird installiert.

- `SKIPPRODUCTCHECK=1|0` bedeutet, dass die Untersuchung auf das Vorhandensein inkompatibler Software aktiviert (1) oder deaktiviert (0) ist. Die Angabe dieses Parameterwerts ist optional. Falls der Parameterwert `SKIPPRODUCTCHECK` im Befehl nicht angegeben wird, führt Kaspersky Endpoint Security eine Untersuchung durch.

- `SKIPPRODUCTUNINSTALL=1|0` bedeutet, dass das automatische Löschen von gefundenen Programmen, die mit Kaspersky Endpoint Security inkompatibel sind, erlaubt (1) oder verboten (0) ist. Die Angabe dieses Parameterwerts ist optional. Wenn im Befehl kein Wert für `SKIPPRODUCTUNINSTALL` angegeben ist, versucht Kaspersky Endpoint Security standardmäßig, alle gefundenen inkompatiblen Programme zu löschen.

Um das Programm zu installieren oder ein Programm-Upgrade auszuführen und dabei einen Benutzernamen und ein Kennwort festzulegen, welche zu Einstellungsänderungen und Aktionen mit dem Programm berechtigen, gehen Sie wie folgt vor:

- Um im interaktiven Modus das Programm zu installieren oder ein Programm-Upgrade auszuführen, geben Sie folgenden Befehl in der Befehlszeile ein:

  ```
  setup.exe /pKLLOGIN=<Benutzername> /pKLPASSWD=***** /pKLPASSWDAREA=
  <Gültigkeitsbereich des Kennworts>
  ```

  oder

  ```
  msiexec /i <Name des Programmpakets> KLLOGIN=<Benutzername> KLPASSWD=*****
  KLPASSWDAREA=<Gültigkeitsbereich des Kennworts>.
  ```

- Um im unbeaufsichtigten Modus das Programm zu installieren oder ein Programm-Upgrade auszuführen, geben Sie folgenden Befehl in der Befehlszeile ein:

  ```
  setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1|0 /pINSTALLLEVEL=<Wert> /pKLLOGIN=
  <Benutzername> /pKLPASSWD=***** /pKLPASSWDAREA=<Gültigkeitsbereich des Kennworts> /s
  ```

  oder

  ```
  msiexec /i <Name des Programmpakets> EULA=1 PRIVACYPOLICY=1 KSN=1|0 INSTALLLEVEL=
  <Wert> KLLOGIN=<Benutzername> KLPASSWD=***** KLPASSWDAREA=<Gültigkeitsbereich des
  Kennworts> ALLOWREBOOT=1|0/qn.
  ```

  Für `<Geltungsbereich des Kennworts>` können Sie als Wert für den Parameter `KLPASSWDAREA` einen oder mehrere der folgenden Werte angeben (durch Semikolon getrennt). Die einzelnen Werte entsprechen den Vorgängen, für die eine Bestätigung erforderlich ist:

  - `SET`. Programmeinstellungen ändern

- `EXIT`. Programm beenden
- `DISPROTECT`. Schutzkomponenten deaktivieren und Untersuchungsaufgaben abbrechen
- `DISPOLICY`. Richtlinie für Kaspersky Security Center deaktivieren
- `DISCTRL`. Kontrollkomponenten deaktivieren
- `REMOVELIC`. Schlüssel löschen
- `UNINST`. Programm entfernen, ändern oder reparieren
- `REPORTS`. Berichte anzeigen

Bei der Installation oder beim Upgrade des Programms im unbeaufsichtigten Modus wird die Verwendung folgender Dateien unterstützt:

- setup.ini mit den allgemeinen Installationsparametern für das Programm
- Konfigurationsdatei install.cfg mit den Funktionseinstellungen für Kaspersky Endpoint Security
- setup.reg, die Registrierungsschlüssel enthält

> Die Dateien setup.ini, install.cfg und setup.reg müssen sich im selben Ordner befinden wie das Programmpaket für Kaspersky Endpoint Security für Windows.

Remote-Installation des Programms mithilfe von System Center Configuration Manager

> Die Anleitung ist gültig für die Version System Center Configuration Manager 2012 R2.

Um das Programm ferngesteuert mithilfe von System Center Configuration Manager zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Konsole von Configuration Manager.
2. Wählen Sie im rechten Konsolenbereich im Abschnitt **Anwendungsverwaltung** den Abschnitt **Pakete**.
3. Klicken Sie im oberen Konsolenbereich in der Symbolleiste auf **Paket erstellen**.
   Der *Assistent zum Erstellen von Paketen und Programmen* wird gestartet.
4. Gehen Sie im Assistenten zum Erstellen von Paketen und Programmen wie folgt vor:
   a. Gehen Sie im Abschnitt **Paket** wie folgt vor:
      - Geben Sie im Feld **Name** den Namen des Installationspakets ein.

- Geben Sie im Feld **Quellordner** den Pfad des Ordners an, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.

b. Wählen Sie im Abschnitt **Programmtyp** die Variante **Standardprogramm**.

c. Gehen Sie im Abschnitt **Standardprogramm** wie folgt vor:

- Geben Sie im Feld **Name** den individuellen Namen des Installationspakets ein (z. B. den Programmnamen mit Versionsangabe).
- Geben Sie im Feld **Befehlszeile** die Befehlszeilenparameter für die Installation von Kaspersky Endpoint Security an.
- Geben Sie mithilfe der Schaltfläche **Durchsuchen** den Pfad der ausführbaren Programmdatei an.
- Vergewissern Sie sich, dass in der Dropdown-Liste **Ausführungsmodus** das Element **Mit Administratorrechten starten** gewählt ist.

d. Gehen Sie im Abschnitt **Anforderungen** wie folgt vor:

- Aktivieren Sie das Kontrollkästchen **Anderes Programm zuerst starten**, damit vor der Installation von Kaspersky Endpoint Security ein anderes Programm gestartet wird.

  Wählen Sie das Programm aus der Dropdown-Liste **Programm** oder geben Sie den Pfad der ausführbaren Datei dieses Programms mithilfe der Schaltfläche **Durchsuchen** an.

- Wählen Sie im Abschnitt **Anforderungen an die Plattform** die Variante **Dieses Programm kann nur auf den angegebenen Plattformen gestartet werden**, damit das Programm auf den angegebenen Betriebssystemen installiert wird.

  Aktivieren Sie in der unten angebrachten Liste die Kontrollkästchen für jene Betriebssysteme, in denen Kaspersky Endpoint Security installiert werden soll.

Dieser Schritt ist optional.

e. Überprüfen Sie im Abschnitt **Zusammenfassung** alle angegebenen Werte und klicken Sie auf **Weiter**.

Das erstellte Installationspaket erscheint im Abschnitt **Pakete** in der Liste für verfügbare Installationspakete.

5. Wählen Sie im Kontextmenü des Installationspakets den Punkt **Verteilen**.

   Der *Assistent zur Software-Verteilung* wird gestartet.

6. Gehen Sie im Assistenten zur Software-Verteilung wie folgt vor:

   a. Gehen Sie im Abschnitt **Allgemein** wie folgt vor:

   - Geben Sie im Feld **Software** den individuellen Namen des Installationspakets an oder wählen Sie mit der Schaltfläche **Durchsuchen** ein Installationspaket aus der Liste.
   - Geben Sie im Feld **Sammlung** den Namen der Gruppe für Computer an, auf denen das Programm installiert werden soll, oder wählen Sie diese Sammlung mithilfe der Schaltfläche **Durchsuchen**.

b. Fügen Sie im Abschnitt **Inhalt** die Verteilungspunkte (Weitere Informationen finden Sie in der Dokumentation zu System Center Configuration Manager).

c. Legen Sie erforderlichenfalls im Assistenten zur Software-Verteilung die Werte für weitere Einstellungen fest. Diese Einstellungen sind für die Remote-Installation von Kaspersky Endpoint Security optional.

d. Überprüfen Sie im Abschnitt **Zusammenfassung** alle angegebenen Werte und klicken Sie auf **Weiter**.

Nach Abschluss des Assistenten zur Software-Verteilung wird eine Aufgabe zur Remote-Installation von Kaspersky Endpoint Security erstellt.

Beschreibung der Installationseinstellungen in der Datei setup.ini

Die Datei setup.ini wird verwendet, wenn das Programm aus der Befehlszeile oder mithilfe des Gruppenrichtlinienverwaltungs-Editors für Microsoft Windows Server installiert wird. Die Datei setup.ini befindet sich im Ordner des Programmpakets für Kaspersky Endpoint Security.

Die Datei setup.ini enthält folgende Parameter:

1. [Setup] - allgemeine Installationsparameter für das Programm:

   - `InstallDir` - Pfad des Installationsordners für das Programm
   - `ActivationCode` - Aktivierungscode für Kaspersky Endpoint Security
   - `Eula` - Akzeptieren oder Ablehnen der Bedingungen des Lizenzvertrags. Mögliche Werte des Parameters `Eula`:
     - `1`. Die Bedingungen des Lizenzvertrags werden akzeptiert.
     - `0`. Die Bedingungen des Lizenzvertrags werden abgelehnt.
   - `PrivacyPolicy` - Zustimmung zu oder Ablehnung der Datenschutzerklärung. Mögliche Werte des Parameters `PrivacyPolicy`:
     - `1`. Zustimmung zu der Datenschutzerklärung.
     - `0`. Ablehnung der Datenschutzerklärung.

     Der Text der Datenschutzerklärung ist im Lieferumfang von Kaspersky Endpoint Security enthalten. Die Bedingungen der Datenschutzerklärung müssen akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann.

   - `KSN` - Akzeptieren oder Ablehnen der Teilnahme an Kaspersky Security Network. Mögliche Werte des Parameters `KSN`:
     - `1`. Die Teilnahme an Kaspersky Security Network wird akzeptiert.

- `0`. Die Teilnahme an Kaspersky Security Network wird abgelehnt.

> Der Lieferumfang von Kaspersky Endpoint Security ist für die Nutzung von Kaspersky Security Network optimiert. Falls Sie die Teilnahme an Kaspersky Security Network abgelehnt haben, aktualisieren Sie Kaspersky Endpoint Security sofort nach dem Abschluss der Installation.

- `Login` - Festlegen des Benutzernamens für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Der Benutzername wird zusammen mit den Parametern `Password` und `Password Area` festgelegt).

- `Password` - Festlegen des Kennworts für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Das Kennwort wird zusammen mit den Parametern `Login` und `Password Area` festgelegt).

> Falls Sie ein Kennwort angegeben haben, aber mithilfe des Parameters `Login` keinen Benutzernamen festgelegt haben, wird standardmäßig der Benutzername KLAdmin verwendet.

- `PasswordArea` - Definition des Gültigkeitsbereichs des Kennworts für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security. Mögliche Werte des Parameters `PasswordArea`. Die Parameter entsprechen den Vorgängen, für die eine Bestätigung erforderlich ist:

  - `SET`. Programmeinstellungen ändern
  - `EXIT`. Programm beenden
  - `DISPROTECT`. Schutzkomponenten deaktivieren und Untersuchungsaufgaben abbrechen
  - `DISPOLICY`. Richtlinie für Kaspersky Security Center deaktivieren
  - `UNINST`. Programm vom Computer entfernen
  - `DISCTRL`. Kontrollkomponenten deaktivieren
  - `REMOVELIC`. Kennwort für das Entfernen des Schlüssels festlegen
  - `REPORTS`. Kennwort für das Anzeigen von Berichten festlegen

- `SelfProtection` - Schutzmechanismus für die Programminstallation aktivieren oder deaktivieren. Mögliche Werte des Parameters `SelfProtection`:

  - `1`. Der Schutzmechanismus für die Programminstallation ist aktiviert.
  - `0`. Der Schutzmechanismus für die Programminstallation ist deaktiviert.

- `Reboot` - Notwendigkeit eines Neustarts des Computers nach dem Abschluss der Programminstallation. Mögliche Werte des Parameters `Reboot`:

- `1`. Nach dem Abschluss der Programminstallation wird ein Neustart des Computers ausgeführt.
- `0`. Nach dem Abschluss der Programminstallation wird kein Neustart des Computers ausgeführt.

- `MSExclusions` - Programme, die von Microsoft empfohlen werden, zu den Untersuchungsausnahmen hinzufügen.

  Dieser Parameter ist nur für Dateiserver mit dem Betriebssystem Microsoft Windows Server verfügbar.

  Mögliche Werte des Parameters `MSExclusions`:

  - `1`. Die von Microsoft empfohlenen Programme werden zu den Untersuchungsausnahmen hinzugefügt.
  - `0`. Die von Microsoft empfohlenen Programme werden nicht zu den Untersuchungsausnahmen hinzugefügt.

- `KLExclusions` - Programme, die von Kaspersky Lab empfohlen werden, zu den Untersuchungsausnahmen hinzufügen. Mögliche Werte des Parameters `KLExclusions`:

  - `1`. Die von Kaspersky Lab empfohlenen Programme werden zu den Untersuchungsausnahmen hinzugefügt.
  - `0`. Die von Kaspersky Lab empfohlenen Programme werden nicht zu den Untersuchungsausnahmen hinzugefügt.

- `AddEnvironment` - Pfad der ausführbaren Dateien, die sich im Installationsordner von Kaspersky Endpoint Security befinden, zur Systemvariablen %PATH% hinzufügen. Mögliche Werte des Parameters `AddEnvironment`:

  - `1`. Der Pfad der ausführbaren Dateien, die sich im Installationsordner von Kaspersky Endpoint Security befinden, wird zur Systemvariablen %PATH% hinzugefügt.
  - `0`. Der Pfad der ausführbaren Dateien, die sich im Installationsordner von Kaspersky Endpoint Security befinden, wird nicht zur Systemvariablen %PATH% hinzugefügt.

2. [Components] - Auswahl der zu installierenden Programmkomponenten:

   - `ALL` - Installation aller Komponenten

     Wenn der Parameterwert 1 angegeben ist, werden alle Komponenten installiert. In diesem Fall bleiben die Parameter, die für die Installation der einzelnen Komponenten angegeben sind, unberücksichtigt.

   - `MailThreatProtection` - Installation der Komponente Schutz vor E-Mail-Bedrohungen

- `WebThreatProtection` - Installation der Komponente Schutz vor Web-Bedrohungen
- `HostIntrusionPrevention` - Installation der Komponente Programm-Überwachung
- `BehaviorDetection` - Installation der Komponente Verhaltensanalyse
- `ExploitPrevention` - Installation der Komponente Exploit-Prävention
- `RemediationEngine` - Installation der Komponente Rollback von schädlichen Aktionen
- `Firewall` - Installation der Komponente Firewall
- `NetworkThreatProtection` - Installation der Komponente Schutz vor Netzwerkbedrohungen
- `WebControl` - Installation der Komponente Web-Kontrolle
- `DeviceControl` - Installation der Komponente Gerätekontrolle
- `ApplicationControl` - Installation der Komponente Programmkontrolle
- `FileEncryption` - Installation von Bibliotheken für die Verschlüsselung von Dateien
- `DiskEncryption` - Installation von Bibliotheken für die vollständige Festplattenverschlüsselung
- `BadUSBAttackPrevention` - Installation der Komponente Schutz vor modifizierten USB-Geräten
- `AntiAPT` - Installation der Komponente Endpoint Sensor
- `MSBitLocker` - Installation der Komponente Microsoft BitLocker Manager
- `AdminKitConnector` - Installation des Administrationsagent-Connectors zur Fernverwaltung des Programms über Kaspersky Security Center

  Mögliche Werte des Parameters für die Installation des Konnektors:

  - `1`. Der Administrationsagent-Connector wird installiert.
  - `0`. Der Administrationsagent-Connector wird nicht installiert.

Wird keine Komponente angegeben, werden alle für dieses Betriebssystem verfügbaren Komponenten installiert.

Der Schutz vor bedrohlichen Dateien ist eine obligatorische Komponente und wird unabhängig davon auf dem Computer installiert, welche Einstellungen in diesem Block angegeben sind.

3. [Tasks] - Auswahl von Aufgaben, welche in die Aufgabenliste von Kaspersky Endpoint Security aufgenommen werden:

   - `ScanMyComputer` - Aufgabe zur vollständigen Untersuchung
   - `ScanCritical` - Aufgabe zur Untersuchung wichtiger Bereiche
   - `Updater` - Update-Aufgabe

   Mögliche Werte der Parameter:

- `1`. Die Aufgabe wird in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen.
- `0`. Die Aufgabe wird nicht in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen.

Wird keine Aufgabe angegeben, werden alle Aufgaben in die Aufgabenliste von Kaspersky Endpoint Security eingetragen.

Anstelle des Wertes `1` können die Werte `yes`, `on`, `enable`, `enabled` verwendet werden. Anstelle des Werts `0` können die Werte `no`, `off`, `disable` oder `disabled` verwendet werden.

Schnellstartassistent

Der Schnellstartassistent von Kaspersky Endpoint Security wird am Ende des Installationsvorgangs gestartet. Der Schnellstartassistent ermöglicht die Aktivierung des Programms und empfängt Informationen über die zum Betriebssystem gehörenden Programme. Diese Programme werden in die Liste für vertrauenswürdige Programme aufgenommen, deren Aktionen im Betriebssystem keinen Einschränkungen unterliegen.

Die Oberfläche des Schnellstartassistenten besteht aus mehreren aufeinander folgenden Fenstern (Schritten). Verwenden Sie die Schaltflächen **Zurück** und **Weiter**, um zwischen den Fenstern des Schnellstartassistenten zu navigieren. Der Schnellstartassistent wird mit einem Klick auf die Schaltfläche **Beenden** abgeschlossen. Der Schnellstartassistent kann auf jedem Schritt mit einem Klick auf **Abbrechen** beendet werden.

Wird der Schnellstartassistent aus irgendeinem Grund abgebrochen, gehen die bereits festgelegten Einstellungswerte verloren. Wird das Programm später gestartet, öffnet sich der Schnellstartassistent erneut und fordert Sie zur Konfiguration der Einstellungen auf.

Schritt 1. Aktivierung des Programms

Auf dem Computer, auf dem das Programm aktiviert wird, müssen Systemdatum und Uhrzeit aktuell sein. Wurden das Systemdatum bzw. die Systemzeit nach der Programmaktivierung geändert, wird der Schlüssel nicht funktionsfähig. Das Programm wechselt in den Modus, in dem Updates und Kaspersky Security Network nicht verfügbar sind. Die Funktionsfähigkeit des Schlüssels kann nur durch eine Neuinstallation des Betriebssystems wiederhergestellt werden.

Wählen Sie bei diesem Schritt eine der folgenden Aktivierungsmethoden für Kaspersky Endpoint Security:

- **Mit Aktivierungscode aktivieren**. Wählen Sie diese Option aus und geben Sie den Aktivierungscode ein, wenn Sie das Programm mithilfe des Aktivierungscodes aktivieren möchten.
- **Mit Schlüsseldatei aktivieren**. Wählen Sie diese Option aus, wenn Sie das Programm mithilfe einer Schlüsseldatei aktivieren möchten.
- **Testversion aktivieren**. Wählen Sie diese Option aus, wenn Sie eine Testversion des Programms aktivieren möchten. Während der Gültigkeitsdauer, die von der Lizenz der Testversion bestimmt wird, kann der Benutzer das Programm mit vollem Funktionsumfang verwenden. Nach Ablauf der Lizenz werden die Programmfunktionen blockiert. Die erneute Aktivierung einer Testlizenz ist nicht möglich.

- **Später aktivieren**. Wählen Sie diese Option, um die Aktivierung von Kaspersky Endpoint Security zu überspringen. Der Benutzer kann in diesem Fall nur die Komponenten Schutz vor bedrohlichen Dateien und Firewall nutzen. Der Benutzer kann die Datenbanken und Module von Kaspersky Endpoint Security nach der Programminstallation nur ein einziges Mal aktualisieren. Die Option **Später aktivieren** steht nur beim ersten Start des Schnellstartassistenten direkt nach der Programminstallation zur Verfügung.

Um eine Testversion des Programms zu aktivieren oder um das Programm mit einem Aktivierungscode zu aktivieren, muss der Computer mit dem Internet verbunden sein.

Wählen Sie zur Fortsetzung des Schnellstartassistenten eine Aktivierungsmethode aus und klicken Sie auf **Weiter**. Klicken Sie auf **Abbrechen**, um den Schnellstartassistenten abzubrechen.

Schritt 2. Aktivierung mit einem Aktivierungscode

Dieser Schritt steht nur bei der Programmaktivierung mit einem Aktivierungscode zur Verfügung. Bei der Aktivierung einer Testversion des Programms oder bei der Programmaktivierung mit einer Schlüsseldatei wird dieser Schritt übersprungen.

Bei diesem Schritt sendet Kaspersky Endpoint Security Daten an den Aktivierungsserver, um den eingegebenen Aktivierungscode zu überprüfen.

- Wenn der Aktivierungscode die Überprüfung besteht, geht der Konfigurationsassistent automatisch zum nächsten Fenster.
- Konnte der Aktivierungscode nicht erfolgreich überprüft werden, erscheint eine entsprechende Meldung auf dem Bildschirm. In diesem Fall sollten Sie sich an den Händler wenden, bei dem Sie die Lizenz für Kaspersky Endpoint Security erworben haben.
- Wurde die zulässige Anzahl der Aktivierungen für diesen Aktivierungscode überschritten, erscheint eine entsprechende Meldung auf dem Bildschirm. Der Schnellstartassistent wird abgebrochen und das Programm fordert Sie auf, sich an den Technischen Support von Kaspersky Lab zu wenden.

Klicken Sie auf **Zurück**, um zum vorherigen Schritt des Schnellstartassistenten zurückzukehren. Klicken Sie auf **Abbrechen**, um den Schnellstartassistenten abzubrechen.

Schritt 3. Aktivierung mit einer Schlüsseldatei

Dieser Schritt steht nur bei der Programmaktivierung mit einer Schlüsseldatei zur Verfügung.

Bei diesem Schritt werden Sie aufgefordert, den Pfad der Schlüsseldatei anzugeben. Klicken Sie dazu auf die Schaltfläche **Durchsuchen** und wählen Sie die Schlüsseldatei im folgenden Format: `<Datei-ID>.key`.

Nach Auswahl der Schlüsseldatei werden im unteren Fensterbereich folgende Informationen angezeigt:

- Schlüssel
- Art der Lizenz (kommerzielle Lizenz oder Testlizenz) und Anzahl der Computer, für welche die Lizenz gilt.
- Aktivierungsdatum des Programms auf dem Computer
- Ablaufdatum der Lizenz
- Funktionalität des Programms, die laut Lizenz verfügbar ist
- Meldung über Probleme mit dem Schlüssel, falls solche Probleme vorliegen Beispiel: *Schwarze Liste der Schlüssel ist beschädigt*.

Klicken Sie auf **Zurück**, um zum vorherigen Schritt des Schnellstartassistenten zurückzukehren. Klicken Sie auf **Weiter**, um den Schnellstartassistenten fortzusetzen. Klicken Sie auf **Abbrechen**, um den Schnellstartassistenten abzubrechen.

Schritt 4. Zu aktivierende Funktionalität auswählen

Dieser Schritt steht nur bei der Aktivierung einer Testversion zur Verfügung.

Bei diesem Schritt können Sie wählen, welche Funktionalität nach der Programmaktivierung verfügbar sein soll:

- **Basisinstallation**: Wenn diese Option ausgewählt ist, sind nach der Programmaktivierung nur die Schutzkomponenten und die Komponente Programm-Überwachung verfügbar.
- **Standardinstallation**: Wenn diese Variante gewählt ist, werden nach der Programmaktivierung Schutz- und Kontrollkomponenten verfügbar sein.
- **Vollständige Installation**: Bei Auswahl dieser Variante sind nach der Programmaktivierung alle installierten Programmkomponenten einschließlich der Funktionalität zur Datenverschlüsselung verfügbar.

Wenn Sie bei der Installation bereits mehr Komponenten gewählt haben, als mit der erworbenen Lizenz zulässig sind, so werden die für diese Lizenz nicht verfügbaren Komponenten zwar nach der Programmaktivierung installiert, allerdings funktionieren sie nicht. Wenn weniger Komponenten installiert sind als laut der erworbenen Lizenz möglich, so werden die nicht installierten Programmkomponenten nach der Programmaktivierung im Fenster **Lizenzverwaltung** angezeigt.

In der Grundeinstellung ist die Standardinstallation ausgewählt.

Klicken Sie auf **Zurück**, um zum vorherigen Schritt des Schnellstartassistenten zurückzukehren. Klicken Sie auf **Weiter**, um den Schnellstartassistenten fortzusetzen. Klicken Sie auf **Abbrechen**, um den Schnellstartassistenten abzubrechen.

Schritt 5. Abschluss der Programmaktivierung

Bei diesem Schritt informiert Sie der Schnellstartassistent über die erfolgreiche Aktivierung von Kaspersky Endpoint Security. Weiterhin erhalten Sie Lizenzinformationen:

- Art der Lizenz (kommerzielle Lizenz oder Testlizenz) und Anzahl der Computer, für welche die Lizenz gilt.
- Ablaufdatum der Lizenz
- Funktionalität des Programms, die laut Lizenz verfügbar ist

Klicken Sie auf **Weiter**, um den Schnellstartassistenten fortzusetzen. Klicken Sie auf **Abbrechen**, um den Schnellstartassistenten abzubrechen.

Schritt 6. Erstkonfiguration des Programms abschließen

Das Abschlussfenster des Schnellstartassistenten enthält Informationen über die Fertigstellung der Installation von Kaspersky Endpoint Security.

Um Kaspersky Endpoint Security zu starten, klicken Sie auf **Beenden**.

Um den Schnellstartassistenten zu verlassen, ohne Kaspersky Endpoint Security anschließend zu starten, deaktivieren Sie das Kontrollkästchen **Kaspersky Endpoint Security für Windows starten** und klicken dann auf **Beenden**.

Schritt 7. Analyse des Betriebssystems

Bei diesem Schritt werden Informationen über die Programme empfangen, die zum Betriebssystem gehören. Diese Programme werden in die Liste für vertrauenswürdige Programme aufgenommen, deren Aktionen im Betriebssystem keinen Einschränkungen unterliegen.

Die Analyse anderer Programme erfolgt, wenn Programme nach der Installation von Kaspersky Endpoint Security zum ersten Mal gestartet werden.

Klicken Sie auf **Abbrechen**, um den Schnellstartassistenten abzubrechen.

Schritt 8. Erklärung zu Kaspersky Security Network

Bei diesem Schritt wird Ihnen vorgeschlagen, an Kaspersky Security Network teilzunehmen. Um an KSN teilzunehmen, sind folgende Aktionen erforderlich:

1. Beachten Sie die "Erklärung zu Kaspersky Security Network".
2. Wählen Sie eine der folgenden Varianten:
   - Wenn Sie mit allen Punkten einverstanden sind, wählen Sie die Variante **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network** aus.
   - Wenn Sie nicht mit den Teilnahmebedingungen für Kaspersky Security Network einverstanden sind, wählen Sie die Variante **Ich lehne die Nutzungsbedingungen für Kaspersky Security Network ab** aus.

Der Lieferumfang von Kaspersky Endpoint Security ist für die Nutzung von Kaspersky Security Network optimiert. Falls Sie die Teilnahme an Kaspersky Security Network abgelehnt haben, aktualisieren Sie Kaspersky Endpoint Security sofort nach dem Abschluss der Installation.

3. Um die Auswahl zu bestätigen, klicken Sie auf **OK**.

Methoden zum Upgrade der Vorgängerversionen des Programms

Um eine Vorgängerversion auf Kaspersky Endpoint Security 11 für Windows zu aktualisieren, müssen alle verschlüsselten Festplatten entschlüsselt werden.

Folgende Programme bieten die Möglichkeit eines Upgrades auf Kaspersky Endpoint Security 11 für Windows:

- Kaspersky Endpoint Security 10 Service Pack 1 für Windows (Version 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 für Windows (Version 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 für Windows (Version 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 für Windows (Version 10.2.5.3201)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 für Windows (Version 10.2.6.3733)
- Kaspersky Endpoint Security 10 Service Pack 2 für Windows (Version 10.3.0.6294)

Wenn Kaspersky Endpoint Security 10 Service Pack 2 für Windows auf die Version Kaspersky Endpoint Security 11 für Windows aktualisiert wird, werden jene Dateien, die in der älteren Programmversion ins Backup und in die Quarantäne verschoben wurden, in das Backup der neuen Programmversion übertragen. Für Versionen von Kaspersky Endpoint Security, die älter sind als Kaspersky Endpoint Security 10 Service Pack 2 für Windows, werden jene Dateien, die in der älteren Programmversion ins Backup und in die Quarantäne verschoben wurden, nicht übertragen.

Für ein Upgrade der Vorgängerversionen des Programms stehen folgende Methoden zur Verfügung:

- Lokal im interaktiven Modus mithilfe des Installationsassistenten
- Lokal im Silent-Modus über die Befehlszeile

- ferngesteuert mithilfe des Programmpakets Kaspersky Security Center (s. Hilfe zu Kaspersky Security Center)
- ferngesteuert über den Gruppenrichtlinienverwaltungs-Editor von Microsoft Windows (s. Dokumentation für das Betriebssystem)

Um ein Upgrade einer Vorgängerversion auf Kaspersky Endpoint Security 11 für Windows vorzunehmen, muss die Vorgängerversion nicht entfernt werden. Vor Beginn des Programm-Upgrades sollten Sie alle laufenden Programme schließen.

Vor dem Upgrade einer älteren Programmversion auf Kaspersky Endpoint Security 11 für Windows wird die Funktionalität zur vollständigen Festplattenverschlüsselung blockiert. Falls die Funktionalität zur vollständigen Festplattenverschlüsselung nicht blockiert werden kann, wird die Upgrade-Installation nicht gestartet.

Programm deinstallieren

Dieser Abschnitt enthält Informationen zur Deinstallation von Kaspersky Endpoint Security.

Methoden zur Deinstallation des Programms

Wenn Kaspersky Endpoint Security entfernt wird, sind der Computer und die Benutzerdaten ungeschützt.

Um das Programm Kaspersky Endpoint Security von einem Computer zu entfernen, gibt es mehrere Möglichkeiten:

- Lokal im interaktiven Modus mithilfe des Installationsassistenten
- Lokal im Silent-Modus über die Befehlszeile
- ferngesteuert mithilfe des Programmpakets Kaspersky Security Center (Informationen s. *Implementierungshandbuch für Kaspersky Security Center*)
- ferngesteuert über den Gruppenrichtlinienverwaltungs-Editor von Microsoft Windows (s. Dokumentation für das Betriebssystem)

Programm mithilfe des Installationsassistenten deinstallieren

Gehen Sie folgendermaßen vor, um Kaspersky Endpoint Security mithilfe des Installationsassistenten zu deinstallieren:

1. Öffnen Sie das Fenster **Systemsteuerung**. Dafür gibt es folgende Methoden:
   - Wenn Sie Windows 7 verwenden, wählen Sie im **Startmenü** den Punkt **Systemsteuerung** aus.

- Wenn Sie Windows 8 oder Windows 8.1 verwenden, drücken Sie die Tastenkombination **Win**+**I** und wählen Sie den Punkt **Systemsteuerung** aus.
- Wenn Sie Windows 10 verwenden, drücken Sie die Tastenkombination **Win**+**X** und wählen Sie den Punkt **Systemsteuerung** aus.

2. Wählen Sie im Fenster **Systemsteuerung** den Punkt **Programme und Features** aus.
3. Wählen Sie in der Liste der installierten Programme das Element **Kaspersky Endpoint Security für Windows** aus.
4. Klicken Sie auf **Deinstallieren/Ändern**.

   Das Fenster **Benutzerdefinierte Installation** des Installationsassistenten wird geöffnet.
5. Klicken Sie im Fenster des Installationsassistenten **Programm ändern, reparieren oder entfernen** auf **Löschen**.
6. Folgen Sie den Anweisungen des Installationsassistenten.

Schritt 1. Programmdaten zur erneuten Verwendung speichern

Bei diesem Schritt können Sie festlegen, welche vom Programm verwendeten Daten Sie beibehalten möchten, um sie später bei einer Neuinstallation des Programms (z. B. einer neueren Version) wiederzuverwenden. Wenn Sie keine Daten angeben, wird das Programm vollständig entfernt.

Um Programmdaten für die erneute Verwendung zu speichern,

aktivieren Sie die Kontrollkästchen der Daten, die gespeichert werden sollen:

- **Aktivierungsdaten** - Wenn das Programm später erneut installiert wird, muss es aufgrund dieser Daten nicht mehr aktiviert werden, sondern kann automatisch mit der aktuellen Lizenz genutzt werden. Voraussetzung ist, dass die Lizenz zum Zeitpunkt der Installation gültig ist.
- **Backup-Dateien** - Dateien, die vom Programm untersucht und ins Backup verschoben wurden.

  Der Zugriff auf Backup-Dateien, die nach der Deinstallation des Programms gespeichert bleiben, ist nur mit der Programmversion möglich, in welcher die Dateien gespeichert wurden.

  Backup-Objekte, die nach der Programmdeinstallation verwendet werden sollen, müssen vor der Deinstallation des Programms wiederhergestellt werden. Die Kaspersky-Lab-Experten raten jedoch davon ab, Objekte aus dem Backup wiederherzustellen, da dadurch der Computer beschädigt werden kann.
- **Programmeinstellungen** - Einstellungen für die Programmausführung, die bei der Nutzung angepasst wurden.

- **Lokaler Speicher für Chiffrierschlüssel** - Daten, die direkten Zugriff auf jene Dateien und Geräte ermöglichen, die vor dem Entfernen des Programms verschlüsselt wurden. Nachdem das Programm mit der Funktionalität zur Datenverschlüsselung neu installiert wurde, ist ein direkter Zugriff auf verschlüsselte Dateien und Geräte möglich.

  Dieses Kontrollkästchen ist standardmäßig aktiviert.

Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**. Klicken Sie auf **Abbrechen**, um den Installationsassistenten abzubrechen.

Schritt 2. Deinstallation des Programms bestätigen

Da die Programmdeinstallation den Schutz Ihres Computers gefährdet, muss das Entfernen des Programms bestätigt werden. Klicken Sie dazu auf die Schaltfläche **Entfernen**.

Sie können diesen Vorgang vor dem Abschluss der Programmdeinstallation jederzeit durch einen Klick auf **Abbrechen** stoppen.

Schritt 3. Deinstallation des Programms. Deinstallation abschließen

Bei diesem Schritt entfernt der Installationsassistent das Programm vom Benutzercomputer. Warten Sie, bis die Programmdeinstallation abgeschlossen wurde.

Während der Deinstallation des Programms kann ein Neustart des Betriebssystems erforderlich werden. Wenn Sie einen sofortigen Neustart ablehnen, wird der Abschluss der Deinstallation aufgeschoben, bis das Betriebssystem neu gestartet oder der Computer herunter- und hochgefahren wird.

Programm über die Befehlszeile deinstallieren

Sie können die Deinstallation des Programms aus der Befehlszeile starten. Dazu wird der entsprechende Befehl aus dem Ordner, in dem sich das Programmpaket befindet, ausgeführt. Die Deinstallation erfolgt im interaktiven oder im unbeaufsichtigten Modus (ohne den Installationsassistenten des Programms zu starten).

Um die Programm-Deinstallation im interaktiven Modus zu starten,

geben Sie in der Befehlszeile `setup_kes.exe /x` oder `msiexec.exe /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3}` ein.

Der Installationsassistent wird gestartet. Folgen Sie den Anweisungen des Installationsassistenten.

Um die Programm-Deinstallation im unbeaufsichtigten Modus zu starten,

geben Sie in der Befehlszeile `setup_kes.exe /s /x` oder `msiexec.exe /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3} /qn` ein.

Die Programm-Deinstallation im unbeaufsichtigten Modus (ohne den Installationsassistenten des Programms zu starten) wird gestartet.

Ist der Vorgang zur Programm-Deinstallation kennwortgeschützt, so müssen in der Befehlszeile der Benutzernamen und das entsprechende Kennwort angegeben werden.

Um das Programm im interaktiven Modus über die Befehlszeile zu entfernen, falls das Entfernen/Ändern/Reparieren von Kaspersky Endpoint Security durch einen Benutzername und ein Kennwort geschützt ist:

geben Sie in der Befehlszeile ein: `setup_kes.exe /pKLLOGIN=<Benutzername> /pKLPASSWD=***** /x` oder

`msiexec.exe KLLOGIN=<Benutzername> KLPASSWD=***** /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3}`.

Der Installationsassistent wird gestartet. Folgen Sie den Anweisungen des Installationsassistenten.

Um das Programm im unbeaufsichtigten Modus über die Befehlszeile zu entfernen, falls das Entfernen/Ändern/Reparieren von Kaspersky Endpoint Security durch einen Benutzername und ein Kennwort geschützt ist:

`geben Sie in der Befehlszeile ein: setup_kes.exe /pKLLOGIN=<Benutzername> /pKLPASSWD=***** /s /x` oder

`msiexec.exe /x {E7012AFE-DB97-4B8B-9513-E98C0C3AACE3} KLLOGIN=<Benutzername> KLPASSWD=***** /qn`.

Objekte und Daten löschen, die nach dem Testlauf des Authentifizierungsagenten verblieben sind

Wenn bei der Deinstallation des Programms Kaspersky Endpoint Security Objekte und Daten gefunden werden, die nach einem Testlauf des Authentifizierungsagenten auf der Systemfestplatte verblieben sind, so wird die Programmdeinstallation abgebrochen und kann erst wieder gestartet werden, nachdem diese Objekte und Daten gelöscht wurden.

Objekte und Daten verbleiben nach einem Testlauf des Authentifizierungsagenten nur in Ausnahmefällen auf der Systemfestplatte. Dies kann beispielsweise vorkommen, wenn der Computer nach dem Übernehmen der Richtlinie für Kaspersky Security Center, die entsprechende Verschlüsselungseinstellungen enthält, noch nicht neu gestartet wurde oder wenn das Programm nach einem Testlauf des Authentifizierungsagenten nicht gestartet wird.

Es gibt zwei Methoden, um Objekte und Daten zu löschen, die nach einem Testlauf des Authentifizierungsagenten auf der Systemfestplatte verblieben sind:

- mithilfe der Richtlinie für Kaspersky Security Center
- mithilfe des Reparatur-Tools

Um die Objekte und Daten, die nach einem Testlauf des Authentifizierungsagenten verblieben sind, mithilfe der Richtlinie für Kaspersky Security Center zu löschen, gehen Sie wie folgt vor:

1. Übernehmen Sie für den Computer die Richtlinie für Kaspersky Security Center mit den Einstellungen, die für die Entschlüsselung aller Computerfestplatten gelten.

2. Starten Sie Kaspersky Endpoint Security.

Um Daten über die Inkompatibilität des Authentifizierungsagenten zu löschen,

geben Sie in der Befehlszeile ein: `avp pbatestreset`.

Damit der Befehl `avp pbatestreset` ausgeführt werden kann, müssen die Verschlüsselungskomponenten installiert sein.

Programmoberfläche

Dieser Abschnitt enthält Informationen zu den wichtigsten Elementen der Programmoberfläche.

Programmsymbol im Infobereich

Sofort nach der Installation von Kaspersky Endpoint Security erscheint das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows.

Das Symbol übernimmt folgende Funktionen:

- Es dient als Indikator für die Ausführung des Programms.
- Es ermöglicht den Zugriff auf das Kontextmenü und auf das Programmhauptfenster.

Indikator für die Programmarbeit

Das Symbol dient als Indikator für die Ausführung des Programms.

- Das Symbol bedeutet, dass alle Schutzkomponenten aktiviert sind.
- Das Symbol bedeutet, dass bei der Ausführung von Kaspersky Endpoint Security wichtige Ereignisse eingetreten sind, die beachtet werden müssen. Beispiele: Die Komponente Schutz vor bedrohlichen Dateien ist deaktiviert oder die Programm-Datenbanken sind veraltet.
- Das Symbol bedeutet, dass bei der Ausführung von Kaspersky Endpoint Security kritische Ereignisse eingetreten sind. Beispiele: Störung bei der Ausführung einer Komponente, Beschädigung der Programm-Datenbanken.

Kontextmenü des Programmsymbols

Das Kontextmenü des Programmsymbols enthält die folgenden Punkte:

- **Kaspersky Endpoint Security für Windows**. Öffnet das Programmhauptfenster. In diesem Fenster können Sie die Funktion der Komponenten und Aufgaben des Programms anpassen sowie eine Statistik zu verarbeiteten Dateien und gefundenen Bedrohungen einsehen.

- **Einstellungen**. Öffnet das Fenster **Einstellungen**. Auf der Registerkarte **Einstellungen** können Sie die Standardeinstellungen des Programms anpassen.

- **Schutz und Kontrolle anhalten** / **Schutz und Kontrolle fortsetzen**. Hält die Schutz- und Kontrollkomponenten vorübergehend an bzw. setzt diese Komponenten fort. Dieser Punkt des Kontextmenüs hat keine Auswirkung auf die Durchführung der Update-Aufgabe und der Untersuchungsaufgaben und ist nur verfügbar, wenn die Richtlinie für Kaspersky Security Center deaktiviert ist.

  Kaspersky Security Network wird von Kaspersky Endpoint Security unabhängig davon verwendet, ob die Schutzkomponenten und Kontrollkomponenten angehalten/fortgesetzt wurden.

- **Richtlinie deaktivieren** / **Richtlinie aktivieren**. Deaktiviert / aktiviert eine Richtlinie für Kaspersky Security Center. Dieser Punkt ist im Kontextmenü verfügbar, wenn der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie unterliegt und in den Richtlinieneinstellungen ein Kennwort für die Deaktivierung der Richtlinie für Kaspersky Security Center festgelegt ist.

- **Über das Programm**. Öffnet ein Informationsfenster mit Angaben zum Programm.

- **Beenden**. Beendet Kaspersky Endpoint Security. Wenn Sie diese Option im Kontextmenü gewählt haben, wird das Programm aus dem Arbeitsspeicher des Computers entfernt.

Kontextmenü des Programmsymbols

Das Kontextmenü von Kaspersky Endpoint Security lässt sich durch einen Rechtsklick auf das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows öffnen.

Programmhauptfenster

In der Benutzeroberfläche des Hauptfensters von Kaspersky Endpoint Security befinden sich Elemente, über die der Benutzer auf die wichtigsten Programmfunktionen zugreifen kann.

Das Programmhauptfenster enthält folgende Elemente:

- Link zu **Kaspersky Endpoint Security für Windows**. Mit diesem Link wird das Fenster **Über das Programm** mit Angaben über die Programmversion geöffnet.

- Schaltfläche ⓘ. Mit dieser Schaltfläche gelangen Sie zum Hilfesystem für Kaspersky Endpoint Security.

- Block **Technologien zum Erkennen von Bedrohungen**. Dieser Block enthält folgende Informationen:

- Der linke Bereich des Blocks enthält eine Liste der Technologien zum Erkennen von Bedrohungen. Rechts vom Namen der jeweiligen Technologie zum Erkennen von Bedrohungen wird die Anzahl der Bedrohungen angezeigt, die mithilfe dieser Technologie gefunden wurden.

- Abhängig davon, ob aktive Bedrohungen vorhanden sind, wird in der Mitte des Blocks einer der folgenden Hinweise angezeigt:

  - **Keine Bedrohungen**. Wird dieser Hinweis angezeigt, so wird bei Klick auf den Block **Technologien zum Erkennen von Bedrohungen** das Fenster **Technologien zum Erkennen von Bedrohungen** geöffnet. Dort finden Sie eine kurze Beschreibung der Technologien zum Erkennen von Bedrohungen sowie den Status und eine globale Statistik über die Infrastruktur der Cloud-Dienste von Kaspersky Security Network.

  - **n aktive Bedrohungen**. Wird dieser Hinweis angezeigt, so wird bei Klick auf den Block **Technologien zum Erkennen von Bedrohungen** das Fenster **Aktive Bedrohungen** geöffnet. Dort finden Sie eine Liste mit Ereignissen, die mit infizierten Dateien zusammenhängen, welche aus bestimmten Gründen nicht verarbeitet wurden.

- Block **Schutzkomponenten**. Bei Klick auf diesen Block wird das Fenster **Schutzkomponenten** geöffnet. In diesem Fenster können Sie den Funktionsstatus der installierten Komponenten einsehen. Außerdem können Sie aus diesem Fenster für eine beliebige der installierten Komponenten, unter Ausnahme der Verschlüsselungskomponenten, den Unterabschnitt im Fenster **Einstellungen** öffnen. Dort befinden sich die Einstellungen dieser Komponente.

- Block **Aufgaben**. Bei Klick auf diesen Block wird das Fenster **Aufgaben** geöffnet. In diesem Fenster können Sie die Aufgaben für Kaspersky Endpoint Security verwalten. Die Aufgaben gewährleisten die Aktualität der Datenbanken und Programm-Module, führen eine Untersuchung von Dateien auf Viren und andere bedrohliche Programme, sowie die Integritätsprüfung für das Programm aus.

- Schaltfläche **Berichte**. Mit dieser Schaltfläche wird das Fenster **Berichte** geöffnet. Es enthält Informationen über Ereignisse, die den generellen Programmbetrieb betreffen, sowie Ereignisse über bestimmte Komponenten und über die Ausführung von Aufgaben.

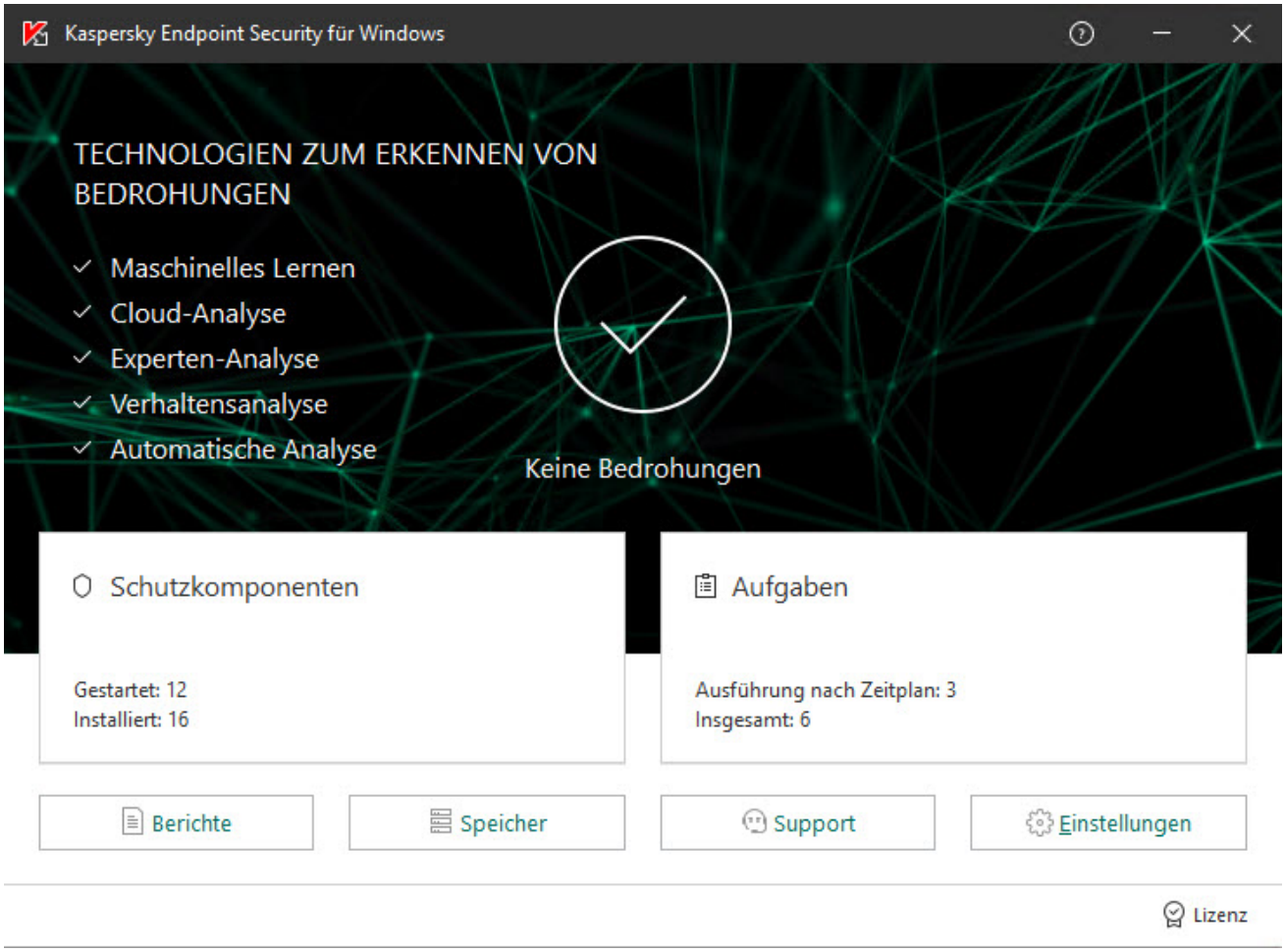
- Schaltfläche **Datenverwaltung**. Mit dieser Schaltfläche wird das Fenster **Backup** geöffnet. In diesem Fenster können Sie eine Liste mit Kopien von infizierten Dateien einsehen, die vom Programm gelöscht wurden.

- Schaltfläche **Support**. Mit dieser Schaltfläche wird das Fenster **Support** geöffnet. Es enthält Informationen über das Betriebssystem und die installierte Version von Kaspersky Endpoint Security sowie Links zu den Informationsressourcen von Kaspersky Lab.

- Schaltfläche **Einstellungen**. Mit dieser Schaltfläche wird das Fenster **Einstellungen** geöffnet, in dem Sie die standardmäßigen Programmeinstellungen ändern können.

- Schaltfläche / / . Mit dieser Schaltfläche wird das Fenster **Ereignisse** geöffnet. Dieses Fenster enthält Informationen über verfügbare Updates sowie Anfragen für den Zugriff auf verschlüsselte Dateien und Geräte.

- Link **Lizenz**. Mit diesem Link wird das Fenster **Lizenzverwaltung** mit Informationen über die aktuelle Lizenz geöffnet.



Programmhauptfenster

Um das Hauptfenster von Kaspersky Endpoint Security zu öffnen, führen Sie eine der folgenden Aktionen aus:

- Klicken Sie auf das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows.
- Wählen Sie im Kontextmenü des Programmsymbols den Punkt **Kaspersky Endpoint Security für Windows**.

Lizenz verlängern

Bevor die Gültigkeit einer Lizenz abläuft, können Sie diese verlängern. So vermeiden Sie, dass der Computer nach Ablauf der Lizenz bis zur Aktivierung des Programms mit der neuen Lizenz ungeschützt ist.

Gehen Sie folgendermaßen vor, um die Gültigkeitsdauer einer Lizenz zu verlängern:

1. Fordern Sie einen neuen Aktivierungscode oder eine Schlüsseldatei für das Programm an.
2. Fügen Sie den Reserveschlüssel mithilfe des angeforderten Aktivierungscodes oder der Schlüsseldatei hinzu.

   Dadurch wird ein Reserveschlüssel hinzugefügt, der zum aktiven Schlüssel wird, sobald die Lizenz abläuft.

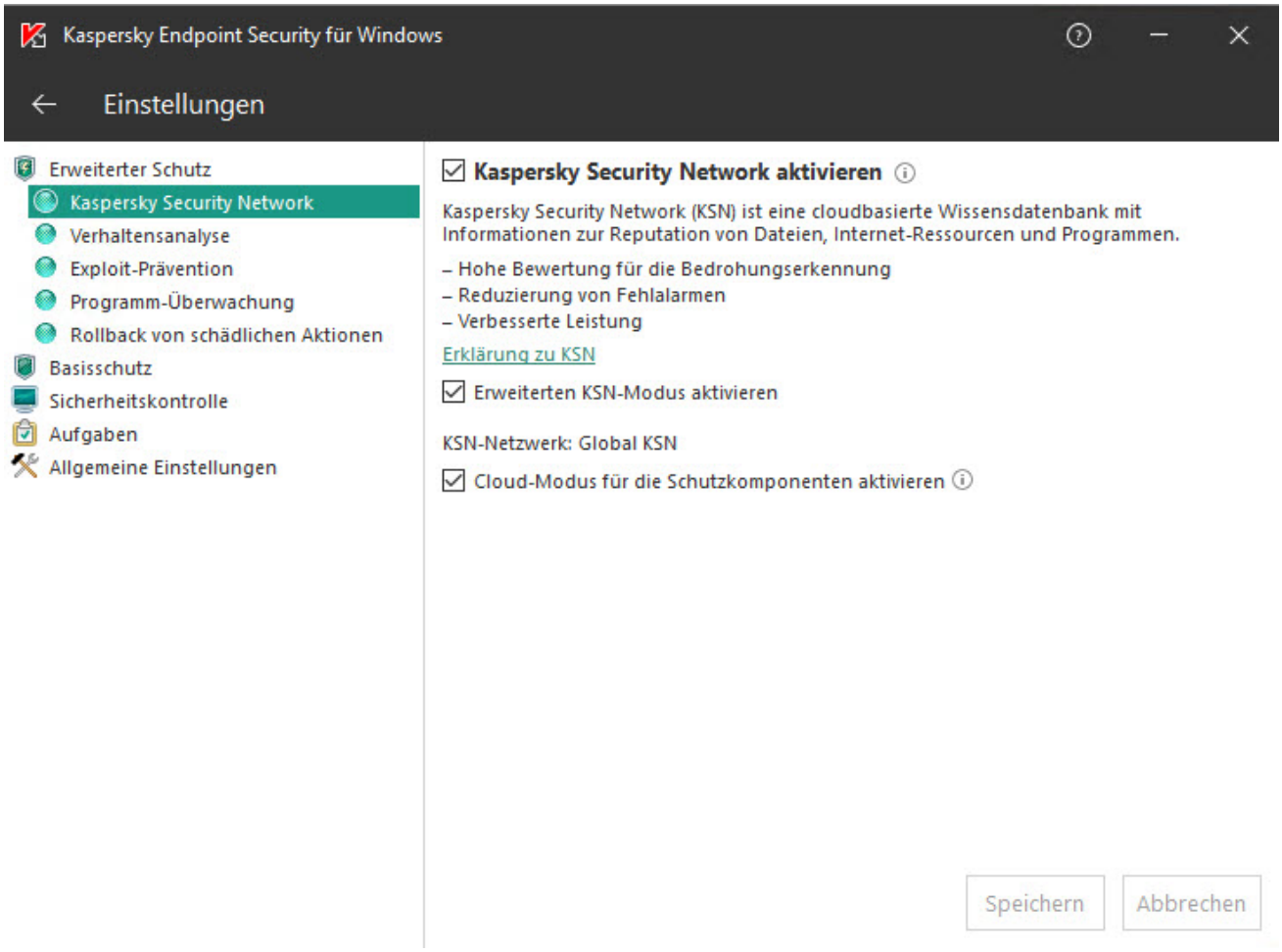
Wenn ein Reserveschlüssel zum aktiven Schlüssel wird, kann es aufgrund der Auslastung der Kaspersky-Lab-Aktivierungsserver zu Verzögerungen kommen.

Registerkarte zum Anpassen der Programmeinstellungen

Im Konfigurationsfenster für Kaspersky Endpoint Security können folgende Einstellungen angepasst werden: allgemeine Programmeinstellungen, Einstellungen für die einzelnen Komponenten, Berichte und Datenverwaltung, Untersuchungsaufgaben, Update-Aufgabe und Verbindung mit den Servern von Kaspersky Security Network.

Die Registerkarte zum Anpassen der Programmeinstellungen besteht aus zwei Bereichen (s. Abb. unten):

- Der linke Bereich enthält Programmkomponenten, Aufgaben und einen Abschnitt mit erweiterten Einstellungen, der aus mehreren Teilabschnitten besteht.
- Der rechte Bereich enthält Steuerungselemente, mit denen die Einstellungen der im linken Fensterbereich ausgewählten Komponente oder Aufgabe sowie die erweiterten Einstellungen angepasst werden können.



Registerkarte zum Anpassen der Programmeinstellungen

Um das Programmkonfigurationsfenster zu öffnen, führen Sie eine der folgenden Aktionen aus:

- Wählen Sie im Programmhauptfenster die Registerkarte **Einstellungen**.

- Wählen Sie im Kontextmenü des Programmsymbols den Punkt **Einstellungen**.

Einfache Programmoberfläche

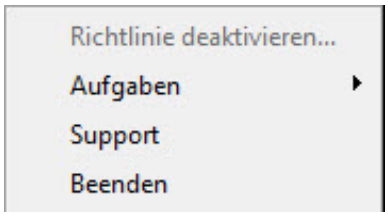
Wenn der Client-Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie von Kaspersky Security Center unterliegt und in dieser Richtlinie die Anzeige der einfachen Programmoberfläche festgelegt ist, so ist das Programmhauptfenster auf diesem Client-Computer nicht verfügbar. Der Benutzer kann durch Rechtsklick das Kontextmenü des Symbols von Kaspersky Endpoint Security öffnen (siehe folgende Abb.), das folgende Punkte enthält:

- **Richtlinie deaktivieren**. Deaktiviert die Richtlinie für Kaspersky Security Center, auf dem Client-Computer, auf welchem das Programm Kaspersky Endpoint Security installiert ist. Dieser Punkt ist im Kontextmenü verfügbar, wenn der Computer einer Richtlinie unterliegt und in den Richtlinieneinstellungen ein Kennwort für die Deaktivierung der Richtlinie für Kaspersky Security Center festgelegt ist.

- **Aufgaben**. Dropdown-Liste mit folgenden Elementen:
  - **Update**.
  - **Update-Rollback**.
  - **Vollständige Untersuchung**.
  - **Benutzerdefinierte Untersuchung**.
  - **Untersuchung wichtiger Bereiche**.
  - **Integritätsprüfung**.

- **Support**. Öffnen des Fensters **Support**, das Informationen enthält, die zur Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab erforderlich sind.

- **Beenden**. Kaspersky Endpoint Security beenden.



Kontextmenü des Programmsymbols bei der Anzeige der einfachen Programmoberfläche

Lizenzierung des Programms

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzverwaltung für das Programm zusammenhängen.

Über den Lizenzvertrag

Der *Lizenzvertrag* ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er bestimmt die Nutzungsbedingungen für das Programm.

Lesen Sie den Lizenzvertrag sorgfältig durch, bevor Sie beginnen, mit dem Programm zu arbeiten.

Die Lizenzbedingungen können Sie wie folgt einsehen:

- Im interaktiven Modus während der Installation von Kaspersky Endpoint Security
- Im Dokument license.txt. Dieses Dokument gehört zum Lieferumfang des Programms.

Wenn Sie bei der Programminstallation den Lizenzbedingungen zustimmen, gilt Ihr Einverständnis mit den Lizenzbedingungen als erteilt. Falls Sie dem Lizenzvertrag nicht zustimmen, müssen Sie die Programminstallation abbrechen.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, das Ihnen auf Basis eines Lizenzvertrags überlassen wird.

Die Lizenz berechtigt Sie zur Nutzung folgender Leistungen:

- Nutzung des Programm in Übereinstimmung mit den Bedingungen des Lizenzvertrags
- Nutzung des Technischen Supports

Der Umfang der verfügbaren Leistungen und die Nutzungsdauer für das Programm sind vom Typ der Lizenz abhängig, mit der das Programm aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen:

- *Testlizenz* - kostenlose Lizenz zum Kennenlernen des Programms.

  Die Testlizenz ist in der Regel nur für eine kurze Zeit gültig. Nach Ablauf der Testlizenz stellt Kaspersky Endpoint Security die Funktion ein. Um das Programm weiterhin nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

- *Kommerzielle Lizenz* - kostenpflichtige Lizenz, die beim Kauf des Programms zur Verfügung gestellt wird.

  Die im Rahmen einer kommerziellen Lizenz verfügbare Programmfunktionalität ist von der Auswahl des Produkts abhängig. Das ausgewählte Produkt ist im Lizenzzertifikat angegeben. Informationen über die verfügbaren Produkte finden Sie auf der Website von Kaspersky Lab.

  Nach Ablauf der kommerziellen Lizenz funktioniert das Programm auch weiterhin, jedoch lediglich mit beschränktem Funktionsumfang. Sie können die Schutz- und Kontrollkomponenten verwenden und eine Untersuchung ausführen. Dabei werden die Programm-Datenbanken verwendet, die bei Ablauf der Lizenz installiert waren. Außerdem verschlüsselt das Programm weiterhin Dateien, die geändert werden und vor Ablauf der Lizenz verschlüsselt worden sind. Neue Dateien werden aber nicht mehr verschlüsselt. Kaspersky Security Network kann nicht genutzt werden.

  Um die Funktionalitätseinschränkungen für Kaspersky Endpoint Security aufzuheben, muss die kommerzielle Lizenz verlängert oder eine neue Lizenz gekauft werden.

Es wird empfohlen, die Lizenz spätestens dann zu verlängern, wenn die aktive Lizenz abläuft. Nur so lässt sich für Ihren Computer ein optimaler Schutz vor Sicherheitsbedrohungen gewährleisten.

Über das Lizenzzertifikat

Das *Lizenzzertifikat* ist ein Dokument, das Sie zusammen mit der Schlüsseldatei oder dem Aktivierungscode erhalten.

Das Lizenzzertifikat enthält folgende Informationen über die vorliegende Lizenz:

- Auftragsnummer
- Informationen über den Benutzer, für den die Lizenz ausgestellt wurde
- Informationen über das Programm, das mit der ausgestellten Lizenz aktiviert werden kann
- quantitative Beschränkungen im Hinblick auf die Lizenzierungseinheiten (beispielsweise Geräte, auf denen das Programm mit dieser Lizenz verwendet werden darf)
- Datum für den Beginn der Lizenzgültigkeit
- Ablaufdatum der Lizenz oder Gültigkeitsdauer der Lizenz
- Lizenztyp

Über das Abo

Ein *Abo für Kaspersky Endpoint Security* ist ein Auftrag, nach dem das Programm mit bestimmten Einstellungen (Abo-Laufzeit, Anzahl der geschützten Geräte) genutzt werden kann. Ein Abo für Kaspersky Endpoint Security kann bei einem Dienstanbieter registriert werden (z. B. bei einem Internet-Provider). Das Abo kann manuell oder automatisch verlängert oder auch gekündigt werden. Das Abo wird auf der Provider-Webseite verwaltet.

Es gibt beschränkte (z. B. auf ein Jahr) und unbefristete (ohne Ablaufdatum) Abos. Um Kaspersky Endpoint Security weiterhin zu nutzen, muss ein beschränktes Abo rechtzeitig verlängert werden. Ein unbefristetes Abo wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Provider überwiesen wird.

Nach Ablauf eines befristeten Abonnements wird möglicherweise eine Nachfrist zur Abo-Verlängerung gewährt, während der die Programmfunktionalität erhalten bleibt. Das Angebot und die Dauer einer Nachfrist sind vom Dienstanbieter abhängig.

Um Kaspersky Endpoint Security mit einem Abo zu nutzen, muss der Aktivierungscode übernommen werden, den der Provider zur Verfügung stellt. Nach Übernahme des Aktivierungscodes wird der aktive Schlüssel installiert, der festlegt, welche Lizenz für die Nutzung des Programms gemäß dem Abo zur Verfügung steht. Hierbei kann ein Reserveschlüssel nur mithilfe eines Aktivierungscodes installiert werden. Mithilfe einer Schlüsseldatei oder auf Abo-Basis ist dies nicht möglich.

Die Programmfunktionen, die auf Grundlage eines Abos zur Verfügung stehen, können den Programmfunktionen der folgenden Arten von kommerziellen Lizenzen entsprechen: Standard, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Diese Lizenztypen sind für den Schutz von Datei-Servern, Workstations sowie Smartphones und Tablet-PCs vorgesehen. Sie erlauben die Verwendung der Überwachungskomponenten auf Workstations, Smartphones und Tablet-PCs.

Für die Abo-Verwaltung stehen je nach Provider unterschiedliche Optionen zur Verfügung. Der Provider stellt möglicherweise keine Nachfrist für die Verlängerung des Abos zur Verfügung, innerhalb der die Programmfunktionen erhalten bleiben.

Auf Grundlage eines Abos erworbene Aktivierungscodes können nicht für die Aktivierung vorheriger Versionen von Kaspersky Endpoint Security genutzt werden.

Über den Aktivierungscode

Ein *Aktivierungscode* besteht aus einer unikalen Folge von zwanzig Ziffern und lateinischen Buchstaben. Diesen Code erhalten Sie beim Kauf einer kommerziellen Lizenz für die Nutzung von Kaspersky Endpoint Security.

Um das Programm mithilfe eines Aktivierungscodes zu aktivieren, ist für den Zugriff auf die Kaspersky-Lab-Aktivierungsserver eine Internetverbindung erforderlich.

Bei der Programmaktivierung mithilfe eines Aktivierungscodes wird der aktive Schlüssel installiert. Hierbei kann ein Reserveschlüssel nur mithilfe eines Aktivierungscodes installiert werden. Mithilfe einer Schlüsseldatei oder auf Abo-Basis ist dies nicht möglich.

Wenn ein Aktivierungscode nach der Programmaktivierung verloren geht, können Sie den Aktivierungscode wiederherstellen. Der Aktivierungscode kann beispielsweise für die Registrierung bei Kaspersky CompanyAccount erforderlich sein. Um einen Aktivierungscode wiederherzustellen, müssen Sie sich an den Technischen Support von Kaspersky Lab wenden.

Über den Schlüssel

Ein *Schlüssel* ist eine individuelle Zeichenabfolge aus Buchstaben und Ziffern. Der Schlüssel gewährleistet die Programmnutzung gemäß den Bedingungen, die im Lizenzzertifikat festgelegt sind (Lizenztyp, Gültigkeitsdauer der Lizenz, Lizenzbeschränkung).

Für Schlüssel, die auf Grundlage eines Abos installiert werden, wird kein Lizenzzertifikat zur Verfügung gestellt.

Ein Schlüssel kann dem Programm mithilfe eines Aktivierungscodes oder einer Schlüsseldatei hinzugefügt werden.

Sie können Schlüssel hinzufügen, ersetzen oder löschen. Kaspersky Lab kann einen Schlüssel blockieren, wenn die Bedingungen des Lizenzvertrags verletzt werden. Wenn ein Schlüssel gesperrt ist, muss ein anderer Schlüssel hinzugefügt werden, damit das Programm funktioniert.

Wenn der Schlüssel für eine Lizenz gelöscht wird, sind die Programmfunktionen mehr verfügbar. Nachdem ein solcher Schlüssel gelöscht wurde, kann er nicht mehr hinzugefügt werden.

Ein Schlüssel kann entweder ein aktiver Schlüssel oder ein Reserveschlüssel sein.

Ein *aktiver Schlüssel* ist ein Schlüssel, der momentan für das Programm verwendet wird. Als aktiver Schlüssel kann entweder ein Schlüssel für eine Testlizenz oder für eine kommerzielle Lizenz hinzugefügt werden. Im Programm kann es nur einen aktiven Schlüssel geben.

Ein *Reserveschlüssel* gewährt das Recht auf die Programmnutzung, wird aber momentan nicht verwendet. Nach Ablauf des aktiven Schlüssels wird automatisch der Reserveschlüssel aktiviert. Ein Reserveschlüssel kann nur hinzugefügt werden, wenn ein aktiver Schlüssel vorhanden ist.

Ein Schlüssel für eine Testlizenz kann nur als aktiver Schlüssel hinzugefügt werden. Er kann nicht als Reserveschlüssel hinzugefügt werden. Ein aktiver Schlüssel kann nicht durch einen Schlüssel für eine Testlizenz ersetzt werden.

Wird ein Schlüssel auf die Schwarze Liste gesetzt, so stehen die Programmfunktionen gemäß der Lizenz, mit der das Programm aktiviert wurde, noch acht Tage lang zur Verfügung. Kaspersky Security Network und die Updates für Datenbanken und Programm-Module sind uneingeschränkt verfügbar. Das Programm benachrichtigt den Benutzer darüber, dass der Schlüssel auf die Schwarze Liste gesetzt wurde. Nach Ablauf von acht Tagen sind die Programmfunktionen im gleichen Umfang verfügbar wie nach dem Ablauf der Lizenz - das Programm funktioniert weiterhin, jedoch ohne Updates und ohne Zugriff auf Kaspersky Security Network.

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key. Diese Datei erhalten Sie nach dem Kauf von Kaspersky Endpoint Security. Mit der Schlüsseldatei wird ein Schlüssel für die Programmaktivierung hinzugefügt.

Um das Programm mithilfe einer Schlüsseldatei zu aktivieren, ist kein Zugriff auf die Kaspersky-Lab-Aktivierungsserver erforderlich.

Wenn eine Schlüsseldatei versehentlich gelöscht wurde, können Sie die Datei wiederherstellen. Eine Schlüsseldatei kann beispielsweise für die Registrierung bei Kaspersky CompanyAccount erforderlich sein.

Es bestehen folgende Möglichkeiten, um eine Schlüsseldatei wiederherzustellen:

- Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab
- Auf der Kaspersky-Lab-Website mithilfe des vorhandenen Aktivierungscodes eine Schlüsseldatei anfordern

Über die Zurverfügungstellung von Daten

Wenn für die Aktivierung von Kaspersky Endpoint Security ein Aktivierungscode verwendet wird, stimmen Sie der automatischen Übertragung folgender Informationen zu, damit die Rechtmäßigkeit der

Programmverwendung überprüft werden kann:

- Typ, Version und Sprachversion von Kaspersky Endpoint Security
- Versionen der installierten Updates für Kaspersky Endpoint Security
- ID des Computers und ID der Installation von Kaspersky Endpoint Security auf dem Computer
- Aktivierungscode und einmalige ID für die Aktivierung der aktuellen Lizenz
- Typ, Version und Bit-Version des Betriebssystems, Name der virtuellen Umgebung, falls das Programm Kaspersky Endpoint Security in einer virtuellen Umgebung installiert ist
- IDs der Komponenten von Kaspersky Endpoint Security, die zum Zeitpunkt der Datenbereitstellung aktiv sind

Kaspersky Lab kann diese Informationen auch verwenden, um statistische Informationen über die Verbreitung und Verwendung von Kaspersky-Lab-Software zu erstellen.

Wenn Sie einen Aktivierungscode verwenden, stimmen Sie der automatischen Übertragung der oben genannten Daten zu. Wenn Sie nicht damit einverstanden sind, Kaspersky Lab diese Informationen bereitzustellen, muss für die Aktivierung von Kaspersky Endpoint Security eine Schlüsseldatei verwendet werden.

Wenn Sie die Bedingungen des Lizenzvertrags akzeptieren, stimmen Sie der automatischen Weitergabe folgender Informationen zu:

- Beim Update von Kaspersky Endpoint Security:
  - Version von Kaspersky Endpoint Security
  - ID der aktuellen Lizenz
  - ID von Kaspersky Endpoint Security
  - Seriennummer der aktuellen Lizenz
  - einmalige ID für den Start der Update-Aufgabe
  - einmalige ID der Installation von Kaspersky Endpoint Security.
- Beim Wechsel mithilfe von Links aus der Benutzeroberfläche von Kaspersky Endpoint Security:
  - Version von Kaspersky Endpoint Security
  - Version des Betriebssystems
  - Aktivierungsdatum von Kaspersky Endpoint Security
  - Ablaufdatum der Lizenz
  - Erstellungsdatum des Schlüssels
  - Installationsdatum von Kaspersky Endpoint Security

- ID von Kaspersky Endpoint Security
- ID der aktuellen Lizenz
- ID der gefundenen Schwachstelle des Betriebssystems
- ID des zuletzt installierten Updates für Kaspersky Endpoint Security
- ID der Schwachstelle, welche bei der Untersuchung auf verwundbare Programme gefunden wurde
- Hash des gefundenen Objekts, das eine Bedrohung darstellt, und Name dieser Bedrohung nach der Kaspersky-Lab-Klassifikation
- Kategorie des Aktivierungsfehlers für Kaspersky Endpoint Security
- Code des aufgetretenen Fehlers
- Code des Aktivierungsfehlers für Kaspersky Endpoint Security
- Anzahl der Tage bis zum Ablauf des Schlüssels
- Anzahl der Tage, die seit dem Hinzufügen des Schlüssels vergangen sind
- Anzahl der Tage, die seit dem Ablauf der Lizenz vergangen sind
- Anzahl der Computer, auf welche sich die aktuellen Lizenzen erstrecken
- Seriennummer der aktuellen Lizenz
- Gültigkeitsdauer der Lizenz für Kaspersky Endpoint Security
- aktueller Status der Lizenz
- Typ der aktuellen Lizenz
- Typ des Programms
- einmalige ID für den Start der Update-Aufgabe
- einmalige ID der Installation von Kaspersky Endpoint Security
- einmalige ID der Software-Installation auf dem Computer
- Sprache der Benutzeroberfläche von Kaspersky Endpoint Security

- Über die Teilnahme an Kaspersky Security Network:
  - Tatsache, ob die Erklärung zu Kaspersky Security Network akzeptiert oder abgelehnt wurde
  - Datum und Uhrzeit der Zustimmung zu / Ablehnung der Erklärung zu Kaspersky Security Network
  - ID der Erklärung zu Kaspersky Security Network und Version der Erklärung zu Kaspersky Security Network, die vom Benutzer akzeptiert oder abgelehnt wurde

- Informationen über die Aktivierung/Deaktivierung des Kontrollkästchens **Kaspersky Security Network aktivieren**
- Informationen über die Aktivierung/Deaktivierung des Kontrollkästchens **Erweiterten KSN-Modus aktivieren**
- einmalige ID des Computers und des Benutzers
- vollständige Programmversion und Typ des Programms

Wenn Kaspersky Security Network vollständig deaktiviert wird, wird diese Statistik ab dem Zeitpunkt der Deaktivierung innerhalb der folgenden 24 Stunden alle 4 Stunden gesendet. Falls die Teilnahme an Kaspersky Security Network im Verlauf der Installation von Kaspersky Endpoint Security abgelehnt wird, wird diese Statistik ab dem Zeitpunkt der Deaktivierung innerhalb der folgenden 24 Stunden ebenfalls alle 4 Stunden gesendet.

Kaspersky Lab schützt die erhaltenen Informationen in Übereinstimmung mit geltenden gesetzlichen Bestimmungen und mit den aktuellen Richtlinien von Kaspersky Lab.

Ausführliche Angaben darüber, wie Informationen über die Programmverwendung empfangen, verarbeitet, gespeichert und gelöscht werden, nachdem der Lizenzvertrag und die Erklärung zu Kaspersky Security Network akzeptiert worden sind, finden Sie in den genannten Dokumenten und auf der Kaspersky-Lab-Website . Die Dateien license.txt und ksn_<ID der Sprache>.txt mit den Texten des Endbenutzer-Lizenzvertrags und der Erklärung zu Kaspersky Security Network gehören zum Lieferumfang des Programms.

Lizenz-Info anzeigen

Gehen Sie folgendermaßen vor, um Informationen zur Lizenz anzuzeigen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche / , die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Lizenzverwaltung** wird geöffnet. Der Abschnitt im oberen Bereich des Fensters **Lizenzverwaltung** bietet Informationen zur Lizenz.

Lizenz kaufen

Sie können die Lizenz auch nach der Installation des Programms erwerben. Beim Kauf einer Lizenz erhalten Sie einen Aktivierungscode oder eine Schlüsseldatei zur Aktivierung des Programms.

Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche / , die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Lizenzverwaltung** wird geöffnet.

3. Führen Sie im Fenster **Lizenzverwaltung** eine der folgenden Aktionen aus:

   - Klicken Sie auf die Schaltfläche **Lizenz kaufen**, wenn kein einziger Schlüssel hinzugefügt wurde oder nur der Schlüssel einer Testlizenz vorhanden ist.
   - Klicken Sie auf die Schaltfläche **Lizenz verlängern**, wenn ein Schlüssel für die kommerzielle Lizenz hinzugefügt wurde.

   Die Website des Kaspersky-Lab-Online-Shops wird geöffnet. Dort können Sie eine Lizenz erwerben.

Abo verlängern

Wenn das Programm im Abo genutzt wird, greift Kaspersky Endpoint Security bis zum Ablauf des Abos in bestimmten Zeitabständen automatisch auf den Aktivierungsserver zu.

Wenn Sie das Programm mit einem unbefristeten Abo nutzen, überprüft Kaspersky Endpoint Security im Hintergrundmodus automatisch, ob auf dem Aktivierungsserver ein aktualisierter Schlüssel vorliegt. Wenn auf dem Aktivierungsserver ein Schlüssel liegt, ersetzt das Programm den vorherigen Schlüssel durch den neuen. Ein unbefristetes Abo für Kaspersky Endpoint Security wird ohne Ihr Eingreifen verlängert.

Wenn Sie das Programm im Rahmen eines befristeten Abonnements nutzen, werden Sie an dem Tag, an dem das Abonnement oder die Nachfrist für die Abo-Verlängerung nach dem Ablauf des Abonnements endet, von Kaspersky Endpoint Security darüber informiert und die Versuche zur automatischen Abo-Verlängerung werden eingestellt. Hierbei verhält sich Kaspersky Endpoint Security genau so wie nach dem Ablauf einer kommerziellen Lizenz für die Programmnutzung, d. h. das Programm funktioniert weiterhin, wird aber nicht mehr aktualisiert und kann nicht auf Kaspersky Security Network zugreifen.

Sie können das Abo auf der Provider-Webseite verlängern.

Sie können den Abo-Status im Fenster **Lizenzverwaltung** manuell aktualisieren. Dies kann erforderlich sein, wenn das Abonnement nach Ablauf der Nachfrist verlängert wurde und das Programm den Abo-Status nicht automatisch aktualisiert.

Zur Provider-Webseite wechseln

Um von der Programmoberfläche aus auf die Provider-Webseite zu gelangen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche / , die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Lizenzverwaltung** wird geöffnet.
3. Klicken Sie im Fenster **Lizenzverwaltung** auf **Abo-Provider kontaktieren**.

Methoden der Programmaktivierung

Durch die *Aktivierung* erlangt die Lizenz, die zur Nutzung der Premiumversion des Programms berechtigt, ihre Gültigkeit für den entsprechenden Zeitraum. Die Aktivierung des Programms besteht darin, dass ein Schlüssel hinzugefügt wird.

Sie können das Programm auf eine der folgenden Weisen aktivieren:

- Während der Installation des Programms mithilfe des Schnellstartassistenten Auf diese Weise können Sie einen aktiven Schlüssel hinzufügen.
- Lokal über die Programmoberfläche mithilfe des Aktivierungsassistenten Auf diese Weise können Sie sowohl einen aktiven als auch einen Reserveschlüssel hinzufügen.
- Ferngesteuert mithilfe des Programmpakets Kaspersky Security Center. Dazu wird eine Aufgabe zum Hinzufügen eines Schlüssels erstellt und anschließend gestartet. Auf diese Weise können Sie sowohl einen aktiven als auch einen Reserveschlüssel hinzufügen.
- Ferngesteuerte Verteilung von Schlüsseln und Aktivierungscodes, die sich in der Schlüsselablage auf dem Administrationsserver für Kaspersky Security Center befinden, an die Client-Computer (Informationen hierzu finden Sie im *Administratorhandbuch zu Kaspersky Security Center*). Auf diese Weise können Sie sowohl einen aktiven als auch einen Reserveschlüssel hinzufügen.

  Ein Aktivierungscode, der mit einem Abo erworben wurde, wird zuerst verteilt.

- Mithilfe der Befehlszeile.

Wenn das Programm ferngesteuert oder bei der Programminstallation im Silent-Modus mit einem Aktivierungscode aktiviert wird, kann es aufgrund der Auslastung der Kaspersky-Lab-Aktivierungsserver zu Verzögerungen kommen. Sollte eine sofortige Programmaktivierung notwendig sein, so können Sie die laufende Aktivierung abbrechen und das Programm mithilfe des Aktivierungs-Assistenten aktivieren.

Programm mithilfe des Aktivierungsassistenten aktivieren

Gehen Sie folgendermaßen vor, um Kaspersky Endpoint Security mithilfe des Aktivierungsassistenten zu aktivieren:

1. Klicken Sie auf die Schaltfläche / , die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Lizenzverwaltung** wird geöffnet.

2. Klicken Sie im Fenster **Lizenzverwaltung** auf **Programm mit neuer Lizenz aktivieren**.

   Der Aktivierungsassistent für das Programm wird gestartet.

3. Folgen Sie den Anweisungen des Aktivierungsassistenten.

Ausführliche Informationen über die Programmaktivierung finden Sie im Abschnitt über den Schnellstartassistenten des Programms.

Programm über die Befehlszeile aktivieren

Um das Programm mithilfe der Befehlszeile zu aktivieren,

geben Sie in der Befehlszeile ein: `avp.com license /add <Aktivierungscode oder Schlüsseldatei> /password=<Kennwort>`

Programm starten und beenden

Dieser Abschnitt enthält Informationen darüber, wie man den automatischen Programmstart einrichtet, das Programm manuell startet und beendet sowie die Schutzkomponenten und Kontrollkomponenten anhält und wieder fortsetzt.

Automatischen Programmstart aktivieren und deaktivieren

Unter automatischem Programmstart wird der Start von Kaspersky Endpoint Security verstanden, der ohne Ihr Zutun nach dem Hochfahren des Betriebssystems ausgeführt wird. Diese Variante des Programmstarts ist standardmäßig eingestellt.

Der erste Start des Programms Kaspersky Endpoint Security erfolgt automatisch nach der Programminstallation.

Es kann bis zu zwei Minuten dauern, bis die Antiviren-Datenbanken für Kaspersky Endpoint Security nach dem Start des Betriebssystems geladen sind. Die Dauer dieses Vorgangs ist von der Leistung (den technischen Möglichkeiten) des Computers abhängig. In diesem Zeitraum ist das Schutzniveau des Computers reduziert. Werden die Antiviren-Datenbanken beim Start von Kaspersky Endpoint Security geladen, wenn das Betriebssystem bereits hochgefahren wurde, so wird das Schutzniveau des Computers nicht beeinflusst.

Gehen Sie folgendermaßen vor, um den automatischen Start des Programms zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Programmeinstellungen** aus.
3. Führen Sie eine der folgenden Aktionen aus:
   - Wenn das Programm automatisch gestartet werden soll, aktivieren Sie das Kontrollkästchen **Kaspersky Endpoint Security für Windows beim Hochfahren des Computers starten**.
   - Um den automatischen Programmstart auszuschalten, deaktivieren Sie das Kontrollkästchen **Kaspersky Endpoint Security für Windows beim Hochfahren des Computers starten**.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Programm manuell starten und beenden

Die Kaspersky-Lab-Experten warnen davor, Kaspersky Endpoint Security zu beenden, da Ihr Computer und Ihre Daten dann bedroht sind. Bei Bedarf können Sie den Computerschutz für einen bestimmten Zeitraum anhalten, ohne das Programm zu beenden.

Kaspersky Endpoint Security muss manuell gestartet werden, wenn Sie den automatischen Programmstart deaktiviert haben.

Um das Programm manuell zu starten,

Wählen Sie im **Startmenü** den Punkt**Programme Kaspersky Endpoint Security für Windows** aus.

Gehen Sie folgendermaßen vor, um das Programm manuell zu beenden:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Wählen Sie im Kontextmenü den Punkt **Beenden**.

Schutz und Kontrolle des Computers anhalten und fortsetzen

Werden der Schutz und die Kontrolle des Computers angehalten, so werden alle Schutzkomponenten und alle Kontrollkomponenten von Kaspersky Endpoint Security vorübergehend deaktiviert.

Der Programmstatus wird mit dem Programmsymbol im Infobereich der Taskleiste visualisiert:

- Das Symbol bedeutet, dass Schutz und Kontrolle des Computers angehalten sind.
- Das Symbol bedeutet, dass Schutz und Kontrolle des Computers deaktiviert sind.

Wenn der Schutz und die Kontrolle des Computers angehalten oder fortgesetzt werden, hat dies keinen Einfluss auf die Ausführung von Untersuchungs- und Update-Aufgaben.

Wenn zum Zeitpunkt, zu dem der Schutz und die Kontrolle des Computers angehalten oder fortgesetzt werden, Netzwerkverbindungen bestehen, informiert eine Bildschirmmeldung darüber, dass diese Verbindungen getrennt werden.

Um den Schutz und die Kontrolle des Computers fortzusetzen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Wählen Sie im Kontextmenü den Punkt **Schutz und Kontrolle anhalten**.

   Das Fenster **Schutz anhalten** wird geöffnet.
3. Wählen Sie eine der folgenden Varianten:
   - **Anhalten für bestimmten Zeitraum** - Der Schutz und die Kontrolle des Computers werden nach Ablauf des Zeitraums aktiviert, der in der unten angebrachten Dropdown-Liste festgelegt wird.

- **Anhalten bis zum Neustart** - Der Schutz und die Kontrolle des Computers werden nach einem Neustart des Programms oder des Betriebssystems aktiviert. Um diese Option zu verwenden, muss der automatische Programmstart aktiviert sein.

- **Anhalten** - Der Schutz und die Kontrolle des Computers werden dann aktiviert, wenn Sie sie fortsetzen.

4. Wenn Sie beim vorherigen Schritt die Variante **Anhalten für bestimmten Zeitraum** ausgewählt haben, wählen Sie in der Dropdown-Liste den gewünschten Zeitraum aus.

Gehen Sie folgendermaßen vor, um den Schutz und die Kontrolle des Computers fortzusetzen:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.

2. Wählen Sie im Kontextmenü den Punkt **Schutz und Kontrolle fortsetzen**.

Sie können den Schutz und die Kontrolle des Computers jederzeit fortsetzen, unabhängig davon, auf welche Weise der Schutz und die Kontrolle des Computers zuvor angehalten wurden.

Teilnahme an Kaspersky Security Network

Dieser Abschnitt informiert über die Teilnahme an Kaspersky Security Network und erklärt, wie sich die Nutzung von Kaspersky Security Network aktivieren und deaktivieren lässt.

Über die Teilnahme an Kaspersky Security Network

Um Benutzercomputer effektiver zu schützen, verwendet Kaspersky Endpoint Security die von Benutzern aus aller Welt empfangenen Daten. Zum Empfangen dieser Daten dient das Netzwerk *Kaspersky Security Network*.

Kaspersky Security Network (KSN) ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Lab-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen.

Abhängig vom Standort der Infrastruktur wird zwischen Global KSN (die Infrastruktur befindet sich auf den Kaspersky-Lab-Servern) und Private KSN unterschieden.

Nach Änderung der Lizenz für die Nutzung von Local KSN müssen dem Provider die Informationen über den neuen Schlüssel zur Verfügung gestellt werden. Andernfalls ist kein Informationsaustausch mit Private KSN möglich.

Durch die Teilnahme von Benutzern an KSN kann Kaspersky Lab schnell aktuelle Informationen über Typen und Quellen von Bedrohungen erhalten und entsprechende Neutralisierungsmethoden entwickeln.

Außerdem lässt sich so die Anzahl von Fehlalarmen für die Programmkomponenten reduzieren.

Wenn der erweiterte KSN-Modus verwendet wird, übermittelt das Programm automatisch statistische Informationen an KSN. Diese Informationen werden bei der Verwendung des Programms empfangen. Zum Zweck einer zusätzlichen Untersuchung kann das Programm außerdem Dateien (oder Dateiteile) an Kaspersky Lab schicken, die von Angreifern zur Beschädigung des Computers oder der Daten verwendet werden können.

Ausführliche Informationen darüber, wie statistische Informationen, die bei der KSN-Nutzung empfangen werden, an Kaspersky Lab gesendet, gespeichert und vernichtet werden, finden Sie in der Erklärung zu Kaspersky Security Network und auf der Kaspersky-Lab-Website . Die Datei ksn_<Sprach-ID>.txt mit dem Text der Erklärung zu Kaspersky Security Network ist im Lieferumfang des Programms enthalten.

Um die Auslastung der KSN-Server zu reduzieren, kann es sein, dass Kaspersky Lab Antiviren-Datenbanken herausgibt, mit denen die Zugriffsmöglichkeit auf das Kaspersky Security Network vorübergehend deaktiviert oder teilweise eingeschränkt wird. In diesem Fall besteht der KSN-Verbindungsstatus *Aktiviert mit Einschränkungen*.

Benutzercomputer, die vom Administrationsserver für Kaspersky Security Center verwaltet werden, können zur Interaktion mit KSN den Dienst KSN Proxy verwenden.

Der Dienst KSN Proxy bietet folgende Möglichkeiten:

- Ein Benutzercomputer kann Anfragen an KSN ausführen und Informationen an KSN übertragen, auch wenn er keinen direkten Internetzugang besitzt.
- Der Dienst KSN Proxy übernimmt die Zwischenspeicherung von aufbereiteten Daten. Dadurch wird die externe Netzwerkverbindung entlastet und der Empfang angeforderter Informationen durch den Benutzercomputer beschleunigt.

Weitere Informationen über den Dienst KSN Proxy bietet das *Administratorhandbuch zu Kaspersky Security Center*.

Die Einstellungen für die Nutzung des Dienstes KSN Proxy befinden sich in den Eigenschaften der Richtlinie für *Kaspersky Security Center*.

Die Verwendung von Kaspersky Security Network ist freiwillig. Das Programm schlägt während der Erstkonfiguration des Programms vor, KSN zu verwenden. Die KSN-Nutzung kann jederzeit begonnen oder beendet werden.

Verwendung von Kaspersky Security Network aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um die Verwendung von Kaspersky Security Network zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Kaspersky Security Network** aus.

   Im rechten Fensterbereich werden die Einstellungen von Kaspersky Security Network angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Kaspersky Security Network aktivieren**, damit die Komponenten von Kaspersky Endpoint Security Informationen über die Reputation von Dateien, Webressourcen und Programmen verwenden. Diese Informationen werden aus den Datenbanken von Kaspersky Security Network empfangen.

     Um die erweiterte Verwendung von Kaspersky Security Network für die Arbeit mit Kaspersky Endpoint Security anzupassen, gehen Sie wie folgt vor:

     - Aktivieren Sie das Kontrollkästchen **Erweiterten KSN-Modus aktivieren**, damit Kaspersky Endpoint Security statistische Informationen, die auf den Arbeitsergebnissen des Programms beruhen, an den Server von Kaspersky Security Network sendet und außerdem Dateien (oder Dateiteile), mit denen Angreifer den Computer oder die Daten beschädigen können, zum Zweck einer zusätzlichen Untersuchung an Kaspersky Lab schickt.

     - Deaktivieren Sie das Kontrollkästchen**Erweiterten KSN-Modus aktivieren**, damit Kaspersky Endpoint Security die Grundfunktionen von Kaspersky Security Network verwendet.

   - Deaktivieren Sie das Kontrollkästchen **Kaspersky Security Network aktivieren**, um die Verwendung von Kaspersky Security Network zu deaktivieren.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Über die Datenbereitstellung bei der Verwendung von Kaspersky Security Network

Wenn Sie die Erklärung zu Kaspersky Security Network akzeptieren, stimmen Sie der automatischen Übertragung folgender Informationen zu:

- Ist das Kontrollkästchen **Kaspersky Security Network aktivieren** aktiviert und das Kontrollkästchen **Erweiterten KSN-Modus aktivieren** deaktiviert, so werden die folgenden Informationen übertragen:

  - Webadresse der Webseite, von welcher zu der untersuchten Webadresse gewechselt wurde
  - Webadresse, für welche die Reputation abgefragt wird
  - Version des verwendeten Protokolls für die Verbindung mit den Kaspersky-Lab-Diensten
  - ID der Antiviren-Datenbanken
  - ID der Untersuchungsaufgabe, mit welcher die Bedrohung gefunden wurde
  - ID des Subsystems, welches die Anfrage initiiert hat
  - ID des Verbindungsprotokolls und Nummer des verwendeten Ports
  - IDs der installierten Updates

- Name und ID der gefundenen Bedrohung gemäß der Kaspersky-Lab-Klassifikation
- öffentlicher Zertifikatschlüssel
- Typ und vollständige Programmversion von Kaspersky Endpoint Security
- Hash (SHA256) des Zertifikats, mit welchem das zu untersuchende Objekt signiert ist
- Hash der zu untersuchenden Datei (MD5, SHA2-256 und SHA1) und der Dateivorlagen (MD5)

- Sind die Kontrollkästchen **Kaspersky Security Network aktivieren** und **Erweiterten KSN-Modus aktivieren** aktiviert, so werden zusätzlich zu den oben genannten Informationen auch die folgenden Informationen übertragen:
  - Vertrauenswürdige ausführbare und nicht ausführbare Dateien oder deren Teile, die zum Zweck der Vermeidung von Fehlalarmen übertragen werden
  - Es werden folgende Informationen übertragen, die aus Berichten über die Aktivität von Programmen stammen:
    - Webadressen und IP-Adressen, auf welche das Programm zugegriffen hat
    - Webadressen und IP-Adressen, von welchen die zu startende Datei empfangen wurde
    - Datum und Uhrzeit für den Beginn und den Ablauf des Zertifikats, falls die gesendete Datei eine digitale Signatur besitzt, Datum und Uhrzeit der Ausstellung, Name des Zertifikatausstellers, Informationen über den Zertifikatinhaber, Fingerabdruck und öffentlicher Schlüssel des Zertifikats und entsprechende Berechnungsalgorithmen, Seriennummer des Zertifikats
    - Kopfzeilen der Prozessfenster
    - ID der Antiviren-Datenbanken, Name der gefundenen Bedrohung gemäß der Klassifikation des Rechteinhabers
    - Namen und Pfade der Dateien, auf welche der Prozess Zugriff erhalten hat
    - Namen und Werte der Registrierungsschlüssel, auf welche der Prozess Zugriff erhalten hat
    - Name des Benutzerkontos, von welchem der Prozess gestartet wurde
    - Name, Größe und Version der zu sendenden Datei, Beschreibung und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, Format-ID, Herstellername, Name des Produkts, zu welchem die Datei gehört, vollständiger Pfad der Datei auf dem Computer und Code für die Pfadvorlage, Datum und Uhrzeit der Erstellung und Modifikation der Datei
    - Informationen über die in der SOFTWARE installierte Lizenz, ID, Typ und Ablaufdatum der Lizenz
    - Prüfsummen (MD5, SHA2-256, SHA1) für den Namen des Computers, auf welchem der Prozess gestartet wurde
    - lokale Zeit des Computers zum Zeitpunkt der Datenbereitstellung

- Es werden folgende sonstige Informationen übertragen:
  - Webadressen und IP-Adressen der angeforderten Webressource, Informationen über die Datei und den Web-Client, welcher auf die Webressource zugegriffen hat, Name, Größe, Prüfsummen (MD5, SHA2-256, SHA1) der Datei, vollständiger Pfad und Code der Pfadvorlage für die Datei, Ergebnis der Untersuchung ihrer digitalen Signatur und ihr Status in KSN
  - Falls ein potentiell schädliches Objekt gefunden wurde, werden Informationen über die Daten im Arbeitsspeicher des Prozesses bereitgestellt: Hierarchie-Elemente von Systemobjekten (ObjectManager), Daten zum Arbeitsspeicher (UEFI BIOS), Namen und Werte von Registrierungsschlüsseln
  - Webseiten und E-Mail-Nachrichten, die verdächtige und schädliche Objekte enthalten
  - Version der Update-Komponente der SOFTWARE, Anzahl der Abstürze der Update-Komponente der SOFTWARE bei der Ausführung von Update-Aufgaben im Rahmen der Komponentenausführung, ID des Typs der Update-Aufgabe, Anzahl der Fehler bei den Update-Aufgaben der Update-Komponente der SOFTWARE
  - Daten über Fehler, welche bei der Ausführung einer SOFTWARE-Komponente aufgetreten sind: Status-ID der SOFTWARE, Typ und Code des Fehlers, Eintrittszeitpunkt des Fehlers, IDs der Komponente, des Moduls und des Produktprozesses, in welchem der Fehler aufgetreten ist, ID der Aufgabe oder Kategorie, bei deren Ausführung ein Fehler aufgetreten ist, Überwachungsdaten der Treiber, welche von der SOFTWARE verwendet werden (Fehlercode, Modulname, Name der Quelldatei und Zeile, in welcher der Fehler aufgetreten ist), ID für die Methode zur Fehlerermittlung bei der Ausführung der SOFTWARE, Name des Prozesses, welcher das Abfangen oder den Austausch des Datenverkehrs initiiert hat, welcher zu einem Fehler bei der Ausführung der SOFTWARE geführt hat
  - Daten zum System-Dump (BSOD): Merkmal für das Auftreten des BSOD auf dem Computer, Name des Treibers, welcher den BSOD hervorgerufen hat, Adresse und Speicherstapel im Treiber, Merkmal für die Dauer der Sitzung des Betriebssystems bis zum Auftreten des BSOD, Speicherstapel des Treiberabsturzes, Typ des gespeicherten Arbeitsspeicher-Dumps, Merkmal für die Tatsache, dass die Sitzung des Betriebssystems bis zum BSOD länger als 10 Minuten gedauert hat, einmalige Dump-ID, Zeitpunkt (Datum und Uhrzeit), zu welchem der BSOD aufgetreten ist
  - Daten zu den Updates für die Antiviren-Datenbanken und SOFTWARE-Komponenten: Namen, Datum und Uhrzeit von Indexdateien, die aufgrund des letzten Updates heruntergeladen wurden und die beim laufenden Update heruntergeladen werden sollen, Zeitpunkt (Datum und Uhrzeit) des Abschlusses des letzten Updates, Namen der Dateien von aktualisierten Kategorien und deren Prüfsummen (MD5, SHA2-256, SHA1)
  - ID der Untersuchungsaufgabe, mit welcher die Bedrohung gefunden wurde
  - Informationen für die Authentizitätsprüfung der Zertifikate, mit welchen die Dateien signiert sind: Fingerabdruck des Zertifikats, Algorithmus zur Berechnung der Prüfsumme, öffentlicher Schlüssel und Seriennummer des Zertifikats, Name des Zertifikatausstellers, Ergebnis der Zertifikatuntersuchung und ID der Zertifikatdatenbank
  - Informationen zur Version des auf dem Computer installierten Betriebssystems und der installierten Service Packs, Bit-Version, Revision und Einstellungen für den Funktionsmodus des Betriebssystems, Version und Prüfsummen (MD5, SHA2-256, SHA1) der Kerneldatei des Betriebssystems

- Informationen über die Ausführung eines Rollbacks der Aktionen von Schadsoftware: Daten über die Datei, deren Aktivität rückgängig gemacht wurde (Name, vollständiger Pfad, Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Datei), Daten über erfolgreiche und erfolglose Aktionen zur Löschung, Umbenennung und zum Kopieren von Dateien und zur Wiederherstellung von Registrierungswerten (Namen und Werte der Registrierungsschlüssel), Informationen über Systemdateien, welche von der Schadsoftware verändert wurden, vor und nach der Ausführung des Rollbacks

- Informationen über die Ausführung einer Emulation der ausführbaren Datei: Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, Version der Emulationskomponente, Emulationstiefe, Vektor der Merkmale für logische Blöcke und Funktionen innerhalb logischer Blöcke, welche im Verlauf der Emulation erhalten wurden, Daten aus der Struktur der PE-Kopfzeile der ausführbaren Datei

- Informationen über das Datum der Installation und der Aktivierung der SOFTWARE auf dem Computer: Typ und Gültigkeitsdauer der installierten Lizenz, ID des Partners, bei welchem die Lizenz gekauft wurde, Seriennummer der Lizenz, Typ der SOFTWARE-Installation auf dem Computer (Erstinstallation, Upgrade usw.), Merkmal für den Erfolg der Installation oder Nummer des Installationsfehlers, einmalige ID für die SOFTWARE-Installation auf dem Computer, Typ und ID der Anwendung, mit welcher das Update ausgeführt wird, ID der Update-Aufgabe

- Informationen über geladene SOFTWARE-Module: Name, Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Moduldatei, vollständiger Pfad und Code der Pfadvorlage für die Datei, Parameter der digitalen Signatur der Moduldatei, Zeitpunkt (Datum und Uhrzeit) der Erstellung der Signatur, Name des Subjekts und Organisation, welche die Moduldatei signiert hat, ID des Prozesses, in welchen das Modul geladen wurde, Name des Modulherstellers, Ordnungsnummer des Moduls in der Ladeabfolge

- Informationen über die Dateien, die vom Benutzer heruntergeladen wurden: Webadressen und IP-Adressen, von welchen der Download erfolgt ist, und Download-Webseiten, ID des Download-Protokolls und Nummer des Verbindungsports, Merkmal für die Schädlichkeit von Adressen, Attribute, Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, Informationen zum Prozess, welcher die Datei heruntergeladen hat (Prüfsummen (MD5, SHA2-256, SHA1), Zeitpunkt (Datum und Uhrzeit) der Erstellung und Verlinkung, Merkmal für das Vorhandensein im Autostart, Attribute, Namen von Packprogrammen, Informationen zur Signatur, Merkmal der ausführbaren Datei, Format-ID, Entropie), Dateiname, Dateipfad auf dem Computer, digitale Signatur der Datei und Informationen über die Ausstellung der Signatur, Webadresse, in welcher der Fund erfolgt ist, Nummer des Skripts auf der Webseite, die als verdächtig oder schädlich betrachtet wird, Informationen über ausgeführte http-Anfragen und damit verbundene Antworten

- Informationen über gestartete Programme und deren Module: Daten über gestartete Prozesse im System (Prozess-ID im System (PID), Prozessname, Daten über das Benutzerkonto, von dem der Prozess gestartet wurde, Programm und Befehl, welcher den Prozess gestartet hat, Merkmal für die Vertrauenswürdigkeit des Programms oder des Prozesses, vollständiger Pfad der Prozessdateien und Befehlszeile für den Start, Integritätsniveau des Prozesses, Beschreibung des Produkts, zu welchem der Prozess gehört (Name des Produkts und Daten zum Herausgeber), sowie Daten über verwendete digitale Zertifikate und Informationen, die für ihre Authentifizierung erforderlich sind, oder Daten über das Fehlen einer digitalen Signatur für die Datei), sowie Informationen über die Module, welche in Prozesse geladen wurden (Name, Größe, Typ, Erstellungsdatum, Attribute, Prüfsummen (MD5, SHA2-256, SHA1), Pfad), Informationen zur Kopfzeile für PE-Dateien, Name des Packprogramms (falls die Datei gepackt ist)

- Informationen über die Zusammensetzung aller installierten Updates sowie über die Zusammensetzung der zuletzt installierten und/oder gelöschten Updates, Typ des Ereignisses, aufgrund dessen Informationen über Updates gesendet wurden, Zeitraum, welcher seit der Installation des letzten Updates vergangen ist, Informationen über die Antiviren-Datenbanken, die zum Zeitpunkt der Datenbereitstellung geladen waren

- Informationen über den letzten fehlgeschlagenen Neustart des Betriebssystems: Anzahl der fehlgeschlagenen Neustarts seit der Installation des Betriebssystems, Daten zum System-Dump (Code und Parameter des Fehlers, Name, Version und Prüfsumme (CRC32) des Moduls, welches den Fehler bei der Arbeit des Betriebssystem hervorgerufen hat, Fehleradresse als Offset im Modul, Prüfsummen (MD5, SHA2-256, SHA1) des System-Dumps)

- Informationen über den Rechteinhaber der SOFTWARE: vollständige Version, Typ, Sprachversion und Funktionsstatus der verwendeten SOFTWARE, Versionen und Funktionsstatus der installierten SOFTWARE-Komponenten, sowie Wert des TARGET-Filters, Version des verwendeten Protokolls für die Version mit den Diensten des Rechteinhabers

- Informationen über untersuchte Objekte: zugewiesene Sicherheitsgruppe, in welche und/oder aus welcher die Datei verschoben wurde, Grund, aus welchem die Datei in diese Kategorie verschoben wurde, ID der Kategorie, Informationen über die Quelle der Kategorien und Version der Datenbank der Kategorien, Merkmal für das Vorhandensein eines vertrauenswürdigen Zertifikats der Datei, Name des Dateiherstellers, Dateiversion, Name und Version der Anwendung, zu welcher die Datei gehört

- Informationen über untersuchte Dateien und Webadressen: Prüfsummen der untersuchten Datei (MD5, SHA2-256, SHA1) und der Dateimuster (MD5), Größe des Musters, Typ der gefundenen Bedrohung und Bedrohungsname gemäß der Klassifikation des Rechteinhabers, ID der Antiviren-Datenbanken, Webadresse, für welche die Reputation abgefragt wird, sowie Webadresse der Webseite, von welcher zu der untersuchten Webadresse gewechselt wurde, ID des Verbindungsprotokolls und Nummer des verwendeten Ports

- Informationen zum Prozess, welcher einen Angriff auf den Selbstschutz der SOFTWARE ausgeführt hat: Name, Größe, Prüfsummen (MD5, SHA2-256, SHA1), vollständiger Pfad und Code der Pfadvorlage der Prozessdatei, Zeitpunkt (Datum und Uhrzeit) der Erstellung und Verlinkung der Prozessdatei, Merkmal der ausführbaren Datei, Attribute der Prozessdatei, Informationen zum Zertifikat, mit welchem die Prozessdatei signiert ist, Code des Benutzerkontos, in deren Namen der Prozess gestartet wurde, ID der Vorgänge, welche für den Zugriff auf den Prozess ausgeführt wurden, Typ der Ressourcen, von welchen der Vorgang ausgeführt wurde (Prozess, Datei, Registrierungsobjekt, Suche des Fensters mithilfe der Funktion FindWindow), Name der Ressource, mit welcher der Vorgang ausgeführt wird, Merkmal für die erfolgreiche Ausführung des Vorgangs, Status der Prozessdatei und ihr Status in KSN

- Informationen über die Arbeit der Schutzkomponenten: vollständige Version der Komponenten, Code des Ereignisses, welches zum Überlauf der Ereigniswarteschlange geführt hat, und Anzahl solcher Ereignisse, Gesamtzahl der Überläufe der Ereigniswarteschlange, Informationen über die initiierende Prozessdatei für das Ereignis (Name und Pfad der Datei auf dem Computer, Code der Pfadvorlage, Prüfsummen (MD5, SHA2-256, SHA1) des Prozesses, welcher mit der Datei verbunden ist, Dateiversion), ID für den ausgeführten Abfangvorgang des Ereignisses, vollständige Version des Abfangfilters, ID des Typs des abgefangenen Ereignisses, Größe der Ereigniswarteschlange und Anzahl der Ereignisse zwischen dem ersten Ereignis in der Warteschlange und dem aktuellen Ereignis, Anzahl der überfälligen Ereignisse in der Warteschlange, Informationen über den initiierenden Prozess des aktuellen Ereignisses (Name der Prozessdatei und Pfad auf dem

Computer, Code der Pfadvorlage, Prüfsummen (MD5, SHA2-256, SHA1) des Prozesses), Dauer der Ereignisverarbeitung, maximal zulässige Verarbeitungsdauer für Ereignisse, Wahrscheinlichkeitswert für das Senden von Daten

- Informationen über die Arbeit der SOFTWARE auf dem Computer: Daten über die Prozessnutzung (CPU), Daten über die Nutzung des Arbeitsspeichers (Private Bytes, Non-Paged Pool, Paged Pool), Anzahl der aktiven Ströme im SOFTWARE-Prozess und der Ströme im Wartezustand, Arbeitsdauer der SOFTWARE bis zum Auftreten des Fehlers

- Informationen zu den Ergebnissen der Kategorisierung der angeforderten Webressourcen, welche folgende Angaben enthält: untersuchte Webadresse und IP-Adresse des Hosts, Version der SOFTWARE-Komponente, welche die Kategorisierung ausgeführt hat, Kategorisierungsmethode und Auswahl der Kategorien, welche für diese Webressource ermittelt wurden

- Informationen über Netzwerkangriffe: IP-Adressen des angreifenden Computers (IPv4 und IPv6), Portnummer des Computers, auf welchen der Netzwerkangriff gerichtet war, ID des Protokolls des IP-Pakets, in welchem der Angriff registriert wurde, Angriffsziel (Name der Organisation, Website), Flag für die Reaktion auf den Angriff, gewichtetes Angriffsniveau, Wert für das Niveau der Vertrauenswürdigkeit

- Informationen über Netzwerkverbindungen: Version und Prüfsummen (MD5, SHA2-256, SHA1) der Prozessdatei, des geöffneten Ports, Pfad und digitale Signatur der Prozessdatei, lokale und Remote-IP-Adresse, Nummern des lokalen und des Remote-Verbindungsports, Verbindungszustand, Dauer, für welche der Port geöffnet war

- Informationen über Ereignisse in Systemprotokollen: Ereigniszeitpunkt, Name des Protokolls, in welchem das Ereignis gefunden wurde, Typ und Kategorie des Ereignisses, Name und Beschreibung der Ereignisquelle

- Informationen über den Zustand des Antiviren-Schutzes des Computers: Version und Zeitpunkt (Datum und Uhrzeit) der Veröffentlichung der verwendeten Antiviren-Datenbanken, statistische Daten über Updates und Verbindungen mit den Diensten des Rechteinhabers, ID der Aufgabe und ID der SOFTWARE-Komponente, welche die Untersuchung ausgeführt hat

- Informationen über Dritthersteller-Anwendungen, welche einen Fehler verursacht haben: Name, Version und Sprachversion, Fehlercode und Informationen über den Fehler aus dem Systemprotokoll der Anwendungen, Adresse und Speicherstapel für das Auftreten des Fehlers einer Dritthersteller-Anwendung, Merkmal für das Auftreten des Fehlers in einer SOFTWARE-Komponente, Arbeitsdauer der Dritthersteller-Anwendung bis zum Auftreten des Fehlers, Prüfsummen (MD5, SHA2-256, SHA1) des Prozessmusters der Anwendung, in welcher der Fehler aufgetreten ist, Pfad dieses Prozessmusters der Anwendung und Code der Pfadvorlage, Informationen aus dem Systemprotokoll des Betriebssystems mit einer Beschreibung des Fehlers, welcher mit der Anwendung verbunden war, Informationen über das Anwendungsmodul, in welchem der Fehler aufgetreten ist (Fehler-ID, Fehleradresse als Offset im Modul, Name und Version des Moduls, ID für den Absturz der Anwendung in einem Plug-in des Rechteinhabers und Speicherstapel für diesen Absturz, Arbeitsdauer der Anwendung bis zum Absturz)

- Informationen über die Abstürze der SOFTWARE: Zeitpunkt (Datum und Uhrzeit) der Dump-Erstellung, Typ und Name des Prozesses, welcher mit dem Prozess zusammenhängt, Version und Zeitpunkt (Datum und Uhrzeit), zu welchem eine Statistik mit dem Dump gesendet wurde, Typ des Ereignisses, welches den Absturz der SOFTWARE verursacht hat

(unerwarteter Stromausfall, Absturz einer Dritthersteller-Anwendung, Verarbeitungsfehler bei einem Abfangvorgang), Zeitpunkt (Datum und Uhrzeit) des unerwarteten Stromausfalls

- Informationen über Angriffe, welche mit dem Spoofing von Netzwerkressourcen verbunden waren, DNS- und IP-Adressen (IPv4 oder IPv6) der besuchten Websites

- Informationen über verwendete digitale Zertifikate, welche für ihre Authentifizierung erforderlich sind: Prüfsummen (SHA256) des Zertifikats, mit welchem das Untersuchungsobjekt signiert ist, und des öffentlichen Zertifikatschlüssels

- Informationen über gefundene Schwachstellen: ID der Schwachstelle in der Datenbank für Schwachstellen, Gefahrenklasse der Schwachstelle und Fundstatus

- Informationen über die Hardware, welche auf dem Computer installiert ist: Typ, Name, Modell, Firmware-Version, Merkmale von integrierten und verbundenen Geräten, einmalige ID des Computers, auf welchem die SOFTWARE installiert ist

- Informationen über die Software, welche auf dem Computer installiert ist: Name und Hersteller der Software, verwendete Registrierungsschlüssel und deren Werte, Informationen über die Dateien der Komponenten der installierten Software (Prüfsummen (MD5, SHA2-256, SHA1), Name, Pfad der Datei auf dem Computer, Größe, Version und digitale Signatur), Informationen über Kernel-Objekte, Treiber, Dienste, Erweiterungen für Microsoft Internet Explorer, Erweiterungen des Drucksystems, Erweiterungen für Windows Explorer, Elemente für Active Setup, Systemsteuerungs-Applets, Einträge der hosts-Datei und der Systemregistrierung, Versionen der Browser und Mail-Clients

- Informationen über alle potentiell schädlichen Objekte und Aktionen: Name des erkannten Objekts und vollständiger Pfad des Objekts auf dem Computer, Prüfsummen der verarbeiteten Objekte (MD5, SHA2-256, SHA1), Zeitpunkt (Datum und Uhrzeit) des Fundes, Namen, Größe und Pfade der infizierten Dateien, Code der Pfadvorlage, Merkmal, ob das Objekt ein Container ist, Name des Packprogramms (falls die Datei gepackt ist), Code des Dateityps, ID des Dateiformats, Liste über die Aktivitäten der Schadsoftware und der entsprechenden Entscheidungen der SOFTWARE und des Benutzers, ID der Antiviren-Datenbanken, auf deren Basis die Entscheidung der SOFTWARE getroffen wurde, Name der gefundenen Bedrohung gemäß der Klassifikation des Rechteinhabers, Gefährlichkeit, Status und Erkennungsmethode, Grund der Aufnahme in den analysierten Kontext und Ordnungsnummer der Datei im Kontext, Prüfsummen (MD5, SHA2-256, SHA1), Name und Attribute der ausführbaren Datei der Anwendung, über welche die infizierte Nachricht oder der Link eingedrungen ist, anonymisierte IP-Adressen (IPv4 und IPv6) des Hosts des blockierten Objekts, Datei-Entropie, Merkmal für das Vorhandensein der Datei im Autostart, Zeitpunkt (Datum und Uhrzeit) des ersten Fundes der Datei im System, Anzahl der Dateistarts seit dem letzten Senden einer Statistik, Informationen über den Namen, die Prüfsummen (MD5, SHA2-256, SHA1) und die Größe des Mail-Clients, über welchen das schädliche Objekt empfangen wurde, ID der SOFTWARE-Aufgabe, welche die Untersuchung ausgeführt hat, Merkmal für die Überprüfung der Reputation oder der Signatur der Datei, Ergebnis der Dateiverarbeitung, Prüfsumme (MD5) des Musters, welches für das Objekt erstellt wurde, und Größe des Musters (in Bytes), technische Eigenschaften der eingesetzten Erkennungstechnologien

- Ausführbare und nicht ausführbare Dateien (vollständig oder teilweise)

- Anzahl der SOFTWARE-Dumps und der System-Dumps (BSOD) ab dem Zeitpunkt der SOFTWARE-Installation und ab dem Zeitpunkt des letzten Updates, ID und Version des SOFTWARE-Moduls, in welchem die Störung aufgetreten ist, Speicherstapel im

Produktprozess und Informationen über die Antiviren-Datenbanken zum Zeitpunkt der Störung

- Beschreibung der Klassen und Exemplarklassen des WMI-Speichers
- Berichte über die Aktivitäten von Anwendungen
- Datenpakete des Netzwerkverkehrs
- Sektoren, die am Ladeprozess des Betriebssystems beteiligt sind
- Verwaltungsinformationen über die Arbeit der SOFTWARE: Compiler-Version, Merkmal der potentiellen Schädlichkeit des untersuchten Objekts, Set-Version der übertragenen Statistik, Informationen über das Vorhandensein und die Gültigkeit der Statistikdaten, ID der Erstellungsbedingung für die übertragene Statistik, Merkmal für die Arbeit der SOFTWARE im interaktiven Modus
- Abschnitte aus dem Arbeitsspeicher des Computers

Cloud-Modus für die Schutzkomponenten aktivieren und deaktivieren

Bei der Verwendung von Kaspersky Private Security Network ist die Funktionalität des Cloud-Modus ab Version 3.0 von Kaspersky Private Security Network verfügbar.

Um den Cloud-Modus für die Schutzkomponenten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Kaspersky Security Network** aus.

   Im rechten Fensterbereich werden die Einstellungen von Kaspersky Security Network angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Cloud-Modus für die Schutzkomponenten aktivieren**.

     Ist das Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security eine eingeschränkte Version der Antiviren-Datenbanken. Dadurch wird die Auslastung der Betriebssystemressourcen verringert.

     Nachdem das Kontrollkästchen aktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update eine eingeschränkte Version der Antiviren-Datenbanken herunter.

     Falls die eingeschränkte Version der Antiviren-Datenbanken nicht verfügbar ist, schaltet Kaspersky Endpoint Security automatisch zur Verwendung der vollständigen Version der

Antiviren-Datenbanken um.

- Deaktivieren Sie das Kontrollkästchen **Cloud-Modus für die Schutzkomponenten aktivieren**.

  Ist das Kontrollkästchen deaktiviert, so verwendet Kaspersky Endpoint Security die vollständige Version der Antiviren-Datenbanken.

  Nachdem das Kontrollkästchen deaktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update die vollständige Version der Antiviren-Datenbanken herunter.

Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Kaspersky Security Network aktivieren** aktiviert ist.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Verbindung zum Kaspersky Security Network prüfen

Gehen Sie folgendermaßen vor, um zu prüfen, ob eine Verbindung zum Kaspersky Security Network besteht:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im oberen Fensterbereich auf den Block **Technologien zum Erkennen von Bedrohungen**.

   Das Fenster **Technologien zum Erkennen von Bedrohungen** wird geöffnet.

   Im unteren Bereich des Fensters **Technologien zum Erkennen von Bedrohungen** werden folgende Informationen über die Arbeit von Kaspersky Security Network angezeigt:

   - Unter der Zeile **KASPERSKY SECURITY NETWORK (KSN)** wird eine der folgenden Statusvarianten für die Verbindung von Kaspersky Endpoint Security mit Kaspersky Security Network angezeigt:

     - *Aktiviert. Verfügbar.*

       Dieser Status bedeutet, dass Kaspersky Security Network von Kaspersky Endpoint Security verwendet wird und die KSN-Server verfügbar sind.

     - *Aktiviert. Nicht verfügbar.*

       Dieser Status bedeutet, dass Kaspersky Security Network von Kaspersky Endpoint Security verwendet wird, die KSN-Server aber nicht verfügbar sind.

     - *Deaktiviert.*

       Dieser Status bedeutet, dass Kaspersky Security Network von Kaspersky Endpoint Security nicht verwendet wird.

   - In den Zeilen **Sichere Objekte**, **Gefährliche Objekte**, **Neutralisierte Bedrohungen pro Tag** wird eine globale Statistik für die Infrastruktur der Cloud-Dienste von Kaspersky Security Network angezeigt.

   - In der Zeile **Letzte Synchronisierung** wird der Zeitpunkt (Datum und Uhrzeit) der letzten Synchronisierung von Kaspersky Endpoint Security mit den KSN-Servern angezeigt.

Das Programm ruft die statistischen Daten zur KSN-Verwendung ab, wenn das Fenster **Technologien zum Erkennen von Bedrohungen** geöffnet wird. Die globale Statistik über die Infrastruktur der Cloud-Dienste von Kaspersky Security Network und die Zeile **Letzte Synchronisierung** werden nicht in Echtzeit aktualisiert.

Wenn seit der letzten Synchronisierung mit den KSN-Servern mehr als 15 Minuten vergangen sind oder der Status *Unbekannt* angezeigt wird, nimmt der Status für die Verbindung von Kaspersky Endpoint Security mit Kaspersky Security Network den Wert *Aktiviert an. Nicht verfügbar.*

Eine fehlende Verbindung mit den Servern von Kaspersky Security Network kann folgende Gründe haben:

- Ihr Computer ist nicht mit dem Internet verbunden.
- Das Programm ist nicht aktiviert.
- Die Lizenz ist abgelaufen.
- Es bestehen Probleme mit dem Schlüssel (z. B. wenn der Schlüssel auf die schwarze Schlüsselliste gesetzt wurde).

Falls mit den Servern von Kaspersky Security Network keine Verbindung mehr wiederherstellt werden kann, sollten Sie sich an den Technischen Support oder an Ihren Dienstleister wenden.

Reputation einer Datei in Kaspersky Security Network überprüfen

Der KSN-Dienst erlaubt es, Informationen über Programme zu erhalten, die in den Reputations-Datenbanken von Kaspersky Lab verzeichnet sind. Dadurch wird erlaubt, unternehmensweite Richtlinien für den Programmstart flexibel zu verwalten. So lässt sich der Start von Adware und legalen Programmen verhindern, mit denen Angreifer den Computer oder die Benutzerdaten beschädigen können.

Um die Reputation einer Datei bei Kaspersky Security Network zu überprüfen, gehen Sie wie folgt vor:

1. Öffnen Sie durch Rechtsklick das Kontextmenü der Datei, deren Reputation Sie überprüfen möchten.
2. Wählen Sie den Punkt **Reputation in KSN überprüfen**.

Dieser Punkt ist verfügbar, wenn Sie die Bedingungen der "Erklärung zu Kaspersky Security Network" akzeptiert haben.

Das Fenster **<Dateiname> - Reputation in KSN** wird geöffnet. Im Fenster **<Dateiname> - Reputation in KSN** werden folgende Informationen über die überprüfte Datei angezeigt:

- **Pfad**. Pfad, unter dem die Datei auf dem Laufwerk gespeichert ist
- **Version**. Programmversion (Diese Information wird nur für ausführbare Dateien angezeigt.)
- **Digitale Signatur**. Vorhandensein einer digitalen Signatur für die Datei
- **Signiert**. Datum, an dem das Zertifikat mit einer digitalen Signatur versehen wurde
- **Erstellt**. Erstellungsdatum der Datei
- **Geändert**. Datum der letzten Änderung
- **Größe**. Speicherplatz, den die Datei auf dem Laufwerk einnimmt
- Informationen darüber, wie viele Benutzer der Datei vertrauen oder die Datei blockieren

Zusätzlicher Schutz durch Verwendung von Kaspersky Security Network

Kaspersky Lab bietet ein zusätzliches Sicherheitsniveau durch Verwendung von Kaspersky Security Network. Ziel dieser Schutzmethode ist der effektive Kampf gegen komplizierte, ständig auftauchende Bedrohungen, sowie Zero-Day-Bedrohungen. Die in Kaspersky Endpoint Security integrierten Cloud-Technologien und das Fachwissen der Virenanalysten von Kaspersky Lab ermöglichen einen hochwertigen Schutz auch vor kompliziertesten Online-Bedrohungen.

Weitere Informationen über den zusätzlichen Schutz von Kaspersky Endpoint Security finden Sie auf der Kaspersky-Lab-Website.

Verhaltensanalyse für Programme

Dieser Abschnitt informiert über die Verhaltensanalyse für Programme und erklärt die Einstellungen der Komponente.

Über die Verhaltensanalyse für Programme

Die Komponente Verhaltensanalyse für Programme empfängt Daten über die Aktionen der Programme auf Ihrem Computer und versorgt andere Schutzkomponenten mit diesen Informationen, um deren Effektivität zu erhöhen.

Die Komponente Verhaltensanalyse für Programme verwendet Vorlagen für gefährliches Programmverhalten (im Weiteren "Vorlagen für gefährliches Verhalten" genannt). Die Vorlagen enthalten Abfolgen von Programmaktionen, die von Kaspersky Endpoint Security als gefährlich eingestuft werden. Stimmt die Aktivität eines Programms mit einer der Aktivitäten aus den Vorlagen für gefährliches Verhalten überein, so führt Kaspersky Endpoint Security die ausgewählte Reaktion aus. Diese Funktionalität von Kaspersky Endpoint Security, die auf Vorlagen für gefährliches Verhalten beruht, bietet einen proaktiven Computerschutz.

Verhaltensanalyse für Programme aktivieren und deaktivieren

Die Verhaltensanalyse für Programme ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie die Verhaltensanalyse für Programme deaktivieren.

Es wird davor gewarnt, die Verhaltensanalyse für Programme ohne triftigen Grund zu deaktivieren, da dies die Effektivität der Schutzkomponenten beeinträchtigt. Die Schutzkomponenten können die von der Verhaltensanalyse für Programme empfangenen Daten abfragen, um Bedrohungen zu erkennen.

Um die Verhaltensanalyse für Programme zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Verhaltensanalyse**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Verhaltensanalyse für Programme angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Kaspersky Endpoint Security die Aktivität der Programme im Betriebssystem mithilfe von Vorlagen für gefährliches Verhalten analysieren soll, aktivieren Sie das Kontrollkästchen **Verhaltensanalyse aktivieren**.
   - Damit Kaspersky Endpoint Security die Aktivität der Programme im Betriebssystem nicht mithilfe von Vorlagen für gefährliches Verhalten analysiert, deaktivieren Sie das Kontrollkästchen **Verhaltensanalyse aktivieren**.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktion beim Fund schädlicher Programmaktivität wählen

Beim Fund einer schädlichen Programmaktivität erstellt Kaspersky Endpoint Security immer einen Berichtseintrag, der Informationen über die gefundene Programmaktivität enthält.

Um eine Aktion für den Fund schädlicher Programmaktivität zu wählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Verhaltensanalyse**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Verhaltensanalyse für Programme angezeigt.
3. Wählen Sie in der Dropdown-Liste **Wenn schädliche Programmaktivität erkannt wird** die erforderliche Aktion aus:

- Datei löschen.

  Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so löscht Kaspersky Endpoint Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an.

- Programm beenden.

  Wenn dieses Element gewählt wird, beendet Kaspersky Endpoint Security beim Auffinden einer schädlichen Programmaktivität die betreffende Anwendung.

- Informieren

  Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so fügt Kaspersky Endpoint Security Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern anpassen

Die Komponente gewährleistet die Vorgangsnachverfolgung nur für jene Dateien, die sich auf Massenspeichergeräten mit NTFS-Dateisystem befinden und die nicht mit einem EFS-System verschlüsselt wurden.

Die Funktion für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern gewährleistet eine Nachverfolgung der folgenden Vorgänge, die von einem Remote-Computer ausgeführt werden können:

- Löschung einer Datei
- Änderung des Inhalts einer Datei
- Änderung der Dateigröße
- Verschieben einer Datei

Um den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern anzupassen, können Sie folgende Aktionen ausführen:

- Aktion auswählen, die beim Erkennen der externen Verschlüsselung gemeinsamer Ordner ausgeführt werden soll
- Adressen von Ausnahmen für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern anpassen

Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern aktivieren und deaktivieren

Der Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ist standardmäßig deaktiviert.

Die Funktionalität für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ist ach der Installation von Kaspersky Endpoint Security bis zum Neustart des Computers beschränkt.

Um den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Verhaltensanalyse**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Verhaltensanalyse für Programme angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Kaspersky Endpoint Security die Vorgänge, die von einem Remote-Computer ausgeführt werden, nachverfolgen soll, aktivieren Sie im Block **Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern** das Kontrollkästchen **Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern aktivieren**:
   - Wenn Kaspersky Endpoint Security die Vorgänge, die von einem Remote-Computer ausgeführt werden, nicht nachverfolgen soll, deaktivieren Sie im Block **Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern** das Kontrollkästchen **Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern aktivieren**.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktion auswählen, die beim Erkennen der externen Verschlüsselung gemeinsamer Ordner ausgeführt werden soll

Wenn ein Versuch zur Änderung von Dateien in gemeinsamen Ordnern erkannt wird, erstellt Kaspersky Endpoint Security einen Berichtseintrag, der Informationen über den erkannten Versuch zur Änderung von Dateien in gemeinsamen Ordnern enthält.

Um die Aktion auszuwählen, die beim Erkennen der externen Verschlüsselung gemeinsamer Ordner ausgeführt werden soll, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Verhaltensanalyse**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Verhaltensanalyse für Programme angezeigt.
3. Wählen Sie im Block **Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern** in der Dropdown-Liste **Wenn eine externe Verschlüsselung gemeinsamer Ordner erkannt wird** die erforderliche Aktion aus:

- Verbindung blockieren.

  Wenn dieses Element ausgewählt ist und ein Versuch zur Änderung von Dateien in gemeinsamen Ordnern erkannt wird, blockiert Kaspersky Endpoint Security die Netzwerkaktivität des Computers, welcher die Änderung ausgeführt hat, legt eine Backup-Kopie der beschädigten Dateien an und erstellt einen Berichtseintrag, der Informationen über diesen Versuch zur Änderung von Dateien in gemeinsamen Ordnern enthält. Ist dabei die Komponente Rollback von schädlichen Aktionen aktiviert, so werden die beschädigten Dateien aus ihren Backup-Kopien wiederhergestellt.

  Falls Sie das Element **Verbindung blockieren**ausgewählt haben, können Sie im Feld **Verbindung blockieren für** angeben, für welchen Zeitraum (in Minuten) die Netzwerkverbindung blockiert werden soll.

- Informieren

  Wenn dieses Element ausgewählt ist und es wird erkannt, dass versucht wird, Dateien in gemeinsamen Ordnern zu ändern, so fügt Kaspersky Endpoint Security Informationen über diesen Versuch zur Liste der aktiven Bedrohungen hinzu.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Adressen von Ausnahmen für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern anpassen

Damit die Funktionalität, mit der bestimmte Adressen aus dem Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ausgeschlossen werden können, funktioniert, muss der Dienst für die Anmeldungsüberwachung aktiviert werden. Der Dienst für die Anmeldungsüberwachung ist standardmäßig deaktiviert (weitere Informationen über die Aktivierung der Anmeldungsüberwachung finden Sie auf der Website der Microsoft Corporation).

Die Funktionalität, mit der bestimmte Adressen aus dem Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ausgeschlossen werden können, funktioniert nicht, wenn der betreffende Remote-Computer bereits vor dem Start von Kaspersky Endpoint Security eingeschaltet war. Sie können diesen Remote-Computer nach dem Start von Kaspersky Endpoint Security neu starten, damit die Funktionalität, mit der Adressen aus dem Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ausgeschlossen werden können, auf diesem Remote-Computer funktioniert.

Um bestimmte Remote-Computer, welche die externe Verschlüsselung von gemeinsamen Ordnern ausführen, vom Schutz auszuschließen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Verhaltensanalyse**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Verhaltensanalyse für Programme angezeigt.

3. Klicken Sie im Block **Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern** auf **Ausnahmen**.

   Das Fenster **Ausnahmen** wird geöffnet.

4. Führen Sie eine der folgenden Aktionen aus:

   - Um die IP-Adresse oder den Namen eines Computers zur Ausnahmeliste hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um die IP-Adresse oder den Namen eines Computers zu ändern, wählen Sie diesen in der Liste aus und klicken Sie auf **Ändern**.

   Das Fenster **Computer** wird geöffnet.

5. Geben Sie die IP-Adresse oder den Namen des Computers ein, dessen Versuche zur externen Verschlüsselung nicht verarbeitet werden sollen.

6. Klicken Sie im Fenster **Computer** auf **OK**.

7. Klicken Sie im Fenster **Ausnahmen** auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Exploit-Prävention

Dieser Abschnitt informiert über die Exploit-Prävention und erklärt die Einstellungen der Komponente.

Über die Exploit-Prävention

Die Komponente Exploit -Prävention überwacht die ausführbaren Dateien, die von verwundbaren Programmen gestartet werden. Wenn der Versuch zum Start einer ausführbaren Datei aus einem verwundbaren Programm nicht vom Benutzer ausgeführt wurde, blockiert Kaspersky Endpoint Security den Start dieser Datei. Informationen über das Startverbot der ausführbaren Datei werden im Bericht für den Exploit-Prävention aufgezeichnet.

Exploit-Prävention aktivieren und deaktivieren

Die Exploit-Prävention ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie die Exploit-Prävention deaktivieren.

Um die Exploit-Prävention zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Exploit-Prävention**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Exploit-Prävention angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

- Wenn Kaspersky Endpoint Security ausführbare Dateien überwachen soll, die von verwundbaren Programmen gestartet werden, aktivieren Sie das Kontrollkästchen **Exploit-Prävention aktivieren**.

  Wenn Kaspersky Endpoint Security erkennt, dass eine ausführbare Datei aus einem verwundbaren Programm nicht vom Benutzer gestartet wurde, führt Kaspersky Endpoint Security die Aktion aus, die in der Dropdown-Liste **Wenn ein Exploit erkannt wurde** ausgewählt ist.

- Wenn Kaspersky Endpoint Security ausführbare Dateien nicht überwachen soll, die von verwundbaren Programmen gestartet werden, deaktivieren Sie das Kontrollkästchen **Exploit-Prävention aktivieren**.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Exploit-Prävention anpassen

Um die Komponente Exploit-Prävention anzupassen, können Sie folgende Aktionen ausführen:

- Aktion für den Fund eines Exploits auswählen
- Schutz für den Arbeitsspeicher von Systemprozessen aktivieren oder deaktivieren

Aktion für den Fund eines Exploits auswählen

Beim Fund eines Exploits blockiert Kaspersky Endpoint Security standardmäßig die Aktivitäten dieses Exploits.

Um eine Aktion für den Fund eines Exploits auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Exploit-Prävention**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Exploit-Prävention angezeigt.

3. Wählen Sie in der Dropdown-Liste **Wenn ein Exploit erkannt wurde** die erforderliche Aktion aus:

   - **Vorgang blockieren**.

     Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, blockiert Kaspersky Endpoint Security die Aktivitäten dieses Exploits und erstellt einen Berichtseintrag, der Informationen über diesen Exploit enthält.

   - **Informieren**

     Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, erstellt Kaspersky Endpoint Security einen Berichtseintrag, der Informationen über diesen Exploit enthält, und fügt Informationen über diesen Exploit zur Liste der aktiven Bedrohungen hinzu.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz für den Arbeitsspeicher von Systemprozessen aktivieren und deaktivieren

Der Schutz für den Arbeitsspeicher von Systemprozessen ist standardmäßig aktiviert.

Um den Schutz für den Arbeitsspeicher von Systemprozessen zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Exploit-Prävention**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Exploit-Prävention angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie im Block **Schutz für den Arbeitsspeicher von Systemprozessen** das Kontrollkästchen **Schutz für den Arbeitsspeicher von Systemprozessen aktivieren**, damit Drittanbieter-Prozesse, die versuchen, auf Systemprozesse zuzugreifen, von Kaspersky Endpoint Security blockiert werden.

   - Deaktivieren Sie im Block **Schutz für den Arbeitsspeicher von Systemprozessen** das Kontrollkästchen **Schutz für den Arbeitsspeicher von Systemprozessen aktivieren**, damit Drittanbieter-Prozesse, die versuchen, auf Systemprozesse zuzugreifen, von Kaspersky Endpoint Security nicht blockiert werden.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Programm-Überwachung

> Diese Komponente ist verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Dateiserver installiert ist.

Dieser Abschnitt informiert über die Programm-Überwachung und erklärt die Einstellungen der Komponente.

Über die Programm-Überwachung

Die Komponente Programm-Überwachung hindert Programme daran, systemgefährdende Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und persönliche Daten.

Diese Komponente kontrolliert die Programmausführung, einschließlich des Zugriffs von Programmen auf geschützte Ressourcen (wie beispielsweise Dateien und Ordner, Registrierungsschlüssel). Dazu werden die *Kontrollregeln für Programme* verwendet. Bei den Aktivitätskontrollregeln für Programme handelt es sich um eine Auswahl an Beschränkungen, die für verschiedene Programmaktionen im Betriebssystem und für Zugriffsrechte für Computerressourcen gelten.

Die Netzwerkaktivität von Programmen wird durch die Komponente Firewall kontrolliert.

Wenn ein Programm zum ersten Mal auf dem Computer gestartet wird, überprüft die Komponente Programm-Überwachung, ob das Programm sicher ist, und ordnet es einer Sicherheitsgruppe zu. Die Sicherheitsgruppe bestimmt die Regeln, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet.

Um die Effektivität der Komponente Programm-Überwachung zu steigern, wird die Teilnahme an Kaspersky Security Network empfohlen. Die Daten, die mithilfe von Kaspersky Security Network ermittelt werden, erlauben es, Programme genauer einer bestimmten Sicherheitsgruppe zuzuordnen und optimale Aktivitätskontrollregeln für Programme anzuwenden.

Wenn ein Programm zum wiederholten Mal gestartet wird, kontrolliert die Programm-Überwachung die Integrität des Programms. Wurde ein Programm nicht verändert, so wendet die Komponente die aktuellen Aktivitätskontrollregeln für Programme darauf an. Wurde ein Programm verändert, wird es von der Programm-Überwachung erneut wie beim ersten Start überprüft.

Beschränkungen für die Kontrolle von Audio- und Videogeräten

Über den Schutz des Audiosignals

Die Funktionalität zum Schutz des Audiosignals besitzt folgende Besonderheiten:

- Damit die Funktionalität einwandfrei funktioniert, muss die Komponente Programm-Überwachung aktiviert sein.
- Hat ein Programm bereits begonnen, ein Audiosignal zu empfangen, bevor die Komponente Programm-Überwachung gestartet wurde, so erlaubt Kaspersky Endpoint Security dem Programm den Empfang des Audiosignals und zeigt keine Benachrichtigungen an.
- Wenn Sie ein Programm in die Gruppe **Nicht vertrauenswürdig** oder **Stark beschränkt** verschoben haben, nachdem das Programm bereits begonnen hat, ein Audiosignal zu empfangen, so erlaubt Kaspersky Endpoint Security dem Programm den Empfang des Audiosignals und zeigt keine Benachrichtigungen an.
- Wenn die Einstellungen für den Zugriff eines Programms auf Tonaufnahmegeräte geändert werden (Beispiel: Im Konfigurationsfenster der Programm-Überwachung wurde einem Programm verboten, Audiosignale zu empfangen), so muss dieses Programm neu gestartet werden, damit es keine Audiosignale mehr empfängt.
- Die Kontrolle über den Empfang eines Audiosignals von Tonaufnahmegeräten ist nicht von den Einstellungen für den Webcam-Schutz abhängig.
- Kaspersky Endpoint Security schützt nur den Zugriff auf integrierte und externe Mikrofone. Andere Tonübertragungsgeräte werden nicht unterstützt.
- Für Audiosignale, die von Geräten wie DSLR-Kameras, tragbaren Videokameras und Action-Cams übertragen werden, kann das Programm Kaspersky Endpoint Security keinen Schutz garantieren.

Besonderheiten von Audio- und Videogeräten bei der Installation und beim Update von Kaspersky Endpoint Security

Wenn das Programm Kaspersky Endpoint Security nach der Installation zum ersten Mal gestartet wird, kann es vorkommen, dass die Wiedergabe oder Aufzeichnung von Audio- und Videodaten in entsprechenden Programmen abgebrochen wird. Dies ist erforderlich, um die Überwachung des Zugriffs von Programmen auf Tonaufnahmegeräte zu aktivieren. Der Systemdienst für die Verwaltung von Audiogeräten wird beim ersten Start des Programms Kaspersky Endpoint Security neu gestartet.

Über den Zugriff von Programmen auf Webcams

Die Funktionalität für den Webcam-Schutz besitzt folgende Besonderheiten und Einschränkungen:

- Das Programm kontrolliert Videos und statische Bilder, die auf Webcam-Daten basieren.
- Das Programm kontrolliert Audiosignale, wenn diese zu einem Videostream der Webcam gehören.
- Das Programm kontrolliert nur Webcams, die über eine USB-Schnittstelle oder IEEE1394-Schnittstelle angeschlossen und im Microsoft Geräte-Manager als **Gerät zur Bildverarbeitung** (Imaging Device) angezeigt werden.

Unterstützte Webcams

Kaspersky Endpoint Security unterstützt folgende Webcams:

- Logitech HD Webcam C270
- Logitech HD Webcam C310
- Logitech Webcam C210
- Logitech Webcam Pro 9000
- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

Kaspersky Lab garantiert nicht, dass Webcams, die nicht in dieser Liste genannt sind, unterstützt werden.

Programm-Überwachung aktivieren und deaktivieren

Die Programm-Überwachung ist standardmäßig aktiviert und läuft im Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie die Komponente Programm-Überwachung deaktivieren.

Um die Komponente Programm-Überwachung zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.
3. Führen Sie im rechten Fensterbereich eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Programm-Überwachung aktivieren**, um die Komponente Programm-Überwachung einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Programm-Überwachung aktivieren**, um die Komponente Programm-Überwachung auszuschalten.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Sicherheitsgruppe für Programme verwenden

Wenn ein Programm zum ersten Mal gestartet wird, überprüft die Komponente Programm-Überwachung, ob das Programm sicher ist, und ordnet es einer Sicherheitsgruppe zu.

Beim ersten Schritt überprüft Kaspersky Endpoint Security, ob das Programm in der internen Datenbank für bekannte Programme verzeichnet ist, und sendet gleichzeitig eine Anfrage an die Datenbank von Kaspersky Security Network (sofern eine Internetverbindung besteht). Abhängig von den Ergebnissen der Überprüfung mit der internen Datenbank und der Datenbank von Kaspersky Security Network wird das Programm einer Sicherheitsgruppe zugeordnet. Bei jedem künftigen Programmstart sendet Kaspersky Endpoint Security eine neue Anfrage an die KSN-Datenbank, und weist das Programm einer anderen Sicherheitsgruppe zu, falls sich die Reputation des Programms in der KSN-Datenbank geändert hat.

Sie können eine Sicherheitsgruppe auswählen, in die Kaspersky Endpoint Security alle unbekannten Programme automatisch verschieben soll. Programme, die vor Kaspersky Endpoint Security gestartet wurden, werden automatisch der Sicherheitsgruppe zugeordnet, die im Fenster Sicherheitsgruppe wählen festgelegt ist.

> Für die Programme, die vor Kaspersky Endpoint Security gestartet wurden, wird nur die Netzwerkaktivität kontrolliert. Die Kontrolle erfolgt nach den Netzwerkregeln, die in den Firewall-Einstellungen festgelegt sind.

Einstellungen für die Zuordnung von Programmen zu Sicherheitsgruppen anpassen

> Wenn die Teilnahme an Kaspersky Security Network aktiviert ist, sendet Kaspersky Endpoint Security jedes Mal, wenn ein Programm gestartet wird, eine Reputationsabfrage an KSN. Aufgrund der

Antwort kann das Programm in eine andere Sicherheitsgruppe verschoben werden, als in den Einstellungen der Komponente Programm-Überwachung vorgegeben.

Programme, die mit Microsoft-Zertifikaten oder mit Kaspersky-Lab-Zertifikaten signiert sind, werden von Kaspersky Endpoint Security immer der Sicherheitsgruppe "Vertrauenswürdig" zugeordnet.

Gehen Sie folgendermaßen vor, um die Zuordnung von Programmen zu den einzelnen Sicherheitsgruppen anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente **Programm-Überwachung** angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Programmen mit digitaler Signatur vertrauen**, damit Programme mit einer digitalen Signatur automatisch in die Sicherheitsgruppe "Vertrauenswürdig" verschoben werden.
4. Damit alle unbekannten Programme einer angegebenen Sicherheitsgruppe zugeordnet werden, wählen Sie die erforderliche Sicherheitsgruppe in der Dropdown-Liste **Programme, für die keine Sicherheitsgruppe ermittelt werden konnte, automatisch verschieben nach** aus.

   Die Sicherheitsgruppe **Vertrauenswürdig** gehört aus Sicherheitsgründen nicht zu den Werten der Einstellung **Programme, für die keine Sicherheitsgruppe ermittelt werden konnte, automatisch verschieben nach**.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Sicherheitsgruppe ändern

Wird ein Programm zum ersten Mal gestartet, verschiebt Kaspersky Endpoint Security das Programm automatisch in die entsprechende Sicherheitsgruppe. Bei Bedarf können Sie ein Programm manuell in eine andere Sicherheitsgruppe verschieben.

Die Kaspersky-Lab-Experten warnen davor, Programme aus einer Sicherheitsgruppe, der sie automatisch zugewiesen wurde, in andere Sicherheitsgruppen zu verschieben. Ändern Sie stattdessen bei Bedarf die Aktivitätskontrollregeln für ein bestimmtes Programm.

Gehen Sie folgendermaßen vor, um die Sicherheitsgruppe zu ändern, in die ein Programm bei seinem ersten Start automatisch von Kaspersky Endpoint Security verschoben wurde:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.

3. Klicken Sie auf die Schaltfläche **Programme**.

   Die Registerkarte **Aktivitätskontrolle für Programme** des Fensters **Programme** wird geöffnet.

4. Wählen Sie auf der Registerkarte **Aktivitätskontrolle für Programme** das entsprechende Programm aus.

5. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie mit der rechten Maustaste auf das Programm. Wählen Sie im Kontextmenü des Programms den Punkt **Verschieben in Gruppe <Name der Gruppe>**.
   - Klicken Sie auf den Link **Vertrauenswürdig** / **Schwach beschränkt** / **Stark beschränkt** / **Nicht vertrauenswürdig**, um das Kontextmenü zu öffnen. Wählen Sie im Kontextmenü die entsprechende Sicherheitsgruppe.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Sicherheitsgruppe für Programme wählen, die vor Kaspersky Endpoint Security gestartet werden

Für die Programme, die vor Kaspersky Endpoint Security gestartet wurden, wird nur die Netzwerkaktivität kontrolliert. Die Kontrolle erfolgt nach den Netzwerkregeln, die in den Firewall-Einstellungen festgelegt sind. Um festzulegen, durch welche Netzwerkregeln die Kontrolle der Netzwerkaktivität solcher Programme reguliert werden soll, muss eine Sicherheitsgruppe angegeben werden.

Um eine Sicherheitsgruppe für Programme zu wählen, die vor Kaspersky Endpoint Security gestartet werden, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.

3. Klicken Sie auf **Ändern**.

   Das Fenster **Sicherheitsgruppe wählen** wird geöffnet.

4. Wählen Sie die erforderliche Sicherheitsgruppe.

5. Klicken Sie auf **OK**.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Arbeit mit den Kontrollregeln für Programme

Für die Programmkontrolle werden standardmäßig die Aktivitätskontrollregeln für Programme verwendet, welche für jene Sicherheitsgruppe gelten, in die das Programm bei seinem ersten Start von Kaspersky Endpoint Security verschoben wurde. Bei Bedarf können Sie die Aktivitätskontrollregeln für Programme für eine gesamte Sicherheitsgruppe, für ein einzelnes Programm oder für eine Programmgruppe innerhalb einer Sicherheitsgruppe ändern.

Aktivitätskontrollregeln für Programme, die sich auf konkrete Programme oder auf Programmgruppen innerhalb einer Sicherheitsgruppe beziehen, besitzen eine höhere Priorität als Aktivitätskontrollregeln für Programme, die sich auf eine Sicherheitsgruppe beziehen. Das bedeutet: Wenn die Einstellungen von Kontrollregeln für Programme, die sich auf ein konkretes Programm oder auf eine Programmgruppe innerhalb einer Sicherheitsgruppe beziehen, sich von den Einstellungen für Kontrollregeln für Programme unterscheiden, die sich auf eine Sicherheitsgruppe beziehen, dann kontrolliert die Programm-Überwachung das Programm oder die Programmgruppe innerhalb der Sicherheitsgruppe gemäß den Kontrollregeln für Programme, die sich auf das Programm oder die Programmgruppe beziehen.

Kontrollregeln für Programme für Sicherheitsgruppen und für Programmgruppen ändern

Standardmäßig sind für die einzelnen Sicherheitsgruppen optimale Aktivitätskontrollregeln für Programme vorgegeben. Die Einstellungen von Kontrollregeln für Programmgruppen, die zu einer Sicherheitsgruppe gehören, erben die Einstellungswerte der Kontrollregeln für die Sicherheitsgruppen. Sie können die vordefinierten Kontrollregeln für Sicherheitsgruppen und Kontrollregeln für Programmgruppen ändern.

Gehen Sie folgendermaßen vor, um vordefinierte Kontrollregeln für Sicherheitsgruppen oder Kontrollregeln für Programmgruppen zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.

3. Klicken Sie auf die Schaltfläche **Programme**.

   Die Registerkarte **Aktivitätskontrolle für Programme** des Fensters **Programm-Überwachung** wird geöffnet.

4. Wählen Sie die erforderliche Sicherheitsgruppe oder Programmgruppe.

5. Wählen Sie im Kontextmenü der Sicherheitsgruppe oder Programmgruppe den Punkt **Gruppenregeln** aus.

   Das Fenster **Kontrollregeln für eine Programmgruppe** wird geöffnet.

6. Führen Sie im Fenster **Kontrollregeln für eine Programmgruppe** eine der folgenden Aktionen aus:

   - Wählen Sie die Registerkarte **Dateien, Systemregistrierung**, um die Kontrollregeln für eine Sicherheitsgruppe oder die Kontrollregeln für eine Programmgruppe zu ändern, wenn sich die Kontrollregeln auf die Rechte der Sicherheitsgruppe oder Programmgruppe für Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen beziehen.

   - Wählen Sie die Registerkarte **Rechte**, um die Kontrollregeln für eine Sicherheitsgruppe oder die Kontrollregeln für eine Programmgruppe zu ändern, wenn sich die Kontrollregeln auf die Rechte der Sicherheitsgruppe oder Programmgruppe für den Zugriff auf Prozesse und Objekte des Betriebssystems beziehen.

7. Klicken Sie mit der rechten Maustaste auf die Spalte der entsprechenden Aktion, um die erforderliche Ressource zu wählen.

8. Wählen Sie im Kontextmenü den entsprechenden Punkt aus:

   - **Erben**.
   - **Erlauben**.
   - **Verbieten**.
   - **Protokollieren**.

   Wenn Sie eine Kontrollregel für eine Sicherheitsgruppe ändern, steht der Punkt **Erben** nicht zur Verfügung.

9. Klicken Sie auf **OK**.

10. Klicken Sie im Fenster **Programme** auf **OK**.

11. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Kontrollregel für ein Programm ändern

Die Einstellungen der Kontrollregeln für Programme, die zu einer Programmgruppe oder Sicherheitsgruppe gehören, erben standardmäßig die Einstellungswerte der Kontrollregeln für die Sicherheitsgruppe. Sie können die Einstellungen von Kontrollregeln für Programme ändern.

Gehen Sie folgendermaßen vor, um eine Kontrollregel für ein Programm zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.

3. Klicken Sie auf die Schaltfläche **Programme**.

   Die Registerkarte **Aktivitätskontrolle für Programme** des Fensters **Programm-Überwachung** wird geöffnet.

4. Wählen Sie das erforderliche Programm.

5. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie im Kontextmenü des Programms den Punkt **Regeln für das Programm** aus.
   - Klicken Sie rechts unten auf der Registerkarte **Aktivitätskontrolle für Programme** auf **Erweitert**.

   Das Fenster **Kontrollregeln für ein Programm** wird geöffnet.

6. Führen Sie im Fenster **Kontrollregeln für ein Programm** eine der folgenden Aktionen aus:

   - Wählen Sie die Registerkarte **Dateien, Systemregistrierung**, um die Kontrollregeln für ein Programm zu ändern, wenn sich die Kontrollregeln auf die Rechte des Programms für Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen beziehen.
   - Wählen Sie die Registerkarte **Rechte**, um die Kontrollregeln für ein Programm zu ändern, wenn sich die Kontrollregeln auf die Rechte des Programms für den Zugriff auf Prozesse und Objekte des Betriebssystems beziehen.

7. Klicken Sie mit der rechten Maustaste auf die Spalte der entsprechenden Aktion, um die erforderliche Ressource zu wählen.

8. Wählen Sie im Kontextmenü den entsprechenden Punkt aus:

   - **Erben**.
   - **Erlauben**.
   - **Verbieten**.
   - **Protokollieren**.

9. Klicken Sie auf **OK**.

10. Klicken Sie im Fenster **Programme** auf **OK**.

11. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Download und Aktualisierung von Kontrollregeln für Programme aus Kaspersky Security Network deaktivieren

Wenn in der Datenbank von Kaspersky Security Network neue Informationen über ein Programm gefunden werden, übernimmt Kaspersky Endpoint Security standardmäßig die aus der KSN-Datenbank heruntergeladenen Kontrollregeln. Die Kontrollregeln für ein Programm können später manuell angepasst werden.

Wenn ein Programm bei seinem ersten Start nicht in der Datenbank von Kaspersky Security Network verzeichnet war, danach jedoch entsprechende Informationen zur Datenbank von Kaspersky Security Network hinzugefügt wurden, so werden die Regeln für die Kontrolle dieses Programms automatisch von Kaspersky Endpoint Security aktualisiert.

Sie können den Download von Kontrollregeln für Programme aus dem Kaspersky Security Network und die automatische Aktualisierung der Kontrollregeln für bisher unbekannte Programme deaktivieren.

Gehen Sie folgendermaßen vor, um den Download und das Update von Kontrollregeln für Programme aus den Datenbanken von Kaspersky Security Network zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.

3. Deaktivieren Sie das Kontrollkästchen **Kontrollregeln für bisher unbekannte Programme aus KSN-Datenbanken aktualisieren**.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Vererbung von Beschränkungen eines übergeordneten Prozesses deaktivieren

Als Initiator für den Start eines Programms kann entweder der Benutzer oder ein anderes laufendes Programm auftreten. Tritt ein anderes Programm als Initiator für den Start auf, ergibt sich eine Startfolge, die über- und untergeordnete Prozesse umfasst.

Versucht ein Programm, Zugriff auf eine geschützte Ressource zu erhalten, so analysiert die Komponente Programm-Überwachung für alle übergeordneten Programmprozesse die Zugriffsrechte auf die geschützte Ressource. Dabei wird die Regel mit der niedrigsten Priorität ausgeführt: Beim Vergleich von Zugriffsrechten eines Programms und eines übergeordneten Prozesses werden auf die Programmaktivität die Zugriffsrechte mit der geringsten Priorität angewendet.

Für Zugriffsrechte ist folgende Priorität möglich:

1. **Erlauben**. Dieses Zugriffsrecht besitzt die höchste Priorität.

2. **Verbieten**. Dieses Zugriffsrecht besitzt die niedrigste Priorität.

Dieser Mechanismus verhindert, dass vertrauenswürdige Programme von zweifelhaften Programmen oder von Programmen, die über beschränkte Rechte verfügen, dazu benutzt werden, um privilegierte Aktionen auszuführen.

Wird eine Programmaktion blockiert, da ein übergeordneter Prozess unzureichende Rechte besitzt, so können Sie diese Rechte ändern oder die Vererbung von Beschränkungen des übergeordneten Prozesses deaktivieren.

Gehen Sie folgendermaßen vor, um die Vererbung von Beschränkungen eines übergeordneten Prozesses zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.
3. Klicken Sie auf die Schaltfläche **Programme**.

   Die Registerkarte **Kontrollregeln für Programme** des Fensters **Programm-Überwachung** wird geöffnet.
4. Wählen Sie das erforderliche Programm.
5. Wählen Sie im Kontextmenü des Programms den Punkt **Regeln für das Programm** aus.

   Das Fenster **Kontrollregeln für ein Programm** wird geöffnet.
6. Wählen Sie im Fenster **Kontrollregeln für ein Programm** die Registerkarte **Ausnahmen**.
7. Aktivieren Sie das Kontrollkästchen **Beschränkungen des übergeordneten Prozesses (Programms) nicht übernehmen**.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Fenster **Programme** auf **OK**.
10. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Ausschluss einiger Programmaktionen aus den Kontrollregeln für Programme

Gehen Sie folgendermaßen vor, um einige Programmaktionen aus den Kontrollregeln für Programme auszuschließen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.
3. Klicken Sie auf die Schaltfläche **Programme**.

   Die Registerkarte **Kontrollregeln für Programme** des Fensters **Programm-Überwachung** wird geöffnet.
4. Wählen Sie das erforderliche Programm.
5. Wählen Sie im Kontextmenü des Programms den Punkt **Regeln für das Programm** aus.

Das Fenster **Kontrollregeln für ein Programm** wird geöffnet.

6. Wählen Sie die Registerkarte **Ausnahmen**.
7. Aktivieren Sie die Kontrollkästchen der Programmaktionen, für die keine Kontrolle erforderlich ist.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Fenster **Programme** auf **OK**.
10. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Veraltete Kontrollregeln für Programme löschen

Standardmäßig werden Kontrollregeln für Programme, die innerhalb der letzten 60 Tage nicht gestartet wurden, automatisch gelöscht. Sie können die Speicherdauer der Kontrollregeln für nicht verwendete Programme ändern oder das automatische Löschen deaktivieren.

Um veraltete Kontrollregeln für Programme zu löschen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Kontrollregeln für Programme löschen, wenn nicht gestartet seit** und legen Sie fest, nach wie vielen Tagen Kontrollregeln für nicht verwendete Programme von Kaspersky Endpoint Security gelöscht werden sollen.
   - Deaktivieren Sie das Kontrollkästchen **Kontrollregeln für Programme löschen, wenn nicht gestartet seit**, um das automatische Löschen von Kontrollregeln für nicht verwendete Programme zu deaktivieren.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz für Betriebssystemressourcen und persönliche Daten

Die Komponente Programm-Überwachung verwaltet die Rechte von Programmen hinsichtlich ihren Vorgängen mit diversen Ressourcenkategorien des Betriebssystems und persönlichen Daten.

Die Kaspersky-Lab-Experten haben Kategorien für geschützte Ressourcen vordefiniert. Die für geschützte Ressourcen vorgegebenen Kategorien und die damit zusammenhängenden geschützten Ressourcen können nicht geändert oder gelöscht werden.

Sie können folgende Aktionen ausführen:

- Hinzufügen einer neuen Kategorie geschützter Ressourcen
- Hinzufügen einer neuen geschützten Ressource
- Deaktivieren des Schutzes für eine Ressource

Kategorie geschützter Ressourcen hinzufügen

Gehen Sie folgendermaßen vor, um eine neue Kategorie geschützter Ressourcen hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.
3. Klicken Sie auf die Schaltfläche **Ressourcen**.

   Die Registerkarte **Geschützte Ressourcen** des Fensters **Programm-Überwachung** wird geöffnet.
4. Wählen Sie im linken Bereich der Registerkarte **Geschützte Ressourcen** den Abschnitt oder die Kategorie der geschützten Ressourcen aus, dem/der Sie die neue Kategorie geschützter Ressourcen hinzufügen möchten.
5. Klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Kategorie**.

   Das Fenster **Kategorie für geschützte Ressourcen** wird geöffnet.
6. Geben Sie im Fenster **Kategorie für geschützte Ressourcen** den Namen der neuen Kategorie geschützter Ressourcen ein.
7. Klicken Sie auf **OK**.

   In der Liste der Kategorien geschützter Ressourcen erscheint ein neues Element.
8. Klicken Sie im Fenster **Programm-Überwachung** auf **OK**.
9. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Nach Hinzufügen einer Kategorie geschützter Ressourcen können Sie diese mithilfe der Schaltflächen **Ändern** oder **Löschen** oben links auf der Registerkarte **Geschützte Ressourcen** ändern oder löschen.

Geschützte Ressource hinzufügen

Gehen Sie folgendermaßen vor, um eine geschützte Ressource hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.

3. Klicken Sie auf die Schaltfläche **Ressourcen**.

   Die Registerkarte **Geschützte Ressourcen** des Fensters **Programm-Überwachung** wird geöffnet.

4. Wählen Sie im linken Bereich der Registerkarte **Geschützte Ressourcen** die Kategorie der geschützten Ressourcen aus, der Sie eine neue geschützte Ressource hinzufügen möchten.

5. Klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste den Ressourcentyp, der hinzugefügt werden soll:

   - **Datei oder Ordner**
   - **Registrierungsschlüssel**

   Das Fenster **Geschützte Ressource** wird geöffnet.

6. Geben Sie im Fenster **Geschützte Ressource** im Feld **Name** die Bezeichnung der zu schützenden Ressource ein.

7. Klicken Sie auf **Durchsuchen**.

8. Geben Sie im folgenden Fenster je nach Typ der zu schützenden Ressource, die Sie hinzufügen möchten, die erforderlichen Einstellungen ein und klicken Sie auf die Schaltfläche **OK**.

9. Klicken Sie im Fenster **Geschützte Ressource** auf **OK**.

   Auf der Registerkarte **Geschützte Ressourcen** erscheint in der Liste der geschützten Ressourcen der gewählten Kategorie ein neues Element.

10. Klicken Sie im Fenster **Programm-Überwachung** auf **OK**.

11. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Nach Hinzufügen der zu schützenden Ressource können Sie diese mithilfe der Schaltflächen **Ändern** und **Löschen** oben links auf der Registerkarte **Geschützte Ressourcen** ändern oder löschen.

Ressourcenschutz deaktivieren

Gehen Sie folgendermaßen vor, um den Ressourcenschutz zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Programm-Überwachung** aus.

Im rechten Fensterbereich werden die Einstellungen für die Komponente Programm-Überwachung angezeigt.

3. Klicken Sie im rechten Fensterbereich auf **Ressourcen**.

   Die Registerkarte **Geschützte Ressourcen** des Fensters **Programm-Überwachung** wird geöffnet.

4. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie in der Liste der geschützten Ressourcen im linken Bereich der Registerkarte die Ressource aus, deren Schutz Sie deaktivieren möchten, und deaktivieren Sie das zugehörige Kontrollkästchen.

   - Klicken Sie auf die Schaltfläche **Ausnahmen** und gehen Sie folgendermaßen vor:

     a. Klicken Sie auf im Fenster **Ausnahmen** auf **Hinzufügen** und wählen Sie in der Dropdown-Liste den Ressourcentyp aus, den Sie zur Ausnahmeliste für die Komponente Programm-Überwachung hinzufügen möchten: **Datei oder Ordner** oder **Registrierungsschlüssel**.

     Das Fenster **Geschützte Ressource** wird geöffnet.

     b. Geben Sie im Fenster **Geschützte Ressource** im Feld **Name** die Bezeichnung der zu schützenden Ressource ein.

     c. Klicken Sie auf **Durchsuchen**.

     d. Geben Sie im folgenden Fenster die erforderlichen Einstellungen für den betreffenden Typ der geschützten Ressource ein, die Sie der Ausnahmeliste hinzufügen möchten, die nicht von der Komponente Programm-Überwachung geschützt werden sollen.

     e. Klicken Sie auf **OK**.

     f. Klicken Sie im Fenster **Geschützte Ressource** auf **OK**.

     In der Liste der Ressourcen, die nicht von der Komponente Programm-Überwachung geschützt werden, erscheint ein neues Element.

     > Nachdem eine Ressource zur Liste der Ausnahmen hinzugefügt wurde, die nicht von der Komponente Programm-Überwachung geschützt werden, können Sie diese Ressource mithilfe der Schaltflächen **Ändern** oder **Löschen** im oberen Bereich des Fensters **Ausnahmen** ändern oder löschen.

     g. Klicken Sie im Fenster **Ausnahmen** auf **OK**.

5. Klicken Sie im Fenster **Programm-Überwachung** auf **OK**.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Rollback von schädlichen Aktionen

Dieser Abschnitt informiert über das Rollback von schädlichen Aktionen und erklärt die Einstellungen der Komponente.

Über das Rollback von schädlichen Aktionen

Mithilfe der Komponente Rollback von schädlichen Aktionen kann Kaspersky Endpoint Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

Beim Rollback von Schadsoftware-Aktionen im Betriebssystem verarbeitet Kaspersky Endpoint Security folgende Typen von schädlicher Programmaktivität:

- Dateiaktivität

  Kaspersky Endpoint Security löscht ausführbare Dateien, die von Schadsoftware erstellt wurden, wobei sich diese mit Ausnahme von Netzwerkdatenträgern auf beliebigen Datenträgern befinden können.

  Kaspersky Endpoint Security löscht ausführbare Dateien, die von einem Programm erstellt wurden, in welches Schadsoftware eingedrungen ist.

  Kaspersky Endpoint Security stellt veränderte oder gelöschte Dateien nicht wieder her.

- Aktivität der Registrierung

  Kaspersky Endpoint Security löscht Registrierungswerte und Registrierungsschlüssel, die von Schadsoftware erstellt wurden.

  Kaspersky Endpoint Security stellt veränderte oder gelöschte Registrierungswerte und -schlüssel nicht wieder her.

- Systemaktivität

  Kaspersky Endpoint Security beendet Prozesse, die von Schadsoftware gestartet wurden.

  Kaspersky Endpoint Security beendet Prozesse, in die Schadsoftware eingedrungen ist.

  Kaspersky Endpoint Security stellt Prozesse nicht wieder her, die von Schadsoftware beendet wurden.

- Netzwerkaktivität

  Kaspersky Endpoint Security verbietet die Netzwerkaktivität von Schadsoftware.

  Kaspersky Endpoint Security verbietet die Netzwerkaktivität von Prozessen, in die Schadsoftware eingedrungen ist.

Ein Rollback von Schadsoftware-Aktionen kann entweder von der Komponente Schutz vor bedrohlichen Dateien oder bei einer Antiviren-Untersuchung gestartet werden.

> Das Rollback der Aktionen schädlicher Programme betrifft lediglich eine eng eingeschränkte Auswahl an Daten. Ein Rollback hat keinerlei negativen Einfluss auf die Funktion des Betriebssystems und die Integrität der Daten auf Ihrem Computer.

Rollback von schädlichen Aktionen aktivieren und deaktivieren

Um das Rollback von schädlichen Aktionen zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Erweiterter Schutz** den Unterabschnitt **Rollback von schädlichen Aktionen**.

3. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Kaspersky Endpoint Security beim Fund von schädlichen Programmen die Aktionen, welche diese Programme im Betriebssystem ausgeführt haben, rückgängig machen soll, aktivieren Sie im rechten Fensterbereich das Kontrollkästchen **Rollback von schädlichen Aktionen aktivieren**.

   - Wenn Kaspersky Endpoint Security beim Fund von schädlichen Programmen die Aktionen, welche diese Programme im Betriebssystem ausgeführt haben, nicht rückgängig machen soll, deaktivieren Sie das Kontrollkästchen **Rollback von schädlichen Aktionen aktivieren**.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz vor bedrohlichen Dateien

Dieser Abschnitt informiert über die Komponente Schutz vor bedrohlichen Dateien und erklärt die Einstellungen dieser Komponente.

Über den Schutz vor bedrohlichen Dateien

Die Komponente Schutz vor bedrohlichen Dateien schützt das Dateisystem des Computers vor einer Infektion. Die Komponente Schutz vor bedrohlichen Dateien wird standardmäßig beim Start von Kaspersky Endpoint Security gestartet und befindet sich ständig im Arbeitsspeicher des Computers. Sie untersucht alle Dateien, die auf dem Computer und auf den verbundenen Laufwerken geöffnet, gespeichert und gestartet werden, auf Viren und andere bedrohliche Programme.

Wenn eine Bedrohung in einer Datei gefunden wird, führt Kaspersky Endpoint Security folgende Aktionen aus:

1. Typ des in einer Datei gefundenen Objekts wird bestimmt (beispielsweise *Virus* oder *trojanisches Programm*).

2. Auf dem Bildschirm wird eine Benachrichtigung über das schädliche Objekt angezeigt, das in der Datei gefunden wurde (falls die Benachrichtigungen aktiviert sind) und mit der Datei wird die Aktion ausgeführt, die in den Einstellungen der Komponente Schutz vor bedrohlichen Dateien vorgegeben ist.

Schutz vor bedrohlichen Dateien aktivieren und deaktivieren

Die Komponente Schutz vor bedrohlichen Dateien ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie den Schutz vor bedrohlichen Dateien deaktivieren.

Um den Schutz vor bedrohlichen Dateien zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

Öffnen Sie das Programmkonfigurationsfenster.

1. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor bedrohlichen Dateien angezeigt.

2. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Schutz vor bedrohlichen Dateien aktivieren**, um den Schutz vor bedrohlichen Dateien einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Schutz vor bedrohlichen Dateien aktivieren**, um den Schutz vor bedrohlichen Dateien auszuschalten.

3. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz vor bedrohlichen Dateien automatisch anhalten

Sie können festlegen, dass der Schutz vor bedrohlichen Dateien zu einem bestimmten Zeitpunkt oder bei der Arbeit mit bestimmten Programmen automatisch angehalten wird.

Es gilt als Notlösung, den Schutz vor bedrohlichen Dateien bei einem Konflikt mit bestimmten Programmen anzuhalten. Sollten bei der Ausführung der Komponente Konflikte auftreten, wenden Sie sich bitte an den Technischen Support von Kaspersky Lab (https://companyaccount.kaspersky.com). Die Experten helfen Ihnen dabei, eine Lösung für die gleichzeitige Verwendung der Komponente Schutz vor bedrohlichen Dateien mit anderen Programmen auf Ihrem Computer zu finden.

Um das automatische Anhalten des Schutzes vor bedrohlichen Dateien anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente **Schutz vor bedrohlichen Dateien** angezeigt.
3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor bedrohlichen Dateien** wird geöffnet.
4. Wählen Sie im Fenster **Schutz vor bedrohlichen Dateien** die Registerkarte **Erweitert**.
5. Führen Sie unter **Aufgabe anhalten** folgende Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **Nach Zeitplan** und klicken Sie auf **Zeitplan**, um festzulegen, zu welchem Zeitpunkt der Schutz vor bedrohlichen Dateien automatisch angehalten werden soll.

     Das Fenster **Aufgabe anhalten** wird geöffnet.
   - Aktivieren Sie das Kontrollkästchen **Bei Programmstart** und klicken Sie auf **Auswählen**, um festzulegen, dass der Schutz vor bedrohlichen Dateien beim Start bestimmter Programme automatisch angehalten werden soll.

     Das Fenster **Programme** wird geöffnet.

6. Führen Sie eine der folgenden Aktionen aus:

   - Um festzulegen, dass der Schutz vor bedrohlichen Dateien zu einen bestimmten Zeitpunkt automatisch angehalten werden soll, geben Sie im Fenster**Aufgabe anhalten** in den Feldern **Anhalten um** und **Fortsetzen um** (im Format hh:mm) den Zeitraum an, für den der Schutz vor bedrohlichen Dateien angehalten werden soll. Klicken Sie auf **OK**.

   - Um festzulegen, dass der Schutz vor bedrohlichen Dateien beim Start bestimmter Programme automatisch angehalten werden soll, erstellen Sie im Fenster **Programme** mit den Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** eine Liste der Programme, bei deren Start der Schutz vor bedrohlichen Dateien angehalten werden soll. Klicken Sie auf **OK**.

7. Klicken Sie im Fenster **Schutz vor bedrohlichen Dateien** auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz vor bedrohlichen Dateien anpassen

Um die Komponente Schutz vor bedrohlichen Dateien anzupassen, können Sie folgende Aktionen ausführen:

- Sicherheitsstufe ändern

  Sie können eine der vordefinierten Sicherheitsstufen wählen oder die Einstellungen einer Sicherheitsstufe anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

- Ändern der Aktion, welche die Komponente Schutz vor bedrohlichen Dateien beim Fund einer infizierten Datei ausführen soll.

- Schutzbereich für die Komponente Schutz vor bedrohlichen Dateien festlegen

  Sie können den Schutzbereich erweitern oder einschränken, indem Sie Untersuchungsobjekte hinzufügen oder entfernen, oder den Typ der zu untersuchenden Dateien ändern.

- Verwendung der heuristischen Analyse anpassen

  Die Komponente Schutz vor bedrohlichen Dateien verwendet die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse. Bei der Signaturanalyse vergleicht die Komponente Schutz vor bedrohlichen Dateien ein gefundenes Objekt mit den Einträgen in den Antiviren-Datenbanken des Programms. Aufgrund von Empfehlungen der Kaspersky-Lab-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.

  Sie können die heuristische Analyse verwenden, um den Schutz noch wirksamer zu gestalten. Bei der heuristischen Analyse analysiert die Komponente Schutz vor bedrohlichen Dateien die Aktivität, die Objekte im System zeigen. Die heuristische Analyse erlaubt die Erkennung schädlicher Objekte, die noch nicht in den Antiviren-Datenbanken des Programms verzeichnet sind.

- Optimierung der Untersuchung

  Um die Dateiuntersuchung mit der Komponente Schutz vor bedrohlichen Dateien zu optimieren, können Sie die Untersuchungsdauer verkürzen und die Leistung von Kaspersky Endpoint Security erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Sie können außerdem die Technologien iChecker und iSwift aktivieren, mit denen sich die Dateiuntersuchung beschleunigen lässt. Dabei werden Dateien von der Untersuchung ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

- Anpassen der Untersuchung von zusammengesetzten Dateien
- Ändern des Untersuchungsmodus für Dateien

Sicherheitsstufe ändern

Der Schutz vor bedrohlichen Dateien bietet unterschiedliche Einstellungsvarianten für den Schutz des Dateisystems eines Computers. Diese Einstellungssätze heißen *Sicherheitsstufen*. Es gibt drei vordefinierte Sicherheitsstufen: **Hoch**, **Empfohlen**, **Niedrig**. Die Sicherheitsstufe **Empfohlen** gilt als optimal und wird von den Kaspersky-Lab-Spezialisten empfohlen.

Um die Sicherheitsstufe zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor bedrohlichen Dateien angezeigt.
3. Führen Sie unter **Sicherheitsstufe** eine der folgenden Aktionen aus:
   - Um eine der vordefinierten Sicherheitsstufen festzulegen (**Hoch**, **Empfohlen**, **Niedrig**), verwenden Sie den Schieberegler.
   - Wenn Sie die Sicherheitsstufe anpassen möchten, klicken Sie auf **Einstellungen** und nehmen Sie im folgenden Fenster **Schutz vor bedrohlichen Dateien** die entsprechenden Einstellungen vor.

     Nachdem Sie die Einstellungen einer Sicherheitsstufe geändert haben, ändert sich der Name der Sicherheitsstufe im Block **Sicherheitsstufe** in **Benutzerdefiniert**.
   - Wenn Sie die Sicherheitsstufe **Empfohlen** festlegen möchten, klicken Sie auf **Standard**.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Ändern der Aktion, welche die Komponente Schutz vor bedrohlichen Dateien mit infizierten Dateien ausführen soll

Die Komponente Schutz vor bedrohlichen Dateien versucht standardmäßig, alle gefundenen infizierten Dateien automatisch zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden diese Dateien von der Komponente „Schutz vor bedrohlichen Dateien" gelöscht.

Zum Ändern der Aktion, welche die Komponente Schutz vor bedrohlichen Dateien mit infizierten Dateien ausführen soll, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor bedrohlichen Dateien angezeigt.

3. Wählen Sie unter **Aktion beim Fund einer Bedrohung** die entsprechende Option:

   - **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**.

     Wenn diese Variante ausgewählt ist, versucht die Komponente „Schutz vor bedrohlichen Dateien" automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden diese Dateien von der Komponente „Schutz vor bedrohlichen Dateien" gelöscht.

   - **Desinfizieren. Blockieren, wenn Desinfektion nicht möglich**.

     Wenn diese Variante ausgewählt ist, versucht die Komponente „Schutz vor bedrohlichen Dateien" automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden diese Dateien von der Komponente „Schutz vor bedrohlichen Dateien" blockiert.

   - **Blockieren**.

     Wenn diese Variante ausgewählt ist, blockiert die Komponente „Schutz vor bedrohlichen Dateien" die infizierten Dateien automatisch, ohne einen Desinfektionsversuch zu unternehmen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutzbereich für die Komponente Schutz vor bedrohlichen Dateien

Der Begriff Schutzbereich bezieht sich auf die Objekte, die von einer Komponente während ihrer Ausführung untersucht werden. Der Schutzbereich besitzt je nach Komponente unterschiedliche Eigenschaften. Der Schutzbereich für die Komponente Schutz vor bedrohlichen Dateien wird durch die Eigenschaften Speicherort und Typ der zu untersuchenden Dateien definiert. Die Komponente Schutz vor bedrohlichen Dateien untersucht standardmäßig nur infizierbare Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers aus gestartet werden.

Gehen Sie folgendermaßen vor, um einen Schutzbereich zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor bedrohlichen Dateien angezeigt.

3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor bedrohlichen Dateien** wird geöffnet.

4. Wählen Sie im Fenster **Schutz vor bedrohlichen Dateien** die Registerkarte **Allgemein**.

5. Geben Sie im Block **Dateitypen** den Typ der Dateien an, die von der Komponente Schutz vor bedrohlichen Dateien untersucht werden sollen:

   - Wählen Sie **Alle Dateien**, wenn alle Dateien untersucht werden sollen.
   - Wählen Sie **Dateien nach Format untersuchen**, wenn Dateien jener Formate untersucht werden sollen, die am häufigsten infiziert werden.
   - Wählen Sie **Dateien nach Erweiterung untersuchen**, wenn Dateien mit solchen Erweiterungen untersucht werden sollen, die am häufigsten infiziert werden.

   Bei der Auswahl des Typs der zu untersuchenden Dateien sollte Folgendes beachtet werden:

   - Es gibt eine Reihe von Dateiformaten (z. B. TXT), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (z. B. die Formate exe, dll, doc). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist relativ hoch.
   - Ein Angreifer kann einen Virus oder ein anderes bedrohliches Programm in einer ausführbaren Datei, deren Erweiterung in TXT geändert wurde, an Ihren Computer senden. Wenn Sie die Dateiuntersuchung nach Erweiterung ausgewählt haben, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Untersuchung von Dateien nach Format ausgewählt, so ignoriert die Komponente Schutz vor bedrohlichen Dateien die Erweiterung und analysiert die Kopfzeile der Datei. Dabei kann sich ergeben, dass die Datei das Format EXE besitzt. Eine solche Datei wird sorgfältig auf Viren und andere bedrohliche Programme untersucht.

6. Führen Sie in der Liste **Schutzbereich** eine der folgenden Aktionen aus:

   - Klicken Sie auf **Hinzufügen**, um ein neues Objekt zum Untersuchungsbereich hinzuzufügen.
   - Um den Ort eines Objekts zu ändern, wählen Sie ein Objekt aus dem Untersuchungsbereich und klicken Sie auf **Ändern**.

   Das Fenster **Untersuchungsbereich wählen** wird geöffnet.

   - Wählen Sie in der Liste der Untersuchungsobjekte ein Objekt und klicken Sie auf **Löschen**, wenn Sie ein Objekt aus der Liste der Untersuchungsobjekte löschen möchten.

     Ein Fenster zur Bestätigung des Löschvorgangs wird geöffnet.

7. Führen Sie eine der folgenden Aktionen aus:

   - Um ein neues Objekt zur Liste der Untersuchungsobjekte hinzuzufügen oder den Speicherort eines vorhandenen Objekts zu ändern, wählen Sie im Fenster **Untersuchungsbereich wählen** ein Objekt aus und klicken Sie auf **Hinzufügen**.

     Alle Objekte, die im Fenster **Untersuchungsbereich wählen** markiert sind, werden im Fenster **Schutz vor bedrohlichen Dateien** in der Liste **Schutzbereich** angezeigt.

     Klicken Sie auf **OK**.

   - Klicken Sie im Bestätigungsfenster auf **Ja**, wenn Sie das Objekt löschen möchten.

8. Wiederholen Sie gegebenenfalls die Punkte 6-7, um ein Objekt hinzuzufügen, den Speicherort eines Objekts zu ändern oder Objekte aus der Liste der Untersuchungsobjekte zu löschen.

9. Wenn ein Objekt aus der Liste der Untersuchungsobjekte ausgeschlossen werden soll, deaktivieren Sie in der Liste **Schutzbereich** das entsprechende Kontrollkästchen. In diesem Fall verbleibt das Objekt in der Liste der Untersuchungsobjekte, wird aber von der Komponente Schutz vor bedrohlichen Dateien aus der Untersuchung ausgeschlossen.

10. Klicken Sie im Fenster **Schutz vor bedrohlichen Dateien** auf **OK**.

11. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Verwendung der heuristischen Analyse durch die Komponente Schutz vor bedrohlichen Dateien

Um die Verwendung der heuristischen Analyse für die Komponente Schutz vor bedrohlichen Dateien anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor bedrohlichen Dateien angezeigt.

3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor bedrohlichen Dateien** wird geöffnet.

4. Wählen Sie im Fenster **Schutz vor bedrohlichen Dateien** die Registerkarte **Leistung**.

5. Führen Sie im Abschnitt **Untersuchungsmethoden** folgende Schritte aus:

   - Wenn die Komponente Schutz vor bedrohlichen Dateien die heuristische Analyse verwenden soll, aktivieren Sie das Kontrollkästchen **Heuristische Analyse** und stellen Sie mit dem Schieberegler die Stufe der heuristischen Analyse ein: **oberflächlich**, **mittel** oder **tief**.

   - Wenn die Komponente Schutz vor bedrohlichen Dateien die heuristische Analyse nicht verwenden soll, deaktivieren Sie das Kontrollkästchen **Heuristische Analyse**.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Verwendung von Untersuchungstechnologien durch die Komponente Schutz vor bedrohlichen Dateien

Um die Verwendung der Untersuchungstechnologien für die Komponente Schutz vor bedrohlichen Dateien anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor bedrohlichen Dateien angezeigt.

3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor bedrohlichen Dateien** wird geöffnet.

4. Wählen Sie im Fenster **Schutz vor bedrohlichen Dateien** die Registerkarte **Erweitert**.

5. Führen Sie im Abschnitt **Untersuchungstechnologien** folgende Schritte aus:

   - Aktivieren Sie die Kontrollkästchen für die Technologien, die von der Komponente Schutz vor bedrohlichen Dateien verwendet werden sollen.

   - Deaktivieren Sie die Kontrollkästchen für die Technologien, die nicht von der Komponente Schutz vor bedrohlichen Dateien verwendet werden sollen.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Dateiuntersuchung optimieren

Gehen Sie folgendermaßen vor, um die Untersuchung von Dateien zu optimieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor bedrohlichen Dateien angezeigt.

3. Klicken Sie auf **Einstellungen**.

   Das Fenster **Schutz vor bedrohlichen Dateien** wird geöffnet.

4. Wählen Sie im Fenster **Schutz vor bedrohlichen Dateien** die Registerkarte **Leistung**.

5. Aktivieren Sie unter **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Untersuchung von zusammengesetzten Dateien

Eine häufige Methode, mit der Viren und andere bedrohliche Programme versteckt werden, ist die Einbettung der Schädlinge in zusammengesetzte Dateien wie beispielsweise Archive oder E-Mail-Datenbanken. Eine zusammengesetzte Datei muss entpackt werden, um Viren und sonstige Schadprogramme aufzuspüren, die auf diese Weise versteckt wurden. Dadurch kann die Untersuchungsgeschwindigkeit sinken. Die Auswahl der zusammengesetzten Dateien, die untersucht werden sollen, lässt sich einschränken. Dadurch erhöht sich das Untersuchungstempo.

Die Verarbeitungsmethode für eine zusammengesetzte infizierte Datei (Löschen oder Desinfektion) ist vom Dateityp abhängig.

Die Komponente Schutz vor bedrohlichen Dateien desinfiziert zusammengesetzte Dateien der Formate RAR, ARJ, ZIP, CAB und LHA, und löscht Dateien aller übrigen Formate (unter Ausnahme von E-Mail-Datenbanken).

Gehen Sie folgendermaßen vor, um die Untersuchung von zusammengesetzten Dateien anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor bedrohlichen Dateien angezeigt.
3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor bedrohlichen Dateien** wird geöffnet.
4. Wählen Sie im Fenster **Schutz vor bedrohlichen Dateien** die Registerkarte **Leistung**.
5. Geben Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Installationspakete oder Office-Format-Dateien.
6. Damit nur neue und veränderte zusammengesetzte Dateien untersucht werden, aktivieren Sie das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

   Die Komponente Schutz vor bedrohlichen Dateien untersucht nur neue und veränderte zusammengesetzte Dateien aller Typen.
7. Klicken Sie auf **Erweitert**.

   Das Fenster **Zusammengesetzte Dateien** wird geöffnet.
8. Führen Sie unter **Untersuchung im Hintergrund** eine der folgenden Aktionen aus:

   - Wenn die Komponente Schutz vor bedrohlichen Dateien zusammengesetzte Dateien nicht im Hintergrund entpacken soll, deaktivieren Sie das Kontrollkästchen **Zusammengesetzte Dateien im Hintergrund entpacken**.

- Wenn die Komponente Schutz vor bedrohlichen Dateien zusammengesetzte Dateien bei der Untersuchung im Hintergrund entpacken soll, aktivieren Sie das Kontrollkästchen **Zusammengesetzte Dateien im Hintergrund entpacken** und geben Sie im Feld **Minimale Dateigröße** einen entsprechenden Wert an.

9. Führen Sie unter **Größenbeschränkung** eine der folgenden Aktionen aus:

   - Wenn die Komponente Schutz vor bedrohlichen Dateien umfangreiche zusammengesetzte Dateien nicht entpacken soll, aktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und geben Sie im Feld **Maximale Dateigröße** einen entsprechenden Wert an. Zusammengesetzte Dateien, welche die angegebene Größe überschreiten, werden von der Komponente Schutz vor bedrohlichen Dateien nicht entpackt.

   - Wenn die Komponente Schutz vor bedrohlichen Dateien umfangreiche zusammengesetzte Dateien entpacken soll, deaktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**.

     Eine Datei gilt als groß, wenn ihre Größe den im Feld **Maximale Dateigröße** angegebenen Wert überschreitet.

   Unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist, werden große Dateien beim Extrahieren aus Archiven von der Komponente Schutz vor bedrohlichen Dateien untersucht.

10. Klicken Sie auf **OK**.

11. Klicken Sie im Fenster **Schutz vor bedrohlichen Dateien** auf **OK**.

12. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Untersuchungsmodus für Dateien ändern

Untersuchungsmodus bedeutet eine Bedingung, unter welcher die Komponente Schutz vor bedrohlichen Dateien die Untersuchung einer Datei starten soll. Kaspersky Endpoint Security verwendet standardmäßig den intelligenten Untersuchungsmodus für Dateien. Um zu entscheiden, ob eine Untersuchung von Dateien erforderlich ist, analysiert die Komponente Schutz vor bedrohlichen Dateien in diesem Modus die Vorgänge, die von einem Benutzer, von einem Programm im Auftrag eines Benutzers (mit dessen Benutzerdaten eine Anmeldung im Betriebssystem erfolgte, oder eines anderen Benutzers) oder vom Betriebssystem ausgeführt werden. Wird beispielsweise mit einem Microsoft-Office-Word-Dokument gearbeitet, so untersucht Kaspersky Endpoint Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für Dateien zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor bedrohlichen Dateien**.

Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor bedrohlichen Dateien angezeigt.

3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor bedrohlichen Dateien** wird geöffnet.

4. Wählen Sie im Fenster **Schutz vor bedrohlichen Dateien** die Registerkarte **Erweitert**.

5. Wählen Sie unter **Untersuchungsmodus** den erforderlichen Modus:

   - **Intelligent**
   - **Bei Zugriff und Veränderungen**
   - **Bei Zugriff**
   - **Bei Ausführung**

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz vor Web-Bedrohungen

Diese Komponente ist verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Dateiserver installiert ist.

Dieser Abschnitt informiert über die Komponente Schutz vor Web-Bedrohungen und erklärt die Einstellungen der Komponente.

Über den Schutz vor Web-Bedrohungen

Bei der Arbeit im Internet besteht für die Daten, die auf dem Computer gespeichert sind, ständig das Risiko einer Infektion durch Viren und andere Schadprogramme. Diese können in den Computer eindringen, wenn der Benutzer kostenlose Programme herunterlädt oder Websites besucht, die zuvor von Angreifern manipuliert worden sind. Netzwürmer können direkt beim Aufbau einer Internetverbindung in den Benutzercomputer eindringen, noch bevor eine Webseite geöffnet oder eine Datei heruntergeladen wurde.

Die Komponente Schutz vor Web-Bedrohungen schützt Informationen, die über die Protokolle HTTP und FTP auf den Benutzercomputer gelangen oder von ihm gesendet werden. Außerdem wird überprüft, ob Links zu bösartigen Webadressen oder zu Phishing-Adressen führen.

Jede Webseite oder Datei, auf die ein Benutzer oder ein bestimmtes Programm über die Protokolle HTTP oder FTP zugreift, wird von der Komponente Schutz vor Web-Bedrohungen abgefangen und auf Viren und andere Schadprogramme hin analysiert. Das weitere Vorgehen sieht vor:

- Wurde auf einer Webseite oder in einer Datei kein Schadcode gefunden, wird sie dem Benutzer sofort zur Verfügung gestellt.

- Enthält eine Webseite oder eine Datei, auf die der Benutzer zugreift, schädlichen Code, so führt das Programm die Aktion aus, die in den Einstellungen für die Komponente Schutz vor Web-Bedrohungen vorgegeben ist.

Schutz vor Web-Bedrohungen aktivieren und deaktivieren

Die Komponente Schutz vor Web-Bedrohungen ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie die Komponente Schutz vor Web-Bedrohungen deaktivieren.

Um die Komponente Schutz vor Web-Bedrohungen zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor Web-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor Web-Bedrohungen angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Schutz vor Web-Bedrohungen aktivieren**, um die Komponente Schutz vor Web-Bedrohungen einzuschalten.

   - Deaktivieren Sie das Kontrollkästchen **Schutz vor Web-Bedrohungen aktivieren**, um die Komponente Schutz vor Web-Bedrohungen auszuschalten.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz vor Web-Bedrohungen anpassen

Um die Komponente Schutz vor Web-Bedrohungen anzupassen, können Sie folgende Aktionen ausführen:

- Ändern der Sicherheitsstufe für den Web-Datenverkehr

  Sie können eine der vordefinierten Sicherheitsstufen für den Web-Datenverkehr wählen, der mit den Protokollen HTTP und FTP empfangen oder übertragen wird, oder die Einstellungen einer Sicherheitsstufe für den Web-Datenverkehr selbstständig anpassen.

  Nachdem Sie die Einstellungen einer Sicherheitsstufe für den Web-Datenverkehr geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

- Ändern der Aktion, die Kaspersky Endpoint Security mit schädlichen Objekten im Web-Datenverkehr ausführen soll.

  Erkennt die Komponente Schutz vor Web-Bedrohungen bei der Untersuchung eines Objekts im Web-Datenverkehr schädlichen Code, so ist das weitere Vorgehen für dieses Objekt von der Aktion abhängig, die Sie festgelegt haben.

- Anpassen der Link-Untersuchung mithilfe der Datenbanken für Phishing-Webadressen und schädliche Adressen durch die Komponente Schutz vor Web-Bedrohungen

- Konfiguration der Verwendung der heuristischen Analyse bei der Untersuchung des Web-Datenverkehrs auf Viren und andere Schadprogramme

  Sie können die heuristische Analyse verwenden, um den Schutz noch wirksamer zu gestalten. Bei der heuristischen Analyse analysiert Kaspersky Endpoint Security die Aktivität, die Programme im Betriebssystem zeigen. Die heuristische Analyse kann Bedrohungen erkennen, über die noch keine Einträge in den Datenbanken von Kaspersky Endpoint Security vorliegen.

- Konfiguration der Verwendung der heuristischen Analyse bei der Untersuchung von Webseiten auf Phishing-Links

- Optimierung der Untersuchung des Web-Datenverkehrs, der mit den Protokollen HTTP und FTP gesendet und empfangen wird, durch die Komponente Schutz vor Web-Bedrohungen

- Erstellen einer Liste mit vertrauenswürdigen Webadressen

  Sie können eine Liste der Webadressen anlegen, deren Inhalt Sie vertrauen. Informationen, die von vertrauenswürdigen Webadressen stammen, werden von der Komponente Schutz vor Web-Bedrohungen nicht auf Viren und andere gefährliche Programme analysiert. Diese Option kann beispielsweise nützlich sein, wenn die Komponente Schutz vor Web-Bedrohungen den Download einer Datei von einer Ihnen bekannten Website verhindert.

  > Der Begriff Webadresse bezieht sich sowohl auf eine bestimmte Webseite, als auch auf eine Website.

Sicherheitsstufe für den Web-Datenverkehr ändern

Die Komponente Schutz vor Web-Bedrohungen bietet unterschiedliche Einstellungsvarianten für den Schutz von Daten, die mit den Protokollen HTTP und FTP empfangen und übertragen werden. Diese Einstellungsvarianten werden *Sicherheitsstufen für den Web-Datenverkehr* genannt. Es gibt drei vordefinierte Sicherheitsstufen für den Web-Datenverkehr: **Hoch**, **Empfohlen**, **Niedrig**. Die Sicherheitsstufe **Empfohlen** gilt für den Web-Datenverkehr als optimal und wird von den Kaspersky-Lab-Spezialisten empfohlen.

Gehen Sie folgendermaßen vor, um die Sicherheitsstufe für den Web-Datenverkehr zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor Web-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor Web-Bedrohungen angezeigt.

3. Führen Sie unter **Sicherheitsstufe** eine der folgenden Aktionen aus:

   - Verwenden Sie den Schieberegler, um eine vordefinierte Sicherheitsstufe für den Web-Datenverkehr zu wählen (**Hoch**, **Empfohlen**, **Niedrig**).

   - Wenn Sie die Sicherheitsstufe für den Web-Datenverkehr selbst anpassen möchten, klicken Sie auf **Einstellungen** und nehmen Sie im folgenden Fenster **Schutz vor Web-Bedrohungen** die entsprechenden Einstellungen vor.

Nachdem Sie die Einstellungen einer Sicherheitsstufe für den Web-Datenverkehr geändert haben, ändert sich der Name der Sicherheitsstufe für den Web-Datenverkehr im Block **Sicherheitsstufe** in **Benutzerdefiniert**.

- Klicken Sie auf **Standard**, um eine benutzerdefinierte Sicherheitsstufe für den Web-Datenverkehr auf die Sicherheitsstufe **Empfohlen** zurückzusetzen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktion für schädliche Objekte im Web-Datenverkehr ändern

Wenn ein infiziertes Objekt im Web-Datenverkehr gefunden wird, blockiert die Komponente Schutz vor Web-Bedrohungen standardmäßig den Zugriff auf das Objekt und zeigt eine Bildschirmmeldung über die Sperrung an.

Gehen Sie folgendermaßen vor, um die Aktion für schädliche Objekte im Web-Datenverkehr zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor Web-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor Web-Bedrohungen angezeigt.

3. Wählen Sie unter **Aktion beim Fund einer Bedrohung** eine Aktion, die Kaspersky Endpoint Security ausführen soll, wenn im Web-Datenverkehr ein schädliches Objekt gefunden wird:

   - **Download verbieten**.

     Wenn diese Variante ausgewählt ist und ein infiziertes Objekt im Web-Datenverkehr gefunden wird, blockiert die Komponente Schutz vor Web-Bedrohungen den Zugriff auf das Objekt, zeigt eine Bildschirmmeldung über die Sperrung an und erstellt einen Berichtseintrag, der Informationen über das infizierte Objekt enthält.

   - **Informieren**

     Wenn diese Aktion ausgewählt ist und ein infiziertes Objekt im Web-Datenverkehr gefunden wird, erlaubt die Komponente Schutz vor Web-Bedrohungen den Download dieses Objekts auf den Computer. Außerdem protokolliert Kaspersky Endpoint Security einen Eintrag, der Informationen über das infizierte Objekt enthält, und fügt zur Liste für aktive Bedrohungen Informationen über das infizierte Objekt hinzu.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Link-Untersuchung mithilfe der Datenbanken für Phishing-Webadressen und schädliche Adressen durch die Komponente Schutz vor Web-Bedrohungen

Durch eine Untersuchung von Links auf Phishing-Webadressen lassen sich *Phishing-Angriffe* vermeiden. Ein häufiges Beispiel für Phishing-Angriffe ist eine E-Mail-Nachricht, die scheinbar von Ihrer Bank stammt und einen Link zur offiziellen Website der Bank enthält. Wenn Sie dem Link folgen, gelangen Sie auf eine Website, die eine exakte Kopie der Bankseite darstellt und für die im Browser sogar deren Webadresse angezeigt wird, obwohl Sie sich in Wirklichkeit auf einer fiktiven Website befinden. Alle Aktionen, die Sie auf dieser Website ausführen, werden verfolgt und können zum Diebstahl Ihres Geldes missbraucht werden.

Da sich ein Phishing-Link nicht nur in E-Mail-Nachrichten, sondern beispielsweise auch im Text einer ICQ-Nachricht befinden kann, überwacht die Komponente Schutz vor Web-Bedrohungen alle Versuche zum Öffnen einer Phishing-Website auf der Ebene des Web-Datenverkehrs und blockiert den Zugriff auf solche Websites. Listen mit Phishing-Webadressen gehören zum Lieferumfang von Kaspersky Endpoint Security.

Um in der Komponente Schutz vor Web-Bedrohungen die Link-Untersuchung anzupassen, bei der die Datenbanken für Phishing-Webadressen und schädliche Adressen verwendet werden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor Web-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor Web-Bedrohungen angezeigt.
3. Klicken Sie auf **Einstellungen**.

   Das Fenster **Schutz vor Web-Bedrohungen** wird geöffnet.
4. Wählen Sie im Fenster **Schutz vor Web-Bedrohungen** die Registerkarte **Allgemein**.
5. Gehen Sie wie folgt vor:

   - Aktivieren Sie im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mithilfe der Datenbank für bösartige Webadressen untersuchen**, damit die Komponente Schutz vor Web-Bedrohungen bei der Link-Untersuchung die Datenbanken für schädliche Webadressen verwendet.
   - Aktivieren Sie im Block **Anti-Phishing-Einstellungen** das Kontrollkästchen **Links mithilfe der Datenbank für Phishing-Webadressen untersuchen**, damit die Komponente Schutz vor Web-Bedrohungen bei der Link-Untersuchung die Datenbanken für Phishing-Webadressen verwendet.

   Zur Untersuchung von Links können Sie auch die Reputations-Datenbanken von Kaspersky Security Network verwenden.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Verwendung der heuristischen Analyse durch die Komponente Schutz vor Web-Bedrohungen

Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor Web-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor Web-Bedrohungen angezeigt.
3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor Web-Bedrohungen** wird geöffnet.
4. Wählen Sie die Registerkarte **Allgemein**.
5. Damit die Komponente Schutz vor Web-Bedrohungen die heuristische Analyse verwendet, wenn der Web-Datenverkehr auf Viren und andere Schadprogramme untersucht wird, aktivieren Sie im Abschnitt **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse zur Virenerkennung verwenden** und legen Sie mit dem Schieberegler die Stufe der heuristischen Analyse fest: **oberflächlich**, **mittel** oder **tief**.
6. Damit die Komponente Schutz vor Web-Bedrohungen die heuristische Analyse verwendet, wenn Webseiten auf Phishing-Links untersucht werden, aktivieren Sie im Abschnitt **Anti-Phishing-Einstellungen** das Kontrollkästchen **Heuristische Analyse zum Erkennen von Phishing-Links verwenden**.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Liste mit vertrauenswürdigen Webadressen erstellen

Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Webadressen anzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor Web-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor Web-Bedrohungen angezeigt.
3. Klicken Sie auf **Einstellungen**.

   Das Fenster **Schutz vor Web-Bedrohungen** wird geöffnet.
4. Wählen Sie die Registerkarte **Vertrauenswürdige Webadressen**.
5. Aktivieren Sie das Kontrollkästchen **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen**.
6. Erstellen Sie eine Liste mit Adressen der Websites / Webseiten, deren Inhalt Sie vertrauen. Um die Liste zu ergänzen, gehen Sie wie folgt vor:

a. Klicken Sie auf **Hinzufügen**.

Das Fenster **Webadresse / Maske für Webadresse** wird geöffnet.

b. Tragen Sie die Adresse einer Website / Webseite oder die Maske einer Website / Webseite ein.

c. Klicken Sie auf **OK**.

Der neue Eintrag erscheint in der Liste der vertrauenswürdigen Webadressen.

7. Klicken Sie auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz vor E-Mail-Bedrohungen

Diese Komponente ist verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Dateiserver installiert ist.

Dieser Abschnitt informiert über die Komponente Schutz vor E-Mail-Bedrohungen und erklärt die Einstellungen der Komponente.

Über den Schutz vor E-Mail-Bedrohungen

Die Komponente Schutz vor E-Mail-Bedrohungen untersucht, ob in ein- und ausgehenden E-Mail-Nachrichten Viren und andere bedrohliche Programme enthalten sind. Mail-Anti-Virus wird beim Start von Kaspersky Endpoint Security gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Nachrichten, die mit den Protokollen POP3, SMTP, IMAP, MAPI und NNTP empfangen oder gesendet werden. Werden in einer E-Mail-Nachricht keine Bedrohungen gefunden, so wird der Zugriff freigegeben und/oder die Nachricht wird verarbeitet.

Wenn in einer E-Mail-Nachricht eine Bedrohung gefunden wird, führt die Komponente Schutz vor E-Mail-Bedrohungen folgende Aktionen aus:

1. Die E-Mail-Nachricht erhält den Status *Infiziert*.

   Dieser Status wird einer E-Mail-Nachricht in folgenden Fällen zugewiesen:

   - Wenn bei der Untersuchung einer E-Mail-Nachricht der Codeabschnitt eines bekannten Virus gefunden wurde, über welchen Informationen in den Antiviren-Datenbanken von Kaspersky Endpoint Security vorliegen.

   - Wenn die E-Mail-Nachricht einen Codeabschnitt, der für Viren oder andere bedrohliche Programme typisch ist, oder den modifizierten Code eines bekannten Virus enthält.

2. Der Typ des Objekts, das in der E-Mail-Nachricht gefunden wurde, wird ermittelt (beispielsweise *trojanisches Programm*).

3. Die E-Mail-Nachricht wird blockiert.

4. Auf dem Bildschirm wird eine Benachrichtigung über das gefundene Objekt angezeigt (falls dies in den Benachrichtigungseinstellungen festgelegt ist).

5. Die Aktion, welche in den Einstellungen der Komponente Schutz vor E-Mail-Bedrohungen festgelegt ist, wird ausgeführt.

Diese Komponente interagiert mit den Mail-Clients, die auf dem Computer installiert sind. Für den Mail-Client Microsoft Office Outlook ist eine integrierbare Erweiterung vorgesehen, mit welcher die Nachrichtenuntersuchung genau angepasst werden kann. Die Erweiterung für die Komponente Schutz vor E-Mail-Bedrohungen wird bei der Installation von Kaspersky Endpoint Security in den Mail-Client Microsoft Office Outlook integriert.

Schutz vor E-Mail-Bedrohungen aktivieren und deaktivieren

Die Komponente Schutz vor E-Mail-Bedrohungen ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie die Komponente Schutz vor E-Mail-Bedrohungen deaktivieren.

Um die Komponente Schutz vor E-Mail-Bedrohungen zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor E-Mail-Bedrohungen** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor E-Mail-Bedrohungen angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Schutz vor E-Mail-Bedrohungen aktivieren**, um die Komponente Schutz vor E-Mail-Bedrohungen einzuschalten.

   - Deaktivieren Sie das Kontrollkästchen **Schutz vor E-Mail-Bedrohungen aktivieren**, um die Komponente Schutz vor E-Mail-Bedrohungen auszuschalten.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz vor E-Mail-Bedrohungen anpassen

Um die Komponente Schutz vor E-Mail-Bedrohungen anzupassen, können Sie folgende Aktionen ausführen:

- Ändern der Sicherheitsstufe für E-Mails

  Sie können eine der vordefinierten Sicherheitsstufen für den E-Mail-Schutz wählen oder die Einstellungen einer Sicherheitsstufe anpassen.

  Nachdem Sie die Einstellungen einer Sicherheitsstufe für den E-Mail-Schutz geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

- Ändern der Aktion, die Kaspersky Endpoint Security mit infizierten Nachrichten ausführen soll
- Schutzbereich für die Komponente Schutz vor E-Mail-Bedrohungen festlegen
- Anpassen der Untersuchung zusammengesetzter Dateien, die an E-Mail-Nachrichten angehängt sind

  Sie können die Untersuchung von Objekten, die an Nachrichten angehängt sind, aktivieren oder deaktivieren, und für zu untersuchende Objekte, die an Nachrichten angehängt sind, eine maximale Größe und eine maximale Untersuchungsdauer festlegen.
- Anpassen der Filterung nach dem Typ der Anhänge von E-Mail-Nachrichten

  Durch die Filterung nach dem Typ der Nachrichtenanhänge können Dateien bestimmter Typen automatisch umbenannt oder gelöscht werden.
- Verwendung der heuristischen Analyse anpassen

  Um einen effektiveren Schutz zu erhalten, können Sie die heuristische Analyse verwenden. Bei der heuristischen Analyse analysiert Kaspersky Endpoint Security die Aktivität, die Programme im Betriebssystem zeigen. Die heuristische Analyse kann in Nachrichten Bedrohungen erkennen, die noch nicht in den Datenbanken von Kaspersky Endpoint Security verzeichnet sind.
- Anpassen der Mailuntersuchung im Mailprogramm Microsoft Office Outlook

  Für den Mail-Client Microsoft Office Outlook ist eine integrierbare Erweiterung vorgesehen, mit der sich die E-Mail-Untersuchung bequem anpassen lässt.

  Bei der Arbeit mit anderen Mail-Clients (einschließlich Microsoft Outlook Express, Windows Mail und Mozilla Thunderbird) untersucht die Komponente Schutz vor E-Mail-Bedrohungen den Datenverkehr der E-Mail-Protokolle SMTP, POP3, IMAP und NNTP.

  > Bei der Verwendung des Mail-Clients Mozilla Thunderbird werden Nachrichten, die mit dem IMAP-Protokoll übertragen werden, von der Komponente Schutz vor E-Mail-Bedrohungen nicht auf Viren und andere bedrohliche Programme untersucht, wenn Filter verwendet werden, die Nachrichten aus dem Ordner **Posteingang** verschieben.

Sicherheitsstufe für E-Mails ändern

Die Komponente Schutz vor E-Mail-Bedrohungen bietet unterschiedliche Einstellungsvarianten für den E-Mail-Schutz. Diese Einstellungsvarianten heißen *Sicherheitsstufen für E-Mails*. Es gibt drei Stufen der E-Mail-Sicherheit: **Hoch**, **Empfohlen**, **Niedrig**. Die Sicherheitsstufe **Empfohlen** gilt für den E-Mail-Schutz als optimal und wird von den Kaspersky-Lab-Spezialisten empfohlen.

Gehen Sie folgendermaßen vor, um die Sicherheitsstufe für E-Mails zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor E-Mail-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor E-Mail-Bedrohungen angezeigt.
3. Führen Sie unter **Sicherheitsstufe** eine der folgenden Aktionen aus:

- Verwenden Sie den Schieberegler, um eine vordefinierte E-Mail-Sicherheitsstufe zu wählen (**Hoch**, **Empfohlen**, **Niedrig**).

- Wenn Sie die E-Mail-Sicherheitsstufe anpassen möchten, klicken Sie auf **Einstellungen** und nehmen Sie im folgenden Fenster **Schutz vor E-Mail-Bedrohungen** die entsprechenden Einstellungen vor.

  Nachdem Sie die Einstellungen einer E-Mail-Sicherheitsstufe geändert haben, ändert sich der Name der E-Mail-Sicherheitsstufe im Block **Sicherheitsstufe** in **Benutzerdefiniert**.

- Klicken Sie auf **Standard**, um eine benutzerdefinierte Sicherheitsstufe für den E-Mail-Schutz auf die Sicherheitsstufe **Empfohlen** zurückzusetzen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktion für infizierte E-Mail-Nachrichten ändern

Die Komponente Schutz vor E-Mail-Bedrohungen versucht standardmäßig, alle gefundenen infizierten E-Mail-Nachrichten automatisch zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden infizierte E-Mail-Nachrichten von der Komponente „Schutz vor E-Mail-Bedrohungen“ gelöscht.

Um die Aktion für infizierte E-Mail-Nachrichten zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor E-Mail-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor E-Mail-Bedrohungen angezeigt.

3. Wählen Sie im Abschnitt **Aktion beim Fund einer Bedrohung** eine Aktion, die Kaspersky Endpoint Security beim Fund einer infizierten Nachricht ausführen soll:

   - **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**.

     Wenn diese Variante ausgewählt ist, versucht die Komponente „Schutz vor E-Mail-Bedrohungen“ automatisch, alle gefundenen infizierten E-Mail-Nachrichten zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden infizierte E-Mail-Nachrichten von der Komponente „Schutz vor E-Mail-Bedrohungen“ gelöscht.

   - **Desinfizieren. Blockieren, wenn Desinfektion nicht möglich**.

     Wenn diese Variante ausgewählt ist, versucht die Komponente „Schutz vor E-Mail-Bedrohungen“ automatisch, alle gefundenen infizierten E-Mail-Nachrichten zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden infizierte E-Mail-Nachrichten von der Komponente „Schutz vor E-Mail-Bedrohungen“ blockiert.

   - **Blockieren**.

     Wenn diese Variante ausgewählt ist, blockiert die Komponente „Schutz vor E-Mail-Bedrohungen“ die infizierten E-Mail-Nachrichten automatisch, ohne einen Desinfektionsversuch zu unternehmen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutzbereich für die Komponente Schutz vor E-Mail-Bedrohungen

Ein Schutzbereich sind die Objekte, die von einer Komponente während der Ausführung untersucht werden. Der Schutzbereich besitzt je nach Komponente unterschiedliche Eigenschaften. Der Schutzbereich für die Komponente Schutz vor E-Mail-Bedrohungen wird durch folgende Eigenschaften definiert: Einstellungen für die Integration der Komponente Schutz vor E-Mail-Bedrohungen in die Mail-Clients, Typ der E-Mail-Nachrichten und der E-Mail-Protokolle, deren Datenverkehr von der Komponente Schutz vor E-Mail-Bedrohungen untersucht wird. Kaspersky Endpoint Security untersucht standardmäßig ein- und ausgehende E-Mail-Nachrichten sowie den Datenverkehr der Mailprotokolle POP3, SMTP, NNTP und IMAP und wird in den Mail-Client Microsoft Office Outlook integriert.

Um den Schutzbereich für die Komponente Schutz vor E-Mail-Bedrohungen zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor E-Mail-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor E-Mail-Bedrohungen angezeigt.

3. Klicken Sie auf **Einstellungen**.

   Das Fenster **Schutz vor E-Mail-Bedrohungen** wird geöffnet.

4. Wählen Sie die Registerkarte **Allgemein**.

5. Führen Sie im Abschnitt **Schutzbereich** eine der folgenden Aktionen aus:

   - Wählen Sie die Variante **Eingehende und ausgehende Nachrichten**, damit die Komponente Schutz vor E-Mail-Bedrohungen alle auf Ihrem Computer ein- und ausgehenden Nachrichten untersucht.

   - Wählen Sie die Variante **Nur eingehende Nachrichten**, damit Komponente Schutz vor E-Mail-Bedrohungen nur die auf Ihrem Computer eingehenden Nachrichten untersucht.

     Wenn Sie nur die Untersuchung eingehender Nachrichten wählen, wird empfohlen, eine einmalige Untersuchung aller ausgehenden Nachrichten vorzunehmen, da sich auf Ihrem Computer Mail-Würmer befinden können, die sich mithilfe von E-Mails ausbreiten. Dadurch lassen sich Probleme vermeiden, die durch unkontrolliertes Versenden infizierter Nachrichten von Ihrem Computer auftreten können.

6. Führen Sie im Abschnitt **Integration ins System** folgende Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **Datenverkehr für POP3/SMTP/NNTP/IMAP**, damit die Komponente Schutz vor E-Mail-Bedrohungen die Nachrichten untersucht, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden. Die Untersuchung erfolgt, bevor die Nachrichten auf den Benutzercomputer heruntergeladen werden.

Deaktivieren Sie das Kontrollkästchen **Datenverkehr für POP3/SMTP/NNTP/IMAP**, damit die Komponente Schutz vor E-Mail-Bedrohungen die Nachrichten, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden, nicht vor dem Eingang auf dem Benutzercomputer untersucht. In diesem Fall werden die Nachrichten von der Erweiterung der Komponente Schutz vor E-Mail-Bedrohungen untersucht, die in den Mail-Client Microsoft Office Outlook integriert ist, wenn das Kontrollkästchen **Zusätzlich: Erweiterung für Microsoft Office Outlook** aktiviert ist. Die Untersuchung erfolgt, nachdem die Nachrichten auf den Benutzercomputer heruntergeladen wurden.

> Wenn Sie einen anderen Mail-Client als Microsoft Office Outlook verwenden und das Kontrollkästchen **Datenverkehr für POP3/SMTP/NNTP/IMAP** deaktiviert ist, werden die Nachrichten, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden, nicht von der Komponente Schutz vor E-Mail-Bedrohungen untersucht.

- Aktivieren Sie das Kontrollkästchen **Zusätzlich: Erweiterung für Microsoft Office Outlook**, um den Zugriff auf die Einstellungen für die Komponente Schutz vor E-Mail-Bedrohungen aus dem Programm Microsoft Office Outlook zu ermöglichen und die Untersuchung von Nachrichten zu aktivieren, die mit den Protokollen POP3, SMTP, NNTP, IMAP und MAPI übertragen werden. Diese Untersuchung erfolgt mithilfe der Erweiterung, die in das Programm Microsoft Office Outlook integriert ist, und wird ausgeführt, nachdem die Nachrichten auf den Benutzercomputer heruntergeladen wurden.

  Deaktivieren Sie das Kontrollkästchen **Zusätzlich: Erweiterung für Microsoft Office Outlook**, um den Zugriff auf die Einstellungen für die Komponente Schutz vor E-Mail-Bedrohungen aus dem Programm Microsoft Office Outlook zu untersagen und die Untersuchung von Nachrichten zu deaktivieren, die mit den Protokollen POP3, SMTP, NNTP, IMAP und MAPI übertragen werden. Diese Option bezieht sich auf die Untersuchung mithilfe der Erweiterung, die in das Programm Microsoft Office Outlook integriert ist, und ausgeführt werden kann, nachdem die Nachrichten auf den Benutzercomputer heruntergeladen wurden.

  > Die Erweiterung für die Komponente Schutz vor E-Mail-Bedrohungen wird bei der Installation von Kaspersky Endpoint Security in den Mail-Client Microsoft Office Outlook integriert.

7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Untersuchung zusammengesetzter Dateien, die an E-Mail-Nachrichten angehängt sind

Um die Untersuchung von zusammengesetzten Dateien anzupassen, die an E-Mail-Nachrichten angehängt sind, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor E-Mail-Bedrohungen**.

Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor E-Mail-Bedrohungen angezeigt.

3. Klicken Sie auf **Einstellungen**.

   Das Fenster **Schutz vor E-Mail-Bedrohungen** wird geöffnet.

4. Wählen Sie die Registerkarte **Allgemein**.

5. Führen Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** folgende Aktionen aus:

   - Deaktivieren Sie das Kontrollkästchen **Angehängte Archive untersuchen**, damit die Komponente Schutz vor E-Mail-Bedrohungen die an Nachrichten angehängten Archive nicht untersucht.
   - Deaktivieren Sie das Kontrollkästchen **Angehängte Office-Format-Dateien untersuchen**, damit die Komponente Schutz vor E-Mail-Bedrohungen die an Nachrichten angehängten Office-Format-Dateien nicht untersucht.
   - Aktivieren Sie das Kontrollkästchen **Archive nicht untersuchen, wenn größer als n MB**, damit die Komponente Schutz vor E-Mail-Bedrohungen die an Nachrichten angehängten Archive nicht untersucht, die größer sind als n MB. Wenn Sie dieses Kontrollkästchen aktiviert haben, geben Sie im entsprechenden Feld eine maximale Archivgröße an.
   - Deaktivieren Sie das Kontrollkästchen **Archive untersuchen für höchstens n Sek.**, damit die Komponente Schutz vor E-Mail-Bedrohungen die an Nachrichten angehängten Archive untersucht, falls die Untersuchung länger dauert als n Sekunden.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Anlagenfilterung in E-Mail-Nachrichten

Die Funktionalität der Anlagenfilterung wird für ausgehende E-Mail-Nachrichten nicht angewendet.

Schädliche Programme können sich in Form von den Anlagen für E-Mail-Nachrichten verbreiten. Sie können eine Filterung nach dem Typ der Nachrichtenanhänge einrichten, damit Dateien der festgelegten Typen automatisch umbenannt oder gelöscht werden. Durch das Umbenennen bestimmter Typen kann Kaspersky Endpoint Security Ihren Computer vor dem automatischen Start von schädlichen Programmen schützen.

Gehen Sie folgendermaßen vor, um die Anlagenfilterung anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor E-Mail-Bedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor E-Mail-Bedrohungen angezeigt.

3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor E-Mail-Bedrohungen** wird geöffnet.

4. Wählen Sie im Fenster **Schutz vor E-Mail-Bedrohungen** die Registerkarte **Anlagenfilterung**.

5. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie die Variante **Filter nicht anwenden**, damit die Komponente Schutz vor E-Mail-Bedrohungen Nachrichtenanhänge nicht filtert.

   - Wählen Sie die Variante **Anhänge der ausgewählten Typen umbenennen**, damit die Komponente Schutz vor E-Mail-Bedrohungen die an Nachrichten angehängten Dateien der angegebenen Typen umbenennt.

     > Beachten Sie, dass das tatsächliche Format einer Datei von dem Format abweichen kann, das die Dateierweiterung angibt.

     Wenn Sie die Anlagenfilterung für E-Mail-Nachrichten aktiviert haben, kann die Komponente Schutz vor E-Mail-Bedrohungen bei der Filterung Dateien mit folgenden Erweiterungen umbenennen oder löschen:

     com – ausführbare Programmdatei mit einer Größe von maximal 64 KB

     exe – ausführbare Datei, selbstextrahierendes Archiv

     sys – Systemdatei von Microsoft Windows

     prg – Text des Programms dBase, Clipper oder Microsoft Visual FoxPro, Programm des Pakets WAVmaker

     bin – Binärdatei

     bat – Batchdatei

     cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2

     dpl – komprimierte Bibliothek für Borland Delphi

     dll – Dynamic Link Library

     scr – Bildschirmschonerdatei für Microsoft Windows

     cpl – Systemsteuerungsmodul (control panel) für Microsoft Windows

     ocx – Microsoft OLE-Objekt (Object Linking and Embedding)

     tsp – Programm, das im Timesharing-Modus arbeitet

     drv – Gerätetreiber

vxd – Treiber für ein virtuelles Microsoft Windows-Gerät

pif – Datei mit Programminformationen

lnk – Linkdatei für Microsoft Windows

reg – Registrierungsschlüsseldatei für Systemregistrierung von Microsoft Windows

ini – Konfigurationsdatei, die Einstellungsdaten für Microsoft Windows, Windows NT und andere Programme enthält

cla – Java-Klasse

vbs – Visual Basic-Skript

vbe – BIOS-Video-Erweiterung

js, jse – JavaScript-Quelltext

htm – Hypertext-Dokument

htt – Hypertext-Dokumentvorlage für Microsoft Windows

hta – Hypertext-Programm für Microsoft Internet Explorer

asp – Active Server Pages-Skript

chm – kompilierte HTML-Datei

pht – HTML-Datei mit eingebetteten PHP-Skripten

php – Skript, das in eine HTML-Datei eingebettet wird

wsh – Datei für Microsoft Windows Script Host

wsf – Skript von Microsoft Windows

the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95

hlp – Hilfedatei im Format Win Help

eml – E-Mail-Nachricht für Microsoft Outlook Express

nws – neue E-Mail-Nachricht für Microsoft Outlook Express

msg – E-Mail-Nachricht für Microsoft Mail

plg – E-Mail-Nachricht

mbx – gespeicherte E-Mail-Nachricht für Microsoft Office Outlook

doc* – Dokumente für Microsoft Office Word, z.B.: doc – Dokumente für Microsoft Office Word, docx – Dokument für Microsoft Office Word 2007 mit XML-Unterstützung, docm – Dokument für Microsoft Office Word 2007 mit Makro-Unterstützung

dot* – Dokumentvorlagen in Microsoft Office Word, z.B. dot – Dokumentvorlage in Microsoft Office Word, dotx – Dokumentvorlage in Microsoft Office Word 2007, dotm – Dokumentvorlage in Microsoft Office Word 2007 mit Makrounterstützung.

fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro

rtf – Rich Text Format-Dokument

shs – Datenauszug für Windows Shell Scrap Object Handler

dwg – Datenbank für AutoCAD-Skizzen

msi – Microsoft Windows Installer-Paket

otm – VBA-Projekt für Microsoft Office Outlook.

pdf – Dokument für Adobe Acrobat

swf – Objekt für Shockwave Flash

jpg, jpeg – komprimierte Bilddatei

emf – Enhanced Metafile Folgegeneration einer Metadatei des Betriebssystems Microsoft Windows. EMF-Dateien werden von 16-Bit-Versionen von Microsoft Windows nicht unterstützt.

ico – Symboldatei für ein Objekt

ov? – ausführbare Dateien für Microsoft Office Word

xl* – Dokumente und Dateien für Microsoft Office Excel, z.B.: xla – Erweiterung für Microsoft Office Excel, xlc – Diagramm, xlt – Dokumentvorlage, xlsx – Arbeitsblatt für Microsoft Office Excel 2007, xltm – Arbeitsblatt für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlsb – Arbeitsblatt für Microsoft Office Excel 2007 im Binärformat (nicht XML), xltx – Vorlage für Microsoft Office Excel 2007, xlsm – Vorlage für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlam – Konfigurationsdatei für Microsoft Office Excel 2007 mit Makro-Unterstützung.

pp* – Dokumente und Dateien für Microsoft Office PowerPoint, z.B.: pps – Folie für Microsoft Office PowerPoint, ppt – Präsentation, pptx – Präsentation für Microsoft Office PowerPoint 2007, pptm – Präsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, potx – Präsentationsvorlage für Microsoft Office PowerPoint 2007, potm – Präsentationsvorlage für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppsx – Folienpräsentation für Microsoft Office PowerPoint 2007, ppsm – Folienpräsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppam – Konfigurationsdatei für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

md* – Dokumente und Dateien für Microsoft Office Access, z.B.: mda – Arbeitsgruppe für Microsoft Office Access, mdb – Datenbank.

sldx – Folie in Microsoft Office PowerPoint 2007

sldm – Folie in Microsoft Office PowerPoint 2007 mit Makrounterstützung

thmx – Thema in Microsoft Office 2007

- Wählen Sie die Variante **Anhänge der ausgewählten Typen löschen**, damit die Komponente Schutz vor E-Mail-Bedrohungen die an Nachrichten angehängten Dateien der angegebenen Typen löscht.

6. Wenn Sie beim vorherigen Schritt der Anleitung die Variante **Anhänge der ausgewählten Typen umbenennen** oder die Variante **Anhänge der ausgewählten Typen löschen** gewählt haben, aktivieren Sie die Kontrollkästchen für die erforderlichen Dateitypen.

   Die Liste der Dateitypen kann mit den Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** bearbeitet werden.

7. Klicken Sie auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

E-Mail-Untersuchung in Microsoft Office Outlook

Bei der Installation von Kaspersky Endpoint Security wird eine Erweiterung für die Komponente Schutz vor E-Mail-Bedrohungen in das Programm Microsoft Office Outlook (im Folgenden "Outlook" genannt) integriert. Sie erlaubt es, aus dem Programm Outlook zu den Einstellungen für die Komponente Schutz vor E-Mail-Bedrohungen zu wechseln und festzulegen, zu welchem Zeitpunkt E-Mail-Nachrichten auf Viren und andere bedrohliche Programme untersucht werden sollen. Die Outlook-Erweiterung für die Komponente Schutz vor E-Mail-Bedrohungen kann ein- und ausgehende E-Mail-Nachrichten untersuchen, die mit den Protokollen POP3, SMTP, NNTP, IMAP und MAPI übertragen werden.

Die Komponente Schutz vor E-Mail-Bedrohungen kann von dem Programm Outlook aus angepasst werden, wenn auf der Programmoberfläche von Kaspersky Endpoint Security das Kontrollkästchen **Zusätzlich: Erweiterung für Microsoft Office Outlook** aktiviert ist.

Im Programm Outlook werden eingehende E-Mail-Nachrichten zuerst von der Komponente Schutz vor E-Mail-Bedrohungen untersucht (wenn auf der Programmoberfläche von Kaspersky Endpoint Security das Kontrollkästchen **Datenverkehr für POP3/SMTP/NNTP/IMAP** aktiviert ist). Anschließend werden eingehende E-Mail-Nachrichten von der Outlook-Erweiterung für die Komponente Schutz vor E-Mail-Bedrohungen gescannt. Findet die Komponente Schutz vor E-Mail-Bedrohungen in einer E-Mail-Nachricht ein schädliches Objekt, so werden Sie darüber informiert.

Ausgehende Nachrichten werden zuerst von der Outlook-Erweiterung für die Komponente Schutz vor E-Mail-Bedrohungen untersucht und anschließend von der Komponente Schutz vor E-Mail-Bedrohungen

gescannt.

E-Mail-Untersuchung im Programm Outlook anpassen

Um die E-Mail-Untersuchung im Programm Outlook 2007 anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Hauptfenster von Outlook 2007.
2. Wählen Sie im Programmmenü den Punkt **Extras** → **Optionen**.

   Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie im Fenster **Einstellungen** die Registerkarte **E-Mail-Schutz**.

Um zu den Einstellungen für die E-Mail-Untersuchung im Programm Outlook 2010 / 2013 / 2016 zu wechseln, gehen Sie wie folgt vor:

1. Öffnen Sie das Hauptfenster von Outlook.

   Öffnen Sie oben links die Registerkarte **Datei**.
2. Klicken Sie auf **Optionen**.

   Das Fenster **Outlook-Optionen** wird geöffnet.
3. Wählen Sie den Abschnitt **Add-ins** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Plug-ins angezeigt, die in Outlook integriert sind.
4. Klicken Sie auf **Add-in-Optionen**.

E-Mail-Untersuchung mithilfe von Kaspersky Security Center anpassen

Wenn die E-Mail-Untersuchung mithilfe der Erweiterung der Komponente „Schutz vor E-Mail-Bedrohungen" für Outlook erfolgt, wird empfohlen, den Cache-Modus für den Exchange-Server zu verwenden (Use Cached Exchange Mode). Ausführliche Informationen über den Exchange-Cache-Modus und Tipps zu seiner Verwendung finden Sie in der Microsoft-Wissensdatenbank: https://technet.microsoft.com/de-de/library/cc179175.aspx .

Um den Modus der Outlook-Erweiterung für den Schutz vor E-Mail-Bedrohungen mithilfe von Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die E-Mail-Untersuchung anpassen möchten.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Wählen Sie die gewünschte Richtlinie aus.

5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:

   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

6. Wählen Sie im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor E-Mail-Bedrohungen**.

7. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster **Schutz vor E-Mail-Bedrohungen** wird geöffnet.

8. Klicken Sie im Abschnitt **Integration ins System** auf **Einstellungen**.

   Das Fenster **E-Mail-Schutz** wird geöffnet.

9. Gehen Sie im Fenster **E-Mail-Schutz** wie folgt vor:

   - Aktivieren Sie das Kontrollkästchen **Beim Empfang untersuchen**, damit die Outlook-Erweiterung für die Komponente Schutz vor E-Mail-Bedrohungen die eingehenden Nachrichten untersucht, wenn sie im E-Mail-Postfach eintreffen.
   - Aktivieren Sie das Kontrollkästchen **Beim Lesen untersuchen**, damit die Outlook-Erweiterung für die Komponente Schutz vor E-Mail-Bedrohungen die eingehenden Nachrichten untersucht, wenn der Benutzer sie zum Lesen öffnen möchte.
   - Aktivieren Sie das Kontrollkästchen **Beim Senden untersuchen**, damit die Outlook-Erweiterung für die Komponente Schutz vor E-Mail-Bedrohungen die ausgehenden Nachrichten beim Senden untersucht.

10. Klicken Sie im Fenster **E-Mail-Schutz** auf **OK**.

11. Klicken Sie im Fenster **Schutz vor E-Mail-Bedrohungen** auf **OK**.

12. Wenden Sie die Richtlinie an.

    Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Schutz vor Netzwerkbedrohungen

Dieser Abschnitt informiert über den Schutz vor Netzwerkbedrohungen und erklärt die Einstellungen der Komponente.

Über den Schutz vor Netzwerkbedrohungen

Die Komponente Schutz vor Netzwerkbedrohungen überwacht den eingehenden Netzwerkverkehr auf Aktivität, die für Netzwerkangriffe typisch ist. Wenn Kaspersky Endpoint Security einen Angriff auf den Computer erkennt, sperrt das Programm die Netzwerkaktivität des angreifenden Computers. Hiernach erscheint auf dem Bildschirm eine Meldung über den Angriffsversuch mit Informationen über den angreifenden Computer.

Die Netzwerkaktivität des angreifenden Computers wird für eine Stunde blockiert. Sie können die Einstellungen für das Blockieren des angreifenden Computers ändern.

Beschreibungen der derzeit bekannten Arten von Netzwerkangriffen und entsprechende Abwehrmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. Die Liste der Netzwerkangriffe, die von der Komponente Schutz vor Netzwerkbedrohungen erkannt werden, wird beim Update der Datenbanken und Programm-Module aktualisiert.

Schutz vor Netzwerkbedrohungen aktivieren und deaktivieren

Der Schutz vor Netzwerkbedrohungen ist standardmäßig aktiviert und läuft im optimalen Modus. Bei Bedarf können Sie den Schutz vor Netzwerkbedrohungen deaktivieren.

Um den Schutz vor Netzwerkbedrohungen zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor Netzwerkbedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor Netzwerkbedrohungen angezeigt.
3. Gehen Sie wie folgt vor:
   - Aktivieren Sie das Kontrollkästchen **Schutz vor Netzwerkbedrohungen aktivieren**, um den Schutz vor Netzwerkbedrohungen einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Schutz vor Netzwerkbedrohungen aktivieren**, um den Schutz vor Netzwerkbedrohungen auszuschalten.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schutz vor Netzwerkbedrohungen anpassen

Um den Schutz vor Netzwerkbedrohungen anzupassen, können Sie folgende Aktionen ausführen:

- Einstellungen für das Blockieren eines angreifenden Computers anpassen
- Liste mit Adressen erstellen, die bei der Sperrung als Ausnahmen gelten sollen

Einstellungen für das Blockieren eines angreifenden Computers ändern

Gehen Sie folgendermaßen vor, um die Einstellungen für das Blockieren eines angreifenden Computers zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor Netzwerkbedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor Netzwerkbedrohungen angezeigt.

3. Aktivieren Sie das Kontrollkästchen **Angreifenden Computer zur Sperrliste hinzufügen für**.

   Wenn dieses Kontrollkästchen aktiviert ist, blockiert der Schutz vor Netzwerkbedrohungen beim Erkennen eines versuchten Netzwerkangriffs die Netzwerkaktivität des angreifenden Computers für einen bestimmten Zeitraum. Dadurch wird der Computer automatisch vor weiteren Netzwerkangriffen geschützt, die von dieser Adresse ausgehen.

   Ist das Kontrollkästchen deaktiviert, so aktiviert der Schutz vor Netzwerkbedrohungen beim Erkennen eines versuchten Netzwerkangriffs den automatischen Schutz vor weiteren Netzwerkangriffen von dieser Adresse nicht.

4. Sie können die Zeit, für die ein angreifender Computer blockiert werden soll, im Feld rechts vom Kontrollkästchen **Angreifenden Computer zur Sperrliste hinzufügen für** ändern.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Adressen anpassen, die bei der Sperrung als Ausnahmen gelten sollen

Um Adressen anzupassen, die bei der Sperrung als Ausnahmen gelten sollen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor Netzwerkbedrohungen**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Schutz vor Netzwerkbedrohungen angezeigt.

3. Klicken Sie auf **Ausnahmen**.

   Das Fenster **Ausnahmen** wird geöffnet.

4. Führen Sie eine der folgenden Aktionen aus:

   - Um eine neue IP-Adresse hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um eine früher hinzugefügte IP-Adresse zu ändern, wählen Sie in der Liste der Adressen eine IP-Adresse und klicken Sie auf **Ändern**.

   Das Fenster **IP-Adresse** wird geöffnet.

5. Geben Sie die IP-Adresse des Computers ein, der blockiert werden soll, wenn Netzwerkangriffe von ihm ausgehen.

6. Klicken Sie im Fenster **IP-Adresse** auf **OK**.

7. Klicken Sie im Fenster **Ausnahmen** auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Firewall

Dieser Abschnitt informiert über die Funktionen der Firewall und erklärt die Einstellungen der Komponente.

Über die Firewall

Bei der Arbeit in lokalen Netzwerken und im Internet besteht für einen Computer nicht nur das Risiko einer Infektion durch Viren und andere Schadprogramme, sondern auch eine Gefahr durch unterschiedliche Arten von Angriffen, die Schwachstellen des Betriebssystems und der Software ausnutzen.

Die Firewall gewährleistet den Schutz der persönlichen Daten, die auf dem Benutzercomputer gespeichert sind. Während eine Verbindung zum Internet oder zum lokalen Netzwerk besteht, werden die meisten Bedrohungen blockiert, die das Betriebssystem gefährden können. Die Firewall erkennt auf einem Benutzercomputer alle Netzwerkverbindungen und erstellt eine Liste mit IP-Adressen und standardmäßigen Statusvarianten der Netzwerkverbindungen.

Die Komponente Firewall filtert die gesamte Netzwerkaktivität in Übereinstimmung mit den Netzwerkregeln. Mithilfe der Netzwerkregeln lässt sich der Computerschutz flexibel anpassen: von einer vollständigen Sperrung des Internetzugriffs für alle Programme bis zur Erlaubnis des unbegrenzten Zugriffs.

Firewall aktivieren und deaktivieren

Die Firewall ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf können Sie die Firewall deaktivieren.

Um die Firewall zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Firewall angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Firewall aktivieren**, um die Firewall einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Firewall aktivieren**, um die Firewall auszuschalten.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Über Netzwerkregeln

Eine *Netzwerkregel* besteht aus einer Erlaubnis- oder Verbotsaktion, die von der Firewall ausgeführt wird, wenn sie den Versuch erkennt, eine Netzwerkverbindung herzustellen.

Die Firewall führt den Schutz vor Netzwerkangriffen auf Netzwerkebene und auf Anwendungsebene aus. Der Schutz auf Netzwerkebene beruht auf Regeln für Netzwerkpakete. Der Schutz auf Anwendungsebene beruht auf Regeln für die Verwendung von Netzwerkressourcen durch die auf dem Benutzercomputer installierten Programme.

Auf Basis der beiden Firewall-Schutzebenen können Sie folgende Regeln anpassen:

- *Netzwerkregeln für Pakete*. Sie dienen zur Definition von Beschränkungen für die Netzwerkpakete, wobei das Programm keine Rolle spielt. Diese Regeln beschränken die ein- und ausgehende Netzwerkaktivität anhand bestimmter Ports für ausgewählte Datenübertragungsprotokolle. Die Firewall gibt eine Standardauswahl von Netzwerkregeln für Pakete vor.

- *Netzwerkregeln für Programme*. Sie dienen zur Definition von Beschränkungen der Netzwerkaktivität eines konkreten Programms. Dabei werden nicht nur die Merkmale des Netzwerkpakets berücksichtigt, sondern auch das konkrete Programm, an das dieses Netzwerkpaket adressiert ist oder welches das Senden dieses Netzwerkpakets initiiert hat. Mithilfe solcher Regeln können Sie die Filterung der Netzwerkaktivität genau anpassen, wenn beispielsweise ein bestimmter Typ von Netzwerkverbindungen für konkrete Programme verboten, für andere aber erlaubt werden soll.

Netzwerkregeln für Pakete besitzen eine höhere Priorität als Netzwerkregeln für Programme. Sind für eine Art der Netzwerkaktivität gleichzeitig Netzwerkregeln für Pakete und Netzwerkregeln für Programme vorhanden, wird diese Netzwerkaktivität nach denNetzwerkregeln für Pakete verarbeitet.

Sie können jeder Netzwerkregel für Pakete und Netzwerkregel für Programme eine Ausführungspriorität zuweisen.

Über die Statusvarianten der Netzwerkverbindung

Die Firewall kontrolliert alle Netzwerkverbindungen auf dem Benutzercomputer und weist jeder gefundenen Netzwerkverbindung automatisch einen Status zu.

Für eine Netzwerkverbindung sind folgende Statusvarianten vorgesehen:

- **Öffentliches Netzwerk**. Dieser Status ist für Netzwerke vorgesehen, die nicht durch Antiviren-Programme, Firewalls, Filter usw. geschützt werden (z. B. für Netzwerke in Internet-Cafés). Für den Benutzer eines Computers, der mit einem solchen Netzwerk verbunden ist, blockiert die Firewall den Zugriff auf die Dateien und Drucker dieses Computers. Auch Drittnutzer erhalten über gemeinsame Ordner oder Fernzugriff keinen Zugang zu Informationen auf dem Desktop Ihres Computers. Die Firewall filtert die Netzwerkaktivität für jedes Programm nach den für dieses Programm vorhandenen Netzwerkregeln.

  Das Internet erhält von der Firewall standardmäßig den Status *Öffentliches Netzwerk*. Der Status des Internets kann nicht geändert werden.

- **Lokales Netzwerk**. Dieser Status ist für Netzwerke vorgesehen, deren Benutzern Sie den Zugriff auf die Dateien und Drucker Ihres Computers gewähren möchten (beispielsweise für interne Firmennetzwerke oder private Netzwerke).

- **Vertrauenswürdiges Netzwerk**. Dieser Status ist für ein sicheres Netzwerk vorgesehen, in dem einem Computer keine Angriffe und unerlaubte Zugriffsversuche auf Daten drohen. Für Netzwerke mit diesem Status erlaubt die Firewall im Rahmen dieses Netzwerks jede beliebige Netzwerkaktivität.

Status einer Netzwerkverbindung ändern

Gehen Sie folgendermaßen vor, um den Status einer Netzwerkverbindung zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Firewall angezeigt.
3. Klicken Sie auf **Verfügbare Netzwerke**.

   Das Fenster **Firewall** wird geöffnet.
4. Wählen Sie die Netzwerkverbindung, deren Status Sie ändern möchten.
5. Wählen Sie im Kontextmenü Status der Netzwerkverbindung aus:
   - **Öffentliches Netzwerk**.
   - **Lokales Netzwerk**.
   - **Vertrauenswürdiges Netzwerk**.
6. Klicken Sie im Fenster **Firewall** auf **OK**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Arbeit mit Netzwerkregeln für Pakete

Bei der Arbeit mit Netzwerkregeln für Pakete können Sie folgende Aktionen ausführen:

- Erstellen einer neuen Netzwerkregel für Pakete

  Sie können eine neue Netzwerkregel für Pakete erstellen. Dazu wird eine Kombination von Bedingungen und Aktionen für Netzwerkpakete und Datenströme festgelegt.
- Aktivieren und Deaktivieren einer Netzwerkregel für Pakete

  Alle Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt werden, besitzen den Status *Aktiv*. Ist eine Netzwerkregel für Pakete aktiviert, wendet die Firewall diese Regel an.

  Sie können eine beliebige Netzwerkregel für Pakete deaktivieren, die auf der Liste der Netzwerkregeln für Pakete steht. Ist eine Netzwerkregel für Pakete deaktiviert, wird diese Regel vorübergehend nicht von der Firewall verwendet.

  > Eine neue Netzwerkregel für Pakete, die vom Benutzer erstellt wurde, wird standardmäßig mit dem Status *Aktiv* zur Liste Netzwerkregeln für Pakete hinzugefügt.

- Ändern der Einstellungen einer vorhandenen Netzwerkregel für Pakete

  Nach Erstellung einer neuen Netzwerkregel für Pakete können Sie ihre Einstellungen jederzeit ändern.

- Ändern der Firewall-Aktion für eine Netzwerkregel für Pakete

  In derListe der Netzwerkregeln für Pakete können Sie die Aktion ändern, die von der Firewall ausgeführt wird, wenn eine Netzwerkaktivität erkannt wird, die der angegebenen Netzwerkregel für Pakete entspricht.

- Ändern der Priorität einer Netzwerkregel für Pakete

  Sie können die Priorität einer in der Liste markierten Netzwerkregel für Pakete ändern.

- Löschen einer Netzwerkregel für Pakete

  Sie können eine Netzwerkregel für Pakete löschen, wenn Sie nicht möchten, dass diese Regel beim Fund einer Netzwerkaktivität von der Firewall angewendet wird und dass die Regel mit dem Status *Deaktiviert* in der Liste der Netzwerkregeln für Pakete erscheint.

Netzwerkregel für Pakete erstellen und ändern

Bei der Erstellung von Netzwerkregeln für Pakete ist zu beachten, dass diesen Vorrang vor den Netzwerkregeln für Programme eingeräumt wird.

Gehen Sie folgendermaßen vor, um eine Netzwerkregel für Pakete zu erstellen oder zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.
3. Klicken Sie auf **Netzwerkregeln für Pakete**.
4. Das Fenster **Firewall** wird auf der Registerkarte **Netzwerkregeln für Pakete** geöffnet.

   Diese Registerkarte bietet eine Liste mit Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt wurden.
5. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf **Hinzufügen**, um eine neue Netzwerkregel für Pakete zu erstellen.
   - Wählen Sie aus der Liste der Netzwerkregeln für Pakete eine Regel und klicken Sie auf **Ändern**, um sie zu ändern.

   Das Fenster **Netzwerkregel** wird geöffnet.
6. Wählen Sie in der Dropdown-Liste **Aktion** die Aktion aus, welche die Firewall bei Erkennen der entsprechenden Art von Netzwerkaktivität ausführen soll:

   - **Erlauben**.

- **Verbieten**.
- **Nach Regeln des Programms**.

7. Geben Sie im Feld **Name** den Namen eines Netzwerkdienstes an. Dafür gibt es folgende Methoden:
   - Klicken Sie auf das Symbol , das sich rechts vom Feld **Name** befindet, und wählen Sie in der Dropdown-Liste den Namen eines Netzwerkdienstes.

     Die Dropdown-Liste enthält die Netzwerkdienste, welche die am häufigsten verwendeten Netzwerkverbindungen beschreiben.
   - Tragen Sie im Feld **Name** manuell den Namen eines Netzwerkdienstes ein.
8. Geben Sie ein Datenübertragungsprotokoll an:
   a. Aktivieren Sie das Kontrollkästchen **Protokoll**.
   b. Wählen Sie in der Dropdown-Liste den Protokolltyp aus, dessen Netzwerkaktivität kontrolliert werden soll.

      Die Firewall kontrolliert Verbindungen der Protokolle TCP, UDP, ICMP, ICMPv6, IGMP und GRE.

      Wenn in der Dropdown-Liste **Name** ein Netzwerkdienst gewählt ist, wird automatisch das Kontrollkästchen **Protokoll** aktiviert und in der Dropdown-Liste neben dem Kontrollkästchen wird der Protokolltyp gewählt, der dem gewählten Netzwerkdienst entspricht. Das Kontrollkästchen **Protokoll** ist standardmäßig deaktiviert.
9. Wählen Sie in der Dropdown-Liste **Richtung** eine Richtung für die zu kontrollierende Netzwerkaktivität.

   Die Firewall kontrolliert Netzwerkverbindungen mit folgenden Richtungen:
   - **Eingehend (Paket)**.
   - **Eingehend**.
   - **Eingehend / Ausgehend**.
   - **Ausgehend (Paket)**.
   - **Ausgehend**.
10. Wurde ICMP oder ICMPv6 als Protokoll gewählt, können Sie Typ und Code des ICMP-Pakets festlegen:
    a. Aktivieren Sie das Kontrollkästchen **ICMP-Typ** und wählen Sie in der Dropdown-Liste einen Typ für das ICMP-Paket.
    b. Aktivieren Sie das Kontrollkästchen **ICMP-Code** und wählen Sie in der Dropdown-Liste einen Typ für den ICMP-Code.
11. Wurde TCP oder UDP als Protokoll gewählt, so können Sie durch Komma getrennt die Portnummern des Benutzercomputers und des Remote-Computers angeben, zwischen denen die Verbindung kontrolliert werden soll:
    a. Geben Sie im Feld **Remote-Ports** den Port des Remote-Computers an.

b. Geben Sie im Feld **Lokale Ports** den Port des Benutzercomputers an.

12. Geben Sie in der Tabelle **Netzwerkadapter** die Einstellungen für die Netzwerkadapter an, von denen Netzwerkpakete gesendet oder empfangen werden können. Verwenden Sie dazu die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**.

13. Wenn Sie die Kontrolle von Netzwerkpaketen im Hinblick auf ihre Lebenszeit (TTL, Time to Live) beschränken möchten, aktivieren Sie das Kontrollkästchen **TTL** und geben Sie im Feld daneben einen Wertebereich für die Lebenszeit gesendeter und/oder empfangener Netzwerkpakete an.

    Die Netzwerkregel kontrolliert die Übertragung von Netzwerkpaketen, deren Lebenszeit den angegebenen Wert nicht überschreitet.

    Andernfalls deaktivieren Sie das Kontrollkästchen **TTL**.

14. Geben Sie die Netzwerkadressen der Remote-Computer an, die Netzwerkpakete senden und/oder empfangen können. Wählen Sie dazu in der Dropdown-Liste **Remote-Adressen** einen der folgenden Werte:

    - **Beliebige Adresse**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Remote-Computer mit einer beliebigen IP-Adresse.
    - **Subnetzadressen**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Remote-Computer mit den IP-Adressen, die zu dem ausgewählten Netzwerktyp gehören: **Vertrauenswürdige Netzwerke**, **Lokale Netzwerke**, **Öffentliche Netzwerke**.
    - **Adressen aus der Liste**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Remote-Computer mit den IP-Adressen, die in der unten angebrachten Liste angegeben werden können. Dazu dienen die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**.

15. Geben Sie die Netzwerkadressen der Computer an, auf denen das Programm Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und/oder empfangen können. Wählen Sie dazu in der Dropdown-Liste **Lokale Adressen** einen der folgenden Werte:

    - **Beliebige Adresse**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Computer, auf denen das Programm Kaspersky Endpoint Security installiert ist und die eine beliebige IP-Adresse besitzen.
    - **Adressen aus der Liste**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Computer, auf denen das Programm Kaspersky Endpoint Security installiert ist und die IP-Adressen besitzen, die in der unten angebrachten Liste angegeben werden können. Dazu dienen die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**.

    > Es kann vorkommen, dass für Programme, die mit Netzwerkpaketen arbeiten, keine lokale Adresse ermittelt werden kann. In diesem Fall wird der Einstellungswert **Lokale Adressen** ignoriert.

16. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

17. Klicken Sie im Fenster **Netzwerkregel** auf **OK**.

Wenn Sie eine neue Netzwerkregel erstellt haben, wird diese auf der Registerkarte **Netzwerkregeln für Pakete** im Fenster **Firewall** angezeigt. Standardmäßig werden neue Netzwerkregeln am Ende der Liste der Netzwerkregeln für Pakete hinzugefügt.

18. Klicken Sie im Fenster **Firewall** auf **OK**.

19. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Netzwerkregel für Pakete aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um eine Netzwerkregel für Pakete zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Firewall angezeigt.

3. Klicken Sie auf **Netzwerkregeln für Pakete**.

   Das Fenster **Firewall** wird auf der Registerkarte **Netzwerkregeln für Pakete** geöffnet.

4. Wählen Sie in der Liste die erforderliche Netzwerkregel für Pakete.

5. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen für die Netzwerkregel für Pakete, die Sie aktivieren möchten.
   - Deaktivieren Sie das Kontrollkästchen für die Netzwerkregel für Pakete, die Sie deaktivieren möchten.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Verhalten der Firewall in Bezug auf Netzwerkregeln für Pakete ändern

Gehen Sie folgendermaßen vor, um die Firewall-Aktion für die Netzwerkregel fürPakete zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Firewall angezeigt.

3. Klicken Sie auf **Netzwerkregeln für Pakete**.

   Das Fenster **Firewall** wird auf der Registerkarte **Netzwerkregeln für Pakete** geöffnet.

4. Wählen Sie in der Liste die Netzwerkregel für Pakete, für welche Sie die Aktion ändern möchten.

5. Klicken Sie mit der rechten Maustaste auf die Spalte **Erlaubnis** und wählen Sie die gewünschte Aktion:
   - **Erlauben**.
   - **Verbieten**.
   - **Gemäß Programmregel**.
   - **Protokollieren**.
6. Klicken Sie im Fenster **Firewall** auf **OK**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Priorität einer Netzwerkregel für Pakete ändern

Die Ausführungspriorität einer Netzwerkregel für Pakete wird durch ihre Position in der Liste der Netzwerkregeln für Pakete bestimmt. Die Netzwerkregel, die in der Liste der Netzwerkregeln für Pakete an erster Stelle steht, besitzt die höchste Priorität.

Jede Netzwerkregel für Pakete, die Sie manuell erstellen, wird am Ende der Liste der Netzwerkregeln für Pakete hinzugefügt und besitzt die niedrigste Priorität.

Die Firewall führt die Regeln in der Reihenfolge aus, in der sie auf der Liste der Netzwerkregeln für Pakete stehen (von oben nach unten). Entsprechend jeder Netzwerkregel für Pakete, die verarbeitet und auf eine bestimmte Netzwerkverbindung angewendet wurde, erlaubt oder verbietet die Firewall den Netzwerkzugriff auf die Adressen und Ports, die in den Einstellungen dieser Netzwerkverbindung angegeben sind.

Gehen Sie folgendermaßen vor, um die Priorität einer Netzwerkregel für Pakete zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Firewall angezeigt.
3. Klicken Sie auf **Netzwerkregeln für Pakete**.

   Das Fenster **Firewall** wird auf der Registerkarte **Netzwerkregeln für Pakete** geöffnet.
4. Wählen Sie in der Liste die Netzwerkregel für Pakete, deren Priorität Sie ändern möchten.
5. Verschieben Sie die Netzwerkregel für Pakete mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Position in der Liste der Netzwerkregeln für Pakete.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Verwendung von Netzwerkregeln für Programme

Kaspersky Endpoint Security ordnet standardmäßig alle Programme, die auf dem Benutzercomputer installiert sind, nach dem Herstellernamen der Programme an, deren Datei- und Netzwerkaktivität kontrolliert wird. Programmgruppen werden nach Sicherheitsgruppen angeordnet. Alle Programme und Programmgruppen erben folgende Eigenschaften der jeweiligen übergeordneten Gruppe: Kontrollregeln für Programme, Netzwerkregeln für das Programm, sowie Ausführungspriorität.

Die Komponenten Programm-Überwachung und Firewall verwenden standardmäßig die Netzwerkregeln für eine Programmgruppe zur Filterung der Netzwerkaktivität aller Programme dieser Gruppe. Die Netzwerkregeln für eine Programmgruppe legen fest, welche Rechte die Programme, die dieser Gruppe angehören, für den Zugriff auf unterschiedliche Netzwerkverbindungen besitzen.

Die Firewall erstellt standardmäßig eine Auswahl von Netzwerkregeln für jede Gruppe von Programmen, die von Kaspersky Endpoint Security auf dem Computer gefunden wurden. Sie können die Firewall-Aktion für die standardmäßig erstellten Netzwerkregeln für eine Programmgruppe ändern. Standardmäßig erstellte Netzwerkregeln für eine Programmgruppe können nicht geändert, gelöscht oder deaktiviert werden. Außerdem ist ihre Priorität unveränderlich.

Sie können eine Netzwerkregel für ein bestimmtes Programm erstellen. Eine solche Regel besitzt eine höhere Priorität als die Netzwerkregel der Gruppe, zu welcher dieses Programm gehört.

Bei der Verwendung von Netzwerkregeln für Programme können Sie folgende Aktionen ausführen:

- Neue Netzwerkregel erstellen

  Sie können eine neue Netzwerkregel erstellen, nach welcher die Firewall die Netzwerkaktivität eines Programms oder der Programme, die zur gewählten Programmgruppe gehören, regulieren soll.

- Netzwerkregel aktivieren und deaktivieren

  Alle Netzwerkregeln werden mit dem Status *Aktiv* zur Liste der Netzwerkregeln hinzugefügt. Ist eine Netzwerkregel aktiviert, so wendet die Firewall diese Regel an.

  Eine manuell erstellte Netzwerkregel kann deaktiviert werden. Ist eine Netzwerkregel deaktiviert, so wird diese Regel von der Firewall vorübergehend nicht verwendet.

- Einstellungen der Netzwerkregel ändern

  Nachdem Sie eine neue Netzwerkregel erstellt haben, können Sie die Einstellungen der Regel jederzeit ändern.

- Firewall-Aktion für die Netzwerkregel ändern

  In der Liste der Netzwerkregeln können Sie die Aktion für die Netzwerkregel ändern, die von der Firewall ausgeführt wird, wenn eine Netzwerkaktivität dieses Programms oder der Programmgruppe erkannt wird.

- Priorität der Netzwerkregel ändern

  Sie können die Priorität einer manuell erstellten Netzwerkregel erhöhen oder reduzieren.

- Netzwerkregel löschen

  Sie können eine manuell erstellte Netzwerkregel löschen, damit die Firewall diese Netzwerkregel beim Fund einer Netzwerkaktivität nicht auf das gewählte Programm oder die Programmgruppe anwendet, und damit die Regel nicht in der Liste der Netzwerkregeln für Programme erscheint.

Netzwerkregel für Programme erstellen und ändern

Gehen Sie folgendermaßen vor, um eine Netzwerkregel für eine Gruppe zu erstellen oder zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.
3. Klicken Sie auf **Regeln für Programme**.

   Das Fenster **Firewall** wird auf der Registerkarte **Netzwerkregeln für Programme** geöffnet.
4. Wählen Sie in der Programmliste ein Programm oder eine Programmgruppe, für die eine Netzwerkregel erstellt oder geändert werden soll.
5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Regeln für das Programm** oder **Regeln für die Gruppe**.

   Das Fenster **Kontrollregeln für ein Programm** oder **Kontrollregeln für eine Programmgruppe** wird geöffnet.
6. Wählen Sie die Registerkarte **Netzwerkregeln** im Fenster **Kontrollregeln für ein Programm** oder **Kontrollregeln für die Programmgruppe** aus.
7. Führen Sie eine der folgenden Aktionen aus:

   - Um eine neue Paketregel zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine Netzwerkregel zu ändern, wählen Sie in der Liste der Netzwerkregeln eine Regel und klicken Sie auf **Ändern**.

   Das Fenster **Netzwerkregel** wird geöffnet.
8. Wählen Sie in der Dropdown-Liste **Aktion** die Aktion aus, welche die Firewall bei Erkennen der entsprechenden Art von Netzwerkaktivität ausführen soll:

   - **Erlauben**.
   - **Verbieten**.
9. Geben Sie im Feld **Name** den Namen eines Netzwerkdienstes an. Dafür gibt es folgende Methoden:

   - Klicken Sie auf das Symbol , das sich rechts vom Feld **Name** befindet, und wählen Sie in der Dropdown-Liste den Namen eines Netzwerkdienstes aus.

     Die Dropdown-Liste enthält die Netzwerkdienste, welche die am häufigsten verwendeten Netzwerkverbindungen beschreiben.
   - Tragen Sie im Feld **Name** manuell den Namen eines Netzwerkdienstes ein.
10. Geben Sie ein Datenübertragungsprotokoll an:

    a. Aktivieren Sie das Kontrollkästchen **Protokoll**.

b. Wählen Sie in der Dropdown-Liste den Typ des Protokolls, mit dem die Kontrolle der Netzwerkaktivität erfolgen soll.

Die Firewall kontrolliert Verbindungen der Protokolle TCP, UDP, ICMP, ICMPv6, IGMP und GRE. Wenn in der Dropdown-Liste **Name** ein Netzwerkdienst gewählt ist, wird automatisch das Kontrollkästchen **Protokoll** aktiviert und in der Dropdown-Liste neben dem Kontrollkästchen wird der Protokolltyp gewählt, der dem gewählten Netzwerkdienst entspricht. Das Kontrollkästchen **Protokoll** ist standardmäßig deaktiviert.

11. Wählen Sie in der Dropdown-Liste **Richtung** eine Richtung für die zu kontrollierende Netzwerkaktivität.

Die Firewall kontrolliert Netzwerkverbindungen mit folgenden Richtungen:

- **Eingehend**.
- **Eingehend / Ausgehend**.
- **Ausgehend**.

12. Wurde ICMP oder ICMPv6 als Protokoll gewählt, können Sie Typ und Code des ICMP-Pakets festlegen:

a. Aktivieren Sie das Kontrollkästchen **ICMP-Typ** und wählen Sie in der Dropdown-Liste einen Typ für das ICMP-Paket.

b. Aktivieren Sie das Kontrollkästchen **ICMP-Code** und wählen Sie in der Dropdown-Liste einen Typ für den ICMP-Code.

13. Wurde TCP oder UDP als Protokoll gewählt, so können Sie durch Komma getrennt die Portnummern des Benutzercomputers und des Remote-Computers angeben, zwischen denen die Verbindung kontrolliert werden soll:

a. Geben Sie im Feld **Remote-Ports** den Port des Remote-Computers an.

b. Geben Sie im Feld **Lokale Ports** den Port des Benutzercomputers an.

14. Geben Sie die Netzwerkadressen der Remote-Computer an, die Netzwerkpakete senden und/oder empfangen können. Wählen Sie dazu in der Dropdown-Liste **Remote-Adressen** einen der folgenden Werte:

- **Beliebige Adresse**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Remote-Computer mit einer beliebigen IP-Adresse.
- **Subnetzadressen**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Remote-Computer mit den IP-Adressen, die zu dem ausgewählten Netzwerktyp gehören: **Vertrauenswürdige Netzwerke**, **Lokale Netzwerke**, **Öffentliche Netzwerke**.
- **Adressen aus der Liste**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Remote-Computer mit den IP-Adressen, die in der unten angebrachten Liste angegeben werden können. Dazu dienen die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**.

15. Geben Sie die Netzwerkadressen der Computer an, auf denen das Programm Kaspersky Endpoint Security installiert ist und die Netzwerkpakete senden und/oder empfangen können. Wählen Sie dazu in der Dropdown-Liste **Lokale Adressen** einen der folgenden Werte:

- **Beliebige Adresse**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Computer, auf denen das Programm Kaspersky Endpoint Security installiert ist und die eine beliebige IP-Adresse besitzen.

- **Adressen aus der Liste**. Die Netzwerkregel kontrolliert das Senden und/oder den Empfang von Netzwerkpaketen durch Computer, auf denen das Programm Kaspersky Endpoint Security installiert ist und die IP-Adressen besitzen, die in der unten angebrachten Liste angegeben werden können. Dazu dienen die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**.

> Es kann vorkommen, dass für Programme, die mit Netzwerkpaketen arbeiten, keine lokale Adresse ermittelt werden kann. In diesem Fall wird der Einstellungswert **Lokale Adressen** ignoriert.

16. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

17. Klicken Sie im Fenster **Netzwerkregel** auf **OK**.

    Eine neu erstellte Netzwerkregel wird auf der Registerkarte **Netzwerkregeln** angezeigt.

18. Klicken Sie auf die Schaltfläche **OK** entweder im Fenster **Kontrollregeln für eine Programmgruppe**, wenn die Regel für eine Programmgruppe vorgesehen ist, oder im Fenster **Kontrollregeln für ein Programm**, wenn die Regel für ein Programm vorgesehen ist.

19. Klicken Sie im Fenster **Firewall** auf **OK**.

20. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Netzwerkregel für Programme aktivieren und deaktivieren

Um eine Netzwerkregel für Programme zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Firewall angezeigt.

3. Klicken Sie auf **Regeln für Programme**.

   Das Fenster **Firewall** wird auf der Registerkarte **Netzwerkregeln für Programme** geöffnet.

4. Wählen Sie in der Liste ein Programm oder eine Programmgruppe, für die eine Netzwerkregel aktiviert oder deaktiviert werden soll.

5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Regeln für das Programm** oder **Regeln für die Gruppe**.

   Das Fenster **Kontrollregeln für ein Programm** oder **Kontrollregeln für eine Programmgruppe** wird geöffnet.

6. Wählen Sie im folgenden Fenster die Registerkarte **Netzwerkregeln**.

7. Wählen Sie in der Liste der Netzwerkregeln dieser Gruppe die entsprechende Netzwerkregel.
8. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen für die Netzwerkregel, die Sie aktivieren möchten.
   - Deaktivieren Sie das Kontrollkästchen für die Netzwerkregel, die Sie deaktivieren möchten.

     Sie können eine Netzwerkregel für Programmgruppen nicht deaktivieren, wenn sie standardmäßig von der Firewall erstellt wurde.
9. Klicken Sie auf die Schaltfläche **OK** entweder im Fenster **Kontrollregeln für eine Programmgruppe**, wenn die Regel für eine Programmgruppe vorgesehen ist, oder im Fenster **Kontrollregeln für ein Programm**, wenn die Regel für ein Programm vorgesehen ist.
10. Klicken Sie im Fenster **Firewall** auf **OK**.
11. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Firewall-Aktion für die Netzwerkregel für Programme ändern

Sie können die Firewall-Aktion für alle standardmäßig erstellten Netzwerkregeln eines Programms oder einer Programmgruppe ändern, und Sie können die Firewall-Aktion für eine bestimmte manuell erstellte Netzwerkregel eines Programms oder einer Programmgruppe ändern.

Um die Firewall-Aktion für alle Netzwerkregeln eines Programms oder einer Programmgruppe zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Firewall angezeigt.
3. Klicken Sie auf **Regeln für Programme**.

   Das Fenster **Firewall** wird auf der Registerkarte **Netzwerkregeln für Programme** geöffnet.
4. Wählen Sie in der Liste ein Programm oder eine Programmgruppe, wenn Sie die Firewall-Aktion für alle entsprechenden standardmäßig erstellten Netzwerkregeln ändern möchten. Manuell erstellte Netzwerkregeln bleiben unverändert.
5. Klicken Sie mit der linken Maustaste auf die Spalte **Netzwerk** und wählen Sie die gewünschte Aktion:
   - **Erben**.
   - **Erlauben**.
   - **Verbieten**.
6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Um die Firewall-Aktion für eine Netzwerkregel eines Programms oder einer Programmgruppe zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Block **Basisschutz** den Unterabschnitt **Firewall**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Firewall angezeigt.
3. Klicken Sie auf **Regeln für Programme**.

   Das Fenster **Firewall** wird auf der Registerkarte **Netzwerkregeln für Programme** geöffnet.
4. Wählen Sie in der Liste ein Programm oder eine Programmgruppe, für welche die Aktion einer Netzwerkregel geändert werden soll.
5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Regeln für das Programm** oder **Regeln für die Gruppe**.

   Das Fenster **Kontrollregeln für ein Programm** oder **Kontrollregeln für eine Programmgruppe** wird geöffnet.
6. Wählen Sie im folgenden Fenster die Registerkarte **Netzwerkregeln**.
7. Wählen Sie die Netzwerkregel, für welche Sie die Firewall-Aktion ändern möchten.
8. Klicken Sie mit der rechten Maustaste auf die Spalte **Erlaubnis** und wählen Sie die gewünschte Aktion:
   - **Erlauben**.
   - **Verbieten**.
   - **Protokollieren**.
9. Klicken Sie auf die Schaltfläche **OK** entweder im Fenster **Kontrollregeln für eine Programmgruppe**, wenn die Regel für eine Programmgruppe vorgesehen ist, oder im Fenster **Kontrollregeln für ein Programm**, wenn die Regel für ein Programm vorgesehen ist.
10. Klicken Sie im Fenster **Firewall** auf **OK**.
11. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Priorität der Netzwerkregel für Programme ändern

Die Ausführungspriorität einer Netzwerkregel wird durch ihre Position in der Liste der Netzwerkregeln bestimmt. Die Firewall führt die Regeln in der Reihenfolge aus, in der sie auf der Liste der Netzwerkregeln stehen (von oben nach unten). Entsprechend jeder Netzwerkregel, die verarbeitet und auf eine bestimmte Netzwerkverbindung angewendet wurde, erlaubt oder verbietet die Firewall den Netzwerkzugriff auf die Adressen und Ports, die in den Einstellungen dieser Netzwerkverbindung angegeben sind.

Manuell erstellte Netzwerkregeln besitzen eine höhere Priorität als standardmäßig erstellte Netzwerkregeln.

Sie können die Priorität von manuell erstellten Netzwerkregeln für Programmgruppen nicht ändern.

Um die Priorität einer Netzwerkregel zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Firewall**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Firewall angezeigt.
3. Klicken Sie auf **Regeln für Programme**.

   Das Fenster **Firewall** wird auf der Registerkarte **Netzwerkregeln für Programme** geöffnet.
4. Wählen Sie in der Programmliste ein Programm oder eine Programmgruppe, für welche die Priorität der Netzwerkregel geändert werden soll.
5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Regeln für das Programm** oder **Regeln für die Gruppe**.

   Das Fenster **Kontrollregeln für ein Programm** oder **Kontrollregeln für eine Programmgruppe** wird geöffnet.
6. Wählen Sie im folgenden Fenster die Registerkarte **Netzwerkregeln**.
7. Wählen Sie die Netzwerkregel, deren Priorität Sie ändern möchten.
8. Verschieben Sie die Netzwerkregel mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Position in der Liste der Netzwerkregeln.
9. Klicken Sie auf die Schaltfläche **OK** entweder im Fenster **Kontrollregeln für eine Programmgruppe**, wenn die Regel für eine Programmgruppe vorgesehen ist, oder im Fenster **Kontrollregeln für ein Programm**, wenn die Regel für ein Programm vorgesehen ist.
10. Klicken Sie im Fenster **Firewall** auf **OK**.
11. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Netzwerkmonitor

Dieser Abschnitt enthält Informationen zum Netzwerkmonitor und eine Anleitung zum Start des Netzwerkmonitors.

Über den Netzwerkmonitor

Der *Netzwerkmonitor* dient dazu, in Echtzeit Informationen über die Netzwerkaktivität des Benutzercomputers anzuzeigen.

Netzwerkmonitor starten

Gehen Sie folgendermaßen vor, um den Netzwerkmonitor zu starten:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie auf den Block **Schutzkomponenten**.

   Das Fenster **Schutzkomponenten** wird geöffnet.

3. Klicken Sie im unteren Fensterbereich auf den Link **Netzwerkmonitor**.

   Das Fenster **Netzwerkmonitor** öffnet sich. Dieses Fenster bietet vier Registerkarten mit Informationen zu den Netzwerkaktivitäten des Benutzercomputers:

   - Auf der Registerkarte **Netzwerkaktivität** werden alle momentan aktiven Netzverbindungen des Computers angezeigt. Es werden sowohl eingehende als auch ausgehende, vom Benutzercomputer initiierte Netzverbindungen dargestellt.

   - Auf der Registerkarte **Offene Ports** sind alle geöffneten Ports des Computers aufgelistet.

   - Auf der Registerkarte **Netzwerkverkehr** wird das Volumen des ein- und ausgehenden Netzwerkverkehrs zwischen dem lokalen Computer und anderen Computern des Netzwerks angezeigt, in dem der Computer momentan arbeitet.

   - Auf der Registerkarte **Blockierte Computer** sind die IP-Adressen jener Remote-Computern aufgelistet, von deren IP-Adresse ein versuchter Netzwerkangriff erkannt wurde und deren Netzwerkaktivität deshalb von der Komponente Schutz vor Netzwerkbedrohungen blockiert wurde.

Schutz vor modifizierten USB-Geräten

Dieser Abschnitt informiert über die Komponente Schutz vor modifizierten USB-Geräten.

Über den Schutz vor modifizierten USB-Geräten

Bestimmte Viren verändern die in USB-Geräten eingebettete Software so, dass das USB-Gerät vom Betriebssystem als Tastatur erkannt wird.

Die Komponente Schutz vor modifizierten USB-Geräten verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem PC verbunden werden.

Wenn ein USB-Gerät an den Computer angeschlossen und vom Betriebssystem als Tastatur erkannt wird, fordert das Programm den Benutzer auf, mit diesem Gerät oder mithilfe der Bildschirmtastatur (falls diese verfügbar ist) einen vom Programm generierten digitalen Code einzugeben. Dieser Vorgang heißt Autorisierung der Tastatur. Das Programm erlaubt die Verwendung einer autorisierten Tastatur. Eine Tastatur, die nicht autorisiert wurde, wird blockiert.

Der Schutz vor modifizierten USB-Geräten läuft sofort nach der Installation der Komponente im Hintergrundmodus. Wenn ein Computer, auf welchem das Programm Kaspersky Endpoint Security installiert ist, keiner Richtlinie für Kaspersky Security Center unterliegt, können Sie den Schutz vor modifizierten USB-Geräten aktivieren und deaktivieren. Dazu können der Schutz und die Überwachung des Computers vorübergehend angehalten und später fortgesetzt werden.

Komponente Schutz vor modifizierten USB-Geräten installieren

Wenn Sie bei der Installation von Kaspersky Endpoint Security die Basis- oder Standardinstallation gewählt haben, ist die Komponente Schutz vor modifizierten USB-Geräten nicht verfügbar. Damit die Komponente installiert wird, muss die Auswahl der Programmkomponenten geändert werden.

Um die Komponente Schutz vor modifizierten USB-Geräten zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Systemsteuerung**. Dafür gibt es folgende Methoden:
   - Wenn Sie Windows 7 verwenden, wählen Sie im **Startmenü** den Punkt **Systemsteuerung** aus.
   - Wenn Sie Windows 8 / Windows 8.1 verwenden, drücken Sie die Tastenkombination **Win**+**I** und wählen Sie den Punkt **Systemsteuerung** aus.
   - Wenn Sie Windows 10 verwenden, drücken Sie die Tastenkombination **Win**+**X** und wählen Sie den Punkt **Systemsteuerung** aus.
2. Wählen Sie im Fenster **Systemsteuerung** den Punkt **Programme und Features** aus.
3. Wählen Sie in der Liste der installierten Programme das Element **Kaspersky Endpoint Security für Windows** aus.
4. Klicken Sie auf **Deinstallieren/Ändern**.
5. Klicken Sie im Fenster des Installationsassistenten **Programm ändern, reparieren oder entfernen** auf **Ändern**.

   Das Fenster **Benutzerdefinierte Installation** des Installationsassistenten wird geöffnet.
6. Wählen Sie in der Komponentengruppe **Basisschutz** im Kontextmenü des Symbols neben dem Namen der Komponente **Schutz vor modifizierten USB-Geräten** den Punkt **Die Komponente wird auf der lokalen Festplatte installiert** aus.
7. Klicken Sie auf **Weiter**.
8. Folgen Sie den Anweisungen des Installationsassistenten.

Schutz vor modifizierten USB-Geräten aktivieren und deaktivieren

Um den Schutz vor modifizierten USB-Geräten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor modifizierten USB-Geräten**.

   Auf der rechten Seite des Fensters werden die Einstellungen der Komponente Schutz vor modifizierten USB-Geräten angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Schutz vor modifizierten USB-Geräten aktivieren**, um den Schutz vor modifizierten USB-Geräten einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Schutz vor modifizierten USB-Geräten aktivieren**, um den Schutz vor modifizierten USB-Geräten auszuschalten.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Verwendung der Bildschirmtastatur bei der Autorisierung erlauben und verbieten

Die Möglichkeit zur Verwendung der Bildschirmtastatur ist nur für die Autorisierung von USB-Geräten vorgesehen, welche die Eingabe beliebiger Zeichen nicht unterstützen (z. B. Strichcodescanner). Es wird davon abgeraten, die Bildschirmtastatur für die Autorisierung unbekannter USB-Geräte zu verwenden.

Um die Verwendung der Bildschirmtastatur bei der Autorisierung zu erlauben oder zu verbieten, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Basisschutz** den Unterabschnitt **Schutz vor modifizierten USB-Geräten**.

   Im rechten Fensterbereich werden die Einstellungen der Komponente angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Um die Verwendung der Bildschirmtastatur für die Autorisierung zu verbieten, aktivieren Sie das Kontrollkästchen **Verwendung der Bildschirmtastatur für die Autorisierung von USB-Geräten verbieten**.
   - Um die Verwendung der Bildschirmtastatur für die Autorisierung zu erlauben, deaktivieren Sie das Kontrollkästchen **Verwendung der Bildschirmtastatur für die Autorisierung von USB-Geräten verbieten**.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Autorisierung der Tastatur

USB-Geräte, die vom Betriebssystem als Tastatur erkannt wurden und vor der Installation der Komponente Schutz vor modifizierten USB-Geräten an den Computer angeschlossen wurden, werden nach der Installation der Komponente als autorisiert betrachtet.

Das Programm fordert die Autorisierung eines verbundenen USB-Geräts, das vom Betriebssystem als Tastatur erkannt wurde, wenn die Autorisierungsanfrage für USB-Tastaturen aktiviert ist. Der Benutzer kann eine nicht autorisierte Tastatur erst verwenden, nachdem sie autorisiert wurde.

Wenn die Autorisierungsanfrage für USB-Tastaturen deaktiviert ist, kann der Benutzer alle angeschlossenen Tastaturen verwenden. Nachdem die Autorisierungsanfrage für USB-Tastaturen aktiviert wurde, fragt das

Programm für jede unautorisierte Tastatur, die angeschlossen wird, nach einer Autorisierung.

Um eine Tastatur zu autorisieren, gehen Sie wie folgt vor:

1. Wenn die Autorisierung von USB-Tastaturen aktiviert ist, schließen Sie die Tastatur an einen USB-Port an.

   Das Fenster **Autorisierung der Tastatur <Name der Tastatur>** mit Informationen über die angeschlossene Tastatur und mit einem digitalen Autorisierungscode wird geöffnet.

2. Geben Sie entweder mit der angeschlossenen Tastatur oder mit der Bildschirmtastatur, falls diese verfügbar ist, den digitalen Code aus dem Autorisierungsfenster ein.

3. Klicken Sie auf **OK**.

   Wurde der richtige Code eingegeben, so speichert das Programm die Identifikationsparameter (VID/PID der Tastatur und Nummer des Ports, über den die Tastatur verbunden ist) in der Liste der autorisierten Tastaturen. Wenn die Tastatur erneut angeschlossen oder das Betriebssystem neu gestartet wird, ist keine Autorisierung erforderlich.

   > Wenn eine autorisierte Tastatur über einen anderen USB-Port mit dem Computer verbunden wird, fragt das Programm erneut nach der Autorisierung.

   Wurde der digitale Code falsch eingegeben, so generiert das Programm einen neuen Code. Die Anzahl der Eingabeversuche für den digitalen Code ist auf drei beschränkt. Nachdem der digitale Code dreimal falsch eingegeben wurde oder das Fenster **Autorisierung der Tastatur <Name der Tastatur>** geschlossen wurde, blockiert das Programm die Eingabe von dieser Tastatur. Wenn die Tastatur erneut angeschlossen oder das Betriebssystem neu gestartet wird, schlägt das Programm erneut vor, die Autorisierung vorzunehmen.

Programmkontrolle

Dieser Abschnitt informiert über die Programmkontrolle und erklärt die Einstellungen der Komponente.

Über die Programmkontrolle

Die Komponente Programmkontrolle überwacht die Versuche von Benutzern, Programme zu starten, und regelt den Programmstart mithilfe der *Regeln der Programmkontrolle*.

Der Start von Programmen, deren Einstellungen keiner Regel der Programmkontrolle entsprechen, wird im ausgewählten Modus der Komponente reguliert. Standardmäßig ist der Modus *Schwarze Liste* ausgewählt. Dieser Modus erlaubt allen Benutzern, ein beliebiges Programm zu starten.

Alle Versuche von Benutzern, Programme zu starten, werden in Berichten protokolliert.

Programmkontrolle aktivieren und deaktivieren

Die Programmkontrolle ist standardmäßig aktiviert. Bei Bedarf können Sie die Programmkontrolle deaktivieren.

Um die Programmkontrolle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Programmkontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Programmkontrolle aktivieren**, um die Programmkontrolle einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Programmkontrolle aktivieren**, um die Programmkontrolle auszuschalten.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Funktionelle Beschränkungen der Programmkontrolle

Die Funktion der Komponente Programmkontrolle ist in folgenden Fällen beschränkt:

- Beim Programm-Upgrade wird der Import von Einstellungen für die Komponente Programmkontrolle nicht unterstützt.
- Beim Programm-Upgrade wird der Import der Einstellungen für die Komponente Programmkontrolle nur beim Upgrade von Kaspersky Endpoint Security 10 Service Pack 2 für Windows auf Kaspersky Endpoint Security 11 für Windows unterstützt.

  Beim Upgrade von anderen Programmversionen als Kaspersky Endpoint Security 10 Service Pack 2 für Windows muss die Komponente Programmkontrolle erneut angepasst werden, um die Funktionsfähigkeit der Komponente zu gewährleisten.
- Wenn keine Verbindung mit den KSN-Servern besteht, empfängt Kaspersky Endpoint Security die Informationen über die Reputation von Programmen und Modulen nur aus den lokalen Datenbanken.

  Abhängig davon, ob eine Verbindung mit den KSN-Servern besteht oder nicht, kann die Liste der Programme, für die Kaspersky Endpoint Security die KL-Kategorie **Programme, die laut KSN-Reputation vertrauenswürdig sind** unterschiedlich sein.
- Kaspersky Security Center kann Informationen über maximal 150.000 verarbeitete Dateien in der Datenbank speichern. Wenn diese Anzahl von Einträgen erreicht ist, werden neue Dateien nicht mehr verarbeitet. Um die Inventarisierung fortzusetzen, müssen von dem Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, Dateien gelöscht werden, die bisher bei der Inventarisierung in der Datenbank für Kaspersky Security Center aufgezeichnet worden sind.

- Der Start von Skripten wird von der Komponente nicht kontrolliert, wenn ein Skript nicht über die Befehlszeile an den Interpreter übermittelt wird.

  Ist der Start des Interpreters durch Regeln der Programmkontrolle erlaubt, so blockiert die Komponente ein Skript nicht, das aus diesem Interpreter gestartet wurde.

- Der Start von Skripten aus Interpretern wird von der Komponente nicht kontrolliert, wenn der Interpreter vom Programm Kaspersky Endpoint Security nicht unterstützt wird.

  Kaspersky Endpoint Security unterstützt folgende Interpreter:

  - Java
  - PowerShell

  Es werden folgende Interpretertypen unterstützt:

  - %ComSpec%
  - %SystemRoot%\\system32\\regedit.exe
  - %SystemRoot%\\regedit.exe
  - %SystemRoot%\\system32\\regedt32.exe
  - %SystemRoot%\\system32\\cscript.exe
  - %SystemRoot%\\system32\\wscript.exe
  - %SystemRoot%\\system32\\msiexec.exe
  - %SystemRoot%\\system32\\mshta.exe
  - %SystemRoot%\\system32\\rundll32.exe
  - %SystemRoot%\\system32\\wwahost.exe
  - %SystemRoot%\\syswow64\\cmd.exe
  - %SystemRoot%\\syswow64\\regedit.exe
  - %SystemRoot%\\syswow64\\regedt32.exe
  - %SystemRoot%\\syswow64\\cscript.exe
  - %SystemRoot%\\syswow64\\wscript.exe
  - %SystemRoot%\\syswow64\\msiexec.exe
  - %SystemRoot%\\syswow64\\mshta.exe
  - %SystemRoot%\\syswow64\\rundll32.exe

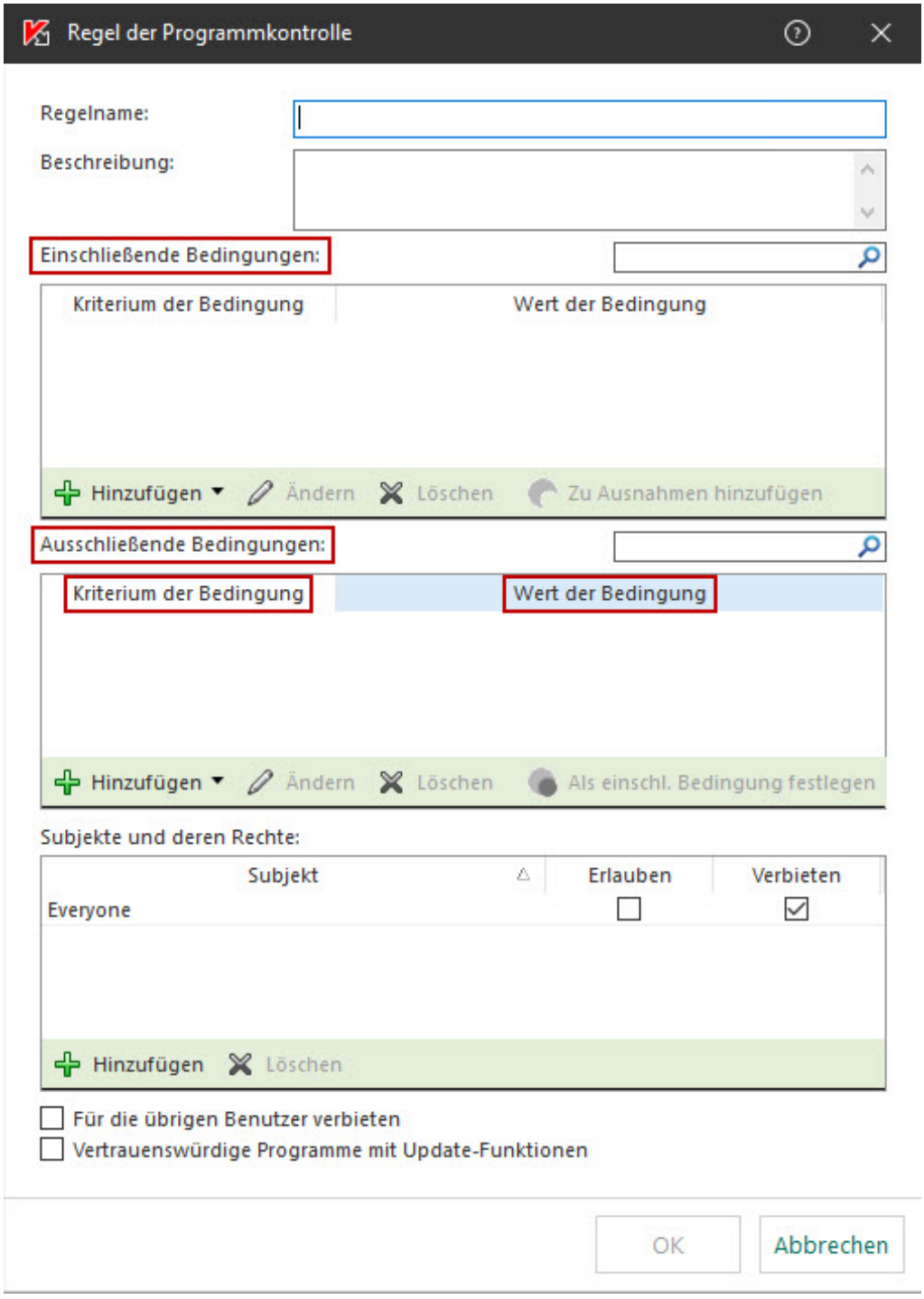
- %SystemRoot%\\syswow64\\wwahost.exe

Über die Regeln der Programmkontrolle

Kaspersky Endpoint Security überwacht mithilfe von Regeln die Versuche von Benutzern, Programme zu starten. Eine Regel der Programmkontrolle enthält Auslösebedingungen und legt eine Aktion fest, die von der Komponente Programmkontrolle beim Auslösen der Regel ausgeführt wird (Erlaubnis oder Verbot des von Benutzern ausgeführten Programmstarts).

Auslösebedingungen für eine Regel

Als Auslösebedingung für eine Regel gilt die Übereinstimmung von "Typ der Bedingung - Kriterium der Bedingung - Wert der Bedingung" (s. Abb. unten). Basierend auf den Auslösebedingungen für eine Regel wendet Kaspersky Endpoint Security die Regel auf ein Programm an (oder wendet die Regel nicht an).



In Regeln werden einschließende und ausschließende Bedingungen verwendet:

- *Einschließende Bedingungen*. Kaspersky Endpoint Security wendet die Regel auf ein Programm an, wenn das Programm mindestens eine einschließende Bedingung erfüllt.
- *Ausschließende Bedingungen*. Kaspersky Endpoint Security wendet die Regel nicht auf ein Programm an, wenn das Programm mindestens eine ausschließende Bedingung oder keine einschließende Bedingung erfüllt.

Auslösebedingungen für eine Regel werden mithilfe von Kriterien definiert. Um in Kaspersky Endpoint Security Bedingungen zu erstellen, werden folgende Kriterien verwendet:

- Pfad des Ordners mit der ausführbaren Programmdatei oder Pfad der ausführbaren Programmdatei
- Metadaten: Name der ausführbaren Programmdatei, Version der ausführbaren Programmdatei, Programmname, Programmversion, Programmhersteller
- Hash der ausführbaren Programmdatei
- Zertifikat: Herausgeber, Subjekt, Fingerabdruck
- Zugehörigkeit eines Programms zu einer KL-Kategorie
- Speicherort der ausführbaren Programmdatei auf dem Wechseldatenträger

Für jedes Kriterium, das in einer Bedingung verwendet wird, muss ein Wert angegeben werden. Entsprechen die Parameter eines zu startenden Programms den Werten von Kriterien, die in einer einschließenden Bedingung angegeben sind, so wird die Regel ausgelöst. In diesem Fall führt die Programmkontrolle die Aktion aus, die in der Regel angegeben ist. Entsprechen die Programmparameter den Werten von Kriterien, die in einer ausschließenden Bedingung angegeben sind, so überwacht die Programmkontrolle den Start des Programms nicht.

Entscheidungen der Komponente Programmkontrolle beim Auslösen einer Regel

Wenn eine Regel ausgelöst wird, verfährt die Programmkontrolle nach der Regel und erlaubt oder verbietet den Benutzern (Benutzergruppen) den Programmstart. Sie können konkrete Benutzer oder Benutzergruppen wählen, denen der Start von Programmen, für welche eine Regel ausgelöst wird, erlaubt oder verboten werden soll.

In einer *Verbotsregel* ist kein Benutzer angegeben, dem der Start von Programmen erlaubt ist, welche die Regel erfüllen.

In einer *Erlaubnisregel* ist kein Benutzer angegeben, dem der Start von Programmen verboten ist, welche die Regel erfüllen.

Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Wenn für eine Benutzergruppe beispielsweise eine Erlaubnisregel der Programmkontrolle festgelegt ist, für einen Benutzer dieser Gruppe aber eine Verbotsregel der Programmkontrolle vorliegt, so wird der Start des Programms für diesen Benutzer verboten.

Status einer Regel

Für die Regeln der Programmkontrolle gibt es folgende Statusvarianten:

- **Ein**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ verwendet wird.
- **Aus**. Dieser Status bedeutet, dass die Regel nicht von der Komponente „Programmkontrolle“ verwendet wird.
- **Test**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, für welche die Regel gilt, erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

Standardmäßige Regeln der Programmkontrolle

Die Programmkontrolle funktioniert standardmäßig im Modus "Schwarze Liste". Die Komponente erlaubt allen Benutzern den Start aller Programme. Wenn der Benutzer versucht, ein Programm zu starten, das durch Regeln der Programmkontrolle verboten ist, so blockiert Kaspersky Endpoint Security den Start dieses Programms (bei Auswahl der Aktion **Blockieren**) oder speichert Informationen über den Start des Programms in einem Bericht (bei Auswahl der Aktion **Benachrichtigen**).

Aktionen mit Regeln der Programmkontrolle

Mit Regeln der Programmkontrolle können folgende Aktionen ausgeführt werden:

- Hinzufügen einer neuen Regel
- Auslösebedingungen für die Regel erstellen oder ändern
- Ändern des Regelstatus

  Eine Regel der Programmkontrolle kann aktiviert oder deaktiviert sein, oder sich im Testmodus befinden. Eine neue Regel der Programmkontrolle ist standardmäßig aktiviert.
- Regel löschen

Regel der Programmkontrolle hinzufügen und ändern

Um eine Regel der Programmkontrolle hinzuzufügen oder zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Programmkontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Programmkontrolle aktivieren**, um Zugriff auf die Einstellungen der Komponente zu erhalten.
4. Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie auf **Hinzufügen**, wenn Sie eine Regel hinzufügen möchten.
- Wenn Sie eine vorhandene Regel ändern möchten, wählen Sie in der Liste eine Regel und klicken Sie auf **Ändern**.

Das Fenster **Regel der Programmkontrolle** wird geöffnet.

5. Geben Sie Einstellungen für die Regel an oder ändern Sie sie:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein oder ändern Sie den Namen.

   b. Erstellen oder ändern Sie in der Tabelle **Einschließende Bedingungen** die Liste der einschließenden Auslösebedingungen für die Regel. Dazu dienen die Schaltflächen **Hinzufügen**, **Ändern**, **Löschen** und **Zu Ausnahmen hinzufügen**.

   c. Erstellen oder ändern Sie in der Tabelle **Ausschließende Bedingungen** eine Liste mit ausschließenden Auslösebedingungen für die Regel. Dazu dienen die Schaltflächen **Hinzufügen**, **Ändern**, **Löschen** und **Als einschl. Bedingung festlegen**.

   d. Ändern Sie erforderlichenfalls den Typ der Auslösebedingung für die Regel.

      - Um den Bedingungstyp von einschließend in ausschließend zu ändern, wählen Sie in der Tabelle **Einschließende Bedingungen** eine Bedingung und klicken Sie auf **Zu Ausnahmen hinzufügen**.
      - Um den Bedingungstyp von ausschließend in einschließend zu ändern, wählen Sie in der Tabelle **Ausschließende Bedingungen** eine Bedingung und klicken Sie auf **Als einschl. Bedingung festlegen**.

   e. Erstellen oder ändern Sie eine Liste der Benutzer und/oder Benutzergruppen, denen erlaubt oder verboten wird, Programme zu starten, welche die Auslösebedingungen der Regel erfüllen. Klicken Sie dazu in der Tabelle **Subjekte und deren Rechte** auf **Hinzufügen**.

      Das Microsoft-Windows-Fenster **Benutzer oder Gruppen auswählen** wird geöffnet. In diesem Fenster können Sie Benutzer und/oder Benutzergruppen wählen.

      Die Benutzerliste enthält standardmäßig den Wert **Everyone**. Die Regel gilt für alle Benutzer.

      > Ist in der Tabelle kein Benutzer angegeben, so kann die Regel nicht gespeichert werden.

   f. Aktivieren Sie in der Tabelle **Subjekte und deren Rechte** die Kontrollkästchen **Erlauben** oder **Verbieten** für die Benutzer und/oder Benutzergruppen, um deren Rechte für den Start von Programmen festzulegen.

      Ob ein Kontrollkästchen standardmäßig aktiviert ist, hängt vom Modus für die Programmkontrolle ab.

   g. Aktivieren Sie das Kontrollkästchen **Für die übrigen Benutzer verbieten**, damit das Programm den Start von Programmen, welche die Auslösebedingungen der Regel erfüllen, für alle Benutzer verbietet, die nicht in der Spalte **Subjekt** angegeben sind und die nicht zu den in der Spalte **Subjekt** angegebenen Benutzergruppen gehören.

Ist das Kontrollkästchen **Für die übrigen Benutzer verbieten** deaktiviert, so kontrolliert Kaspersky Endpoint Security den Start von Programmen für jene Benutzer nicht, die nicht in der Tabelle **Subjekte und deren Rechte** angegeben sind und die nicht zu den in der Tabelle **Subjekte und deren Rechte** angegebenen Benutzergruppen gehören.

h. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen**, damit Programme, welche die Auslösebedingungen der Regel erfüllen, von Kaspersky Endpoint Security als vertrauenswürdige Programme mit Update-Funktionen betrachtet werden, die berechtigt sind, andere ausführbare Dateien, deren Start künftig zugelassen wird, zu erstellen.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Auslösebedingung für eine Regel der Programmkontrolle hinzufügen

Um eine neue Auslösebedingung zu einer Regel der Programmkontrolle hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt Programmkontrolle.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.

3. Aktivieren Sie das Kontrollkästchen **Programmkontrolle aktivieren**, um Zugriff auf die Einstellungen der Komponente zu erhalten.

4. Führen Sie eine der folgenden Aktionen aus:

   - Um eine neue Regel zu erstellen und der Regel eine Auslösebedingung hinzuzufügen, klicken Sie auf **Hinzufügen**.

   - Um eine Auslösebedingung zu einer vorhandenen Regel hinzuzufügen, wählen Sie in der Liste eine Regel und klicken Sie auf **Ändern**.

   Das Fenster **Regel der Programmkontrolle** wird geöffnet.

5. Klicken Sie in der Tabelle **Einschließende Bedingungen** oder **Ausschließende Bedingungen** auf **Hinzufügen**.

Mithilfe der Dropdown-Liste der Schaltfläche **Hinzufügen** können Sie unterschiedliche Auslösebedingungen zu einer Regel hinzufügen (s. Anleitung unten).

Um eine Auslösebedingung für eine Regel auf Basis der Eigenschaften von Dateien in einem bestimmten Ordner hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Dropdown-Liste der Schaltfläche **Hinzufügen** den Punkt **Bedingung(en) aus den Dateieigenschaften des angegebenen Ordners**.

   Das standardmäßige Microsoft-Windows-Fenster **Ordner wählen** wird geöffnet.

2. Wählen Sie im Fenster **Ordner wählen** einen Ordner mit den ausführbaren Programmdateien, deren Eigenschaften als Basis für eine oder mehrere Auslösebedingungen der Regel dienen sollen.

3. Klicken Sie auf **OK**.

   Das Fenster **Bedingungen hinzufügen** wird geöffnet.

4. Wählen Sie in der Dropdown-Liste **Kriterium anzeigen** ein Kriterium, das als Basis für eine oder mehrere Auslösebedingungen der Regel dienen soll: **Datei-Hash**, **Zertifikat**, **KL-Kategorie**, **Metadaten** oder **Ordnerpfad**.

   Kaspersky Endpoint Security unterstützt den MD5-Datei-Hash nicht und kontrolliert den Start von Anwendungen nicht auf Basis des MD5-Hashs. Als Auslösebedingung für eine Regel wird der SHA256-Hash verwendet.

5. Wenn Sie in der Dropdown-Liste **Kriterium anzeigen** das Element **Metadaten** gewählt haben, aktivieren Sie die Kontrollkästchen für jene Eigenschaften der ausführbaren Programmdateien, die Sie in der Auslösebedingung der Regel verwenden möchten: **Dateiname**, **Dateiversion**, **Programmname**, **Programmversion**, **Hersteller**.

   Wenn keine der angegebenen Eigenschaften gewählt ist, kann die Regel nicht gespeichert sein.

6. Wenn Sie in der Dropdown-Liste **Kriterium anzeigen** das Element Zertifikat ausgewählt haben, aktivieren Sie die Kontrollkästchen für jene Parameter, die Sie in der Auslösebedingung der Regel verwenden möchten: Herausgeber, Subjekt, Fingerabdruck.

   Wenn keiner der angegebenen Parameter gewählt ist, kann die Regel nicht gespeichert sein.

   Es wird davor gewarnt, als Auslösebedingungen für Regeln nur die Kriterien **Herausgeber** und **Subjekt** zu verwenden. Die Verwendung dieser Kriterien ist unzuverlässig.

7. Aktivieren Sie die Kontrollkästchen für die Namen der ausführbaren Programmdateien, deren Eigenschaften Sie in die Auslösebedingungen der Regel aufnehmen möchten.

8. Klicken Sie auf **Weiter**.

   Eine Liste der erstellten Auslösebedingungen für die Regel wird angezeigt.

9. Gehen Sie zur Liste der für diese Regel erstellten Auslösebedingungen und aktivieren Sie die Kontrollkästchen für jene Auslösebedingungen, die zu der Regel der Programmkontrolle hinzugefügt werden sollen.

10. Klicken Sie auf **Beenden**.

Um eine Auslösebedingung für eine Regel auf Basis der Eigenschaften von Programmen, die auf dem Computer gestartet wurden, hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Dropdown-Liste der Schaltfläche **Hinzufügen** den Punkt **Bedingung(en) aus den Eigenschaften der gestarteten Programme**.

2. Wählen Sie im Fenster **Bedingungen hinzufügen** in der Dropdown-Liste **Kriterium anzeigen** ein Kriterium, das als Basis für eine oder mehrere Auslösebedingungen der Regel dienen soll: **Datei-Hash**, **Zertifikat**, **KL-Kategorie**, **Metadaten** oder **Ordnerpfad**.

3. Wenn Sie in der Dropdown-Liste **Kriterium anzeigen** das Element **Metadaten** gewählt haben, aktivieren Sie die Kontrollkästchen für jene Eigenschaften der ausführbaren Programmdateien, die Sie in der Auslösebedingung der Regel verwenden möchten: **Dateiname**, **Dateiversion**, **Programmname**, **Programmversion**, **Hersteller**.

   Wenn keine der angegebenen Eigenschaften gewählt ist, kann die Regel nicht gespeichert sein.

4. Wenn Sie in der Dropdown-Liste **Kriterium anzeigen** das Element **Zertifikat** gewählt haben, aktivieren Sie die Kontrollkästchen für jene Parameter, die Sie in der Auslösebedingung der Regel verwenden möchten: **Herausgeber**, **Subjekt**, **Fingerabdruck**.

   Wenn keiner der angegebenen Parameter gewählt ist, kann die Regel nicht gespeichert sein.

   > Es wird davor gewarnt, als Auslösebedingungen für Regeln nur die Kriterien **Herausgeber** und **Subjekt** zu verwenden. Die Verwendung dieser Kriterien ist unzuverlässig.

5. Aktivieren Sie die Kontrollkästchen für die Namen der ausführbaren Programmdateien, deren Eigenschaften Sie in die Auslösebedingungen der Regel aufnehmen möchten.

6. Klicken Sie auf **Weiter**.

   Eine Liste der erstellten Auslösebedingungen für die Regel wird angezeigt.

7. Gehen Sie zur Liste der für diese Regel erstellten Auslösebedingungen und aktivieren Sie die Kontrollkästchen für jene Auslösebedingungen, die zu der Regel der Programmkontrolle hinzugefügt werden sollen.

8. Klicken Sie auf **Beenden**.

Um eine Auslösebedingung für eine Regel auf Basis einer KL-Kategorie hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Dropdown-Liste der Schaltfläche **Hinzufügen** den Punkt **Bedingung(en) "KL-Kategorie"**.

   Eine *KL-Kategorie* ist eine von den Kaspersky-Lab-Experten erstellte Liste für Programme mit gemeinsamen thematischen Merkmalen. So enthält die KL-Kategorie "Office-Programme" beispielsweise Programme aus den Paketen Microsoft Office, Adobe Acrobat und anderen.

2. Aktivieren Sie im Fenster **Bedingung(en) "KL-Kategorie"** die Kontrollkästchen für die Namen jener KL-Kategorien, auf deren Basis eine Auslösebedingung für die Regel erstellt werden soll.

   Um die untergeordneten KL-Kategorien anzuzeigen, klicken Sie links vom Namen der KL-Kategorie auf die Schaltfläche .

3. Klicken Sie auf **OK**.

Um eine manuell definierte Auslösebedingung für eine Regel hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Dropdown-Liste unter der Schaltfläche **Hinzufügen** den Punkt **Bedingung manuell festlegen** aus.
2. Klicken Sie im Fenster **Benutzerdefinierte Bedingung** auf **Auswählen** und geben Sie den Pfad der ausführbaren Programmdatei an.
3. Wählen Sie ein Kriterium, auf dessen Basis Sie die Auslösebedingung der Regel erstellen möchten: **Datei-Hash**, **Zertifikat**, **Metadaten** oder **Datei- oder Ordnerpfad**.

   Wenn Sie im Feld **Datei- oder Ordnerpfad** einen symbolischen Link verwenden, wird empfohlen, den symbolischen Link aufzulösen, damit die Regel der Programmkontrolle korrekt funktioniert. Klicken Sie dazu auf **Symbolischen Link auflösen**.

4. Passen Sie die Parameter des gewählten Kriteriums erforderlichenfalls an.
5. Klicken Sie auf **OK**.

Um eine Auslösebedingung auf Basis von Informationen über den Datenträger der ausführbaren Programmdatei hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Dropdown-Liste unter der Schaltfläche **Hinzufügen** den Punkt **Bedingung nach Datenträger** aus.
2. Wählen Sie im Fenster **Bedingung nach Datenträger** in der Dropdown-Liste **Datenträger** einen Datenträgertyp aus. Der Start von Programmen von diesem Datenträgertyp gilt als Auslösebedingung für die Regel.
3. Klicken Sie auf **OK**.

Status einer Regel der Programmkontrolle ändern

Um den Status einer Regel der Programmkontrolle zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Programmkontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.

3. Aktivieren Sie das Kontrollkästchen **Programmkontrolle aktivieren**, um Zugriff auf die Einstellungen der Komponente zu erhalten.
4. Wählen Sie die Regel, deren Status Sie ändern möchten.

5. Öffnen Sie in der Spalte **Status** durch Linksklick das Kontextmenü und wählen Sie einen der folgenden Punkte aus:

   - **Ein**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle" verwendet wird.
   - **Aus**. Dieser Status bedeutet, dass die Regel nicht von der Komponente „Programmkontrolle" verwendet wird.
   - **Test**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, für welche diese Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

     Mithilfe des Status **Test** können Sie für einen Teil der Regeln die Aktion **Benachrichtigen** festlegen, wenn in der Dropdown-Liste **Aktion** die Variante **Blockieren** ausgewählt ist.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Regeln der Programmkontrolle testen

Um sicherzustellen, dass Programme, die Sie zum Arbeiten benötigen, nicht durch Regeln der Programmkontrolle blockiert werden, wird empfohlen, neu erstellte Regeln in den Testmodus zu versetzen und zu analysieren.

Für die Analyse von Regeln der Programmkontrolle müssen in Kaspersky Security Center die Ereignisse überprüft werden, welche die Ausführung der Komponente Programmkontrolle betreffen. Wenn der Start für alle Programme erlaubt ist, die der Benutzer zum Arbeiten benötigt, so sind die Regeln korrekt. Andernfalls sollten die Einstellungen der von Ihnen erstellten Regeln genauer angepasst werden.

Der Testmodus für die Regeln der Programmkontrolle ist standardmäßig deaktiviert.

Um den Testmodus für die Regeln der Programmkontrolle zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Programmkontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Programmkontrolle aktivieren**, um Zugriff auf die Einstellungen der Komponente zu erhalten.
4. Wählen Sie in der Dropdown-Liste **Modus für die Programmkontrolle** eines der folgenden Elemente aus:

   - **Schwarze Liste**, wenn Sie den Start aller Programme erlauben möchten, unter Ausnahme jener Programme, die in Verbotsregeln angegeben sind.

- **Weiße Liste**, wenn Sie den Start aller Programme verbieten möchten, unter Ausnahme jener Programme, die in Erlaubnisregeln angegeben sind.

5. Wählen Sie in der Dropdown-Liste **Aktion** das Element **Benachrichtigen**.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Programme, für welche der Start durch Regeln der Programmkontrolle verboten ist, werden von Kaspersky Endpoint Security nicht blockiert. Es werden aber Benachrichtigungen über ihren Start an den Administrationsserver gesendet.

Meldungsvorlagen für die Programmkontrolle ändern

Versucht ein Benutzer, ein Programm zu starten, das durch eine Regel der Programmkontrolle verboten ist, so meldet Kaspersky Endpoint Security, dass der Programmstart blockiert wurde. Wenn der Benutzer der Meinung ist, der Programmstart sei irrtümlich blockiert worden, kann der Benutzer aus der Sperrmeldung eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks senden.

Für die Meldung über die Sperrung des Programmstarts sowie für die Nachricht an den Administrator sind Vorlagen vorgesehen. Die Meldungsvorlagen können geändert werden.

Gehen Sie folgendermaßen vor, um eine Meldungsvorlage zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Programmkontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.

3. Aktivieren Sie das Kontrollkästchen **Programmkontrolle aktivieren**, um Zugriff auf die Einstellungen der Komponente zu erhalten.

4. Klicken Sie auf die Schaltfläche **Vorlagen**.

   Das Fenster **Vorlagen für Nachrichten** wird geöffnet.

5. Führen Sie eine der folgenden Aktionen aus:

   - Um die Vorlage für eine Meldung über die Sperrung des Programmstarts zu ändern, wählen Sie die Registerkarte **Sperrung**.

   - Um die Vorlage für die Nachricht an den Administrator des lokalen Unternehmensnetzwerks zu ändern, wählen Sie die Registerkarte **Nachricht an den Administrator**.

6. Ändern Sie die Vorlage für die Sperrmeldung oder für die Nachricht an den Administrator. Verwenden Sie dazu die Schaltflächen **Standard** und **Variable**.

7. Klicken Sie auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Über die Modi für die Programmkontrolle

Die Komponente Programmkontrolle bietet zwei Modi:

- **Schwarze Liste**. In diesem Modus erlaubt die Programmkontrolle allen Benutzern den Start beliebiger Programme. Eine Ausnahme sind Programme, welche in den Verbotsregeln für die Programmkontrolle angegeben sind.

  Dieser Modus ist für die Programmkontrolle standardmäßig ausgewählt.

- **Weiße Liste**. In diesem Modus verbietet die Programmkontrolle allen Benutzern den Start beliebiger Programme. Eine Ausnahme sind Programme, welche in den Erlaubnisregeln der Programmkontrolle angegeben sind.

  Wenn eine extrem genaue Erlaubnisregel für die Programmkontrolle erstellt wurde, verbietet die Komponente den Start aller neuen Programme, die noch nicht vom Administrator des lokalen Unternehmensnetzwerks überprüft wurden, gewährleistet dabei aber die Funktionsfähigkeit des Betriebssystems und der bereits untersuchten Programme, die von Benutzern für dienstliche Zwecke benötigt werden.

  Beachten Sie die Tipps für die Anpassung von Kontrollregeln für Programme im Weiße-Liste-Modus.

In jedem Modus sind zwei Aktionen für zu startende Programme verfügbar: Kaspersky Endpoint Security kann entweder den Programmstart blockieren oder den Benutzer über den Start eines Programms benachrichtigen, das den Bedingungen der Regeln der Programmkontrolle entspricht.

Diese Modi für die Programmkontrolle können sowohl auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security als auch mithilfe von Kaspersky Security Center angepasst werden.

Allerdings verfügt Kaspersky Security Center über Tools, die auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht verfügbar sind und für folgende Aufgaben dienen:

- Programmkategorien erstellen

  Die Regeln der Programmkontrolle, die in der Verwaltungskonsole von Kaspersky Security Center erstellt wurden, beruhen auf den von Ihnen erstellten Programmkategorien, und nicht wie in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security auf ein- und ausschließenden Bedingungen.

- Empfang von Informationen über die Programme, die auf den Computern des lokalen Unternehmensnetzwerks installiert sind

Deshalb wird empfohlen, die Komponente Programmkontrolle mithilfe von Kaspersky Security Center anzupassen.

Modus der Programmkontrolle auswählen

Um einen Modus für die Programmkontrolle auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Programmkontrolle**.

Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.

3. Aktivieren Sie das Kontrollkästchen **Programmkontrolle aktivieren**, um Zugriff auf die Einstellungen der Komponente zu erhalten.

4. Wählen Sie in der Dropdown-Liste **Modus für die Programmkontrolle** eines der folgenden Elemente aus:

   - **Schwarze Liste**, wenn Sie den Start aller Programme erlauben möchten, unter Ausnahme jener Programme, die in Verbotsregeln angegeben sind.

   - **Weiße Liste**, wenn Sie den Start aller Programme verbieten möchten, unter Ausnahme jener Programme, die in Erlaubnisregeln angegeben sind.

     Für den Weiße-Liste-Modus sind standardmäßig folgende Regeln festgelegt: die Regel **Betriebssystem und seine Komponenten**, welche den Start von Programmen aus der KL-Kategorie "Goldene Kategorie" erlaubt, und die Regel **Vertrauenswürdige Programme mit Update-Funktionen**, welche den Start von Programmen aus der KL-Kategorie "Vertrauenswürdige Programme mit Update-Funktionen" erlaubt. Zur KL-Kategorie "Goldene Kategorie" gehören jene Programme, welche die normale Funktion des Betriebssystems gewährleisten. Zur KL-Kategorie "Vertrauenswürdige Programme mit Update-Funktionen" gehören Programme mit Update-Funktionen der gängigen Softwarehersteller. Diese Regeln können nicht gelöscht werden. Die Einstellungen dieser Regeln können nicht geändert werden. Standardmäßig ist die Regel **Betriebssystem und seine Komponenten** aktiviert, und die Regel **Vertrauenswürdige Programme mit Update-Funktionen** ist deaktiviert. Der Start von Programmen, welche den Auslösebedingungen dieser Regeln entsprechen, ist für alle Benutzer erlaubt.

   Wenn der Modus gewechselt wird, werden alle Regeln gespeichert, die in diesem Modus erstellt wurden. So ist eine erneute Verwendung der Regeln möglich. Um diese Regeln erneut zu verwenden, ist es ausreichend, den gewünschten Modus in der Dropdown-Liste **Modus für die Programmkontrolle** auszuwählen.

5. Wählen Sie in der Dropdown-Liste **Aktion** aus, welche Aktion die Komponente ausführen soll, wenn der Benutzer versucht, ein Programm auszuführen, das durch Regeln der Programmkontrolle verboten ist.

6. Aktivieren Sie das Kontrollkästchen **DLL und Treiber kontrollieren**, damit Kaspersky Endpoint Security das Laden von DLL-Modulen kontrolliert, wenn der Benutzer Programme startet.

   Informationen über das Modul und das Programm, das dieses Modul geladen hat, werden im Bericht gespeichert.

   Kaspersky Endpoint Security kontrolliert nur jene DLL-Module und Treiber, die geladen werden, nachdem das Kontrollkästchen **DLL und Treiber kontrollieren** aktiviert wurde. Starten Sie den Computer neu, nachdem das Kontrollkästchen **DLL und Treiber kontrollieren** aktiviert wurde. So wird gewährleistet, dass Kaspersky Endpoint Security alle DLL-Module und Treiber kontrolliert, einschließlich jener, die vor dem Start von Kaspersky Endpoint Security geladen wurden.

   Wenn die Funktion zur Kontrolle des Ladens von DLL-Modulen und Treibern aktiviert ist, vergewissern Sie sich, dass im Abschnitt **Programmkontrolle** entweder die Regel **Betriebssystem**

und seine Komponenten oder eine andere Regel aktiviert ist, welche die KL-Kategorie Vertrauenswürdige Zertifikate enthält und das Laden von DLL-Modulen und Treibern vor dem Start von Kaspersky Endpoint Security gewährleistet. Wenn die Kontrolle von DLL-Modulen und Treibern gleichzeitig mit der Regel **Betriebssystem und seine Komponenten** aktiviert ist, kann es zur Instabilität des Betriebssystems kommen.

Regeln der Programmkontrolle, die auf Basis anderer KL-Kategorien erstellt wurden (unter Ausnahme der KL-Kategorie Vertrauenswürdige Zertifikate) werden bei der Kontrolle des Ladens von DLL-Modulen und Treibern nicht angewendet.

Es wird empfohlen, den Kennwortschutz für die Programmeinstellungen zu aktivieren, damit jene Verbotsregeln deaktiviert werden können, die den Start von DLL-Modulen und Treibern mit kritischer Priorität blockieren, ohne dazu die Richtlinieneinstellungen für Kaspersky Security Center zu ändern.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Regeln der Programmkontrolle mithilfe von Kaspersky Security Center verwalten

Dieser Abschnitt informiert darüber, wie die Programmkontrolle mithilfe von Kaspersky Security Center angepasst wird, und bietet Tipps zur optimalen Verwendung der Programmkontrolle.

Empfang von Informationen über die Programme, die auf Benutzercomputern installiert sind

Um optimale Regeln der Programmkontrolle zu erstellen, sollte bekannt sein, welche Programme auf den Computern des lokalen Unternehmensnetzwerks eingesetzt werden. Dazu können Sie folgende Informationen erhalten:

- Hersteller, Versionen und Sprachversionen der Programme, die im lokalen Unternehmensnetzwerk verwendet werden
- Häufigkeit von Programm-Updates
- im Unternehmen geltende Richtlinien für die Nutzung von Programmen (Dies können Sicherheitsrichtlinien oder administrative Richtlinien sein.)
- Speicherort für Programmpakete

Um Informationen über die Programme zu erhalten, die auf den Computern des lokalen Unternehmensnetzwerks im Einsatz sind, können Sie Daten aus den Ordnern **Programm-Registry** und **Ausführbare Dateien** verwenden. Die Ordner **Programm-Registry** und **Ausführbare Dateien** gehören zum Ordner **Programmverwaltung** in der Verwaltungskonsolenstruktur von Kaspersky Security Center.

Der Ordner **Programmverzeichnis** enthält eine Liste von Programmen, die der Administrationsagent auf den Client-Computern gefunden hat, auf denen er installiert ist.

Der Ordner **Ausführbare Dateien** enthält eine Liste mit den ausführbaren Dateien, die bisher auf dem Client-Computern gestartet oder bei einer Inventarisierungsaufgabe für Kaspersky Endpoint Security gefunden wurden.

Im Eigenschaftenfenster eines gewählten Programms finden Sie im Ordner **Programm-Registry** oder **Ausführbare Dateien** allgemeine Informationen über das Programm und über seine ausführbaren Dateien. Außerdem steht eine Liste der Computer bereit, auf denen dieses Programm installiert ist.

Empfang von Informationen über die Programme, die auf Benutzercomputern gestartet werden

Um den Versand von Informationen über die Programme, die auf Computern, auf welchem das Programm Kaspersky Endpoint Security installiert ist, ausgeführt werden, an den Administrationsserver zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Berichte und Speicher** aus.
7. Klicken Sie im rechten Fensterbereich im Block **Datenübertragung an den Administrationsserver** auf **Einstellungen**.

   Das Fenster **Informieren** wird geöffnet.
8. Aktivieren Sie das Kontrollkästchen **Über gestartete Programme**.
9. Klicken Sie im Fenster **Informieren** auf **OK**.
10. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**.

Programmkategorien erstellen

Um das Anlegen von Regeln der Programmkontrolle zu vereinfachen, können Sie Programmkategorien erstellen.

Es wird empfohlen, die Kategorie "Programme für die Arbeit" zu erstellen und eine Standardauswahl von Programmen in diese Kategorie aufzunehmen, die im Unternehmen eingesetzt werden. Falls bestimmte Benutzergruppen unterschiedliche Programmsets einsetzen, können Sie für jede Benutzergruppe eine separate Programmkategorie erstellen.

Gehen Sie folgendermaßen vor, um eine Programmkategorie zu erstellen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert** → **Programmverwaltung** → **Programmkategorien**.
3. Klicken Sie im Arbeitsbereich auf **Kategorie erstellen**.

   Der Assistent zum Erstellen einer benutzerdefinierten Kategorie wird gestartet.
4. Folgen Sie den Anweisungen des Assistenten zum Erstellen einer benutzerdefinierten Kategorie.

Schritt 1. Kategorietyp auswählen

Wählen Sie bei diesem Schritt einen der folgenden Typen für die Programmkategorien aus:

- **Manuell zu erweiternde Kategorie**. Wenn Sie diesen Kategorietyp ausgewählt haben, können Sie beim Schritt "Legen Sie die Bedingungen für die Aufnahme der Programme in die Kategorie fest" und beim Schritt "Legen Sie die Bedingungen für den Ausschluss der Programme aus der Kategorie fest" jene Kriterien festlegen, nach denen ausführbare Dateien in die erstellte Kategorie aufgenommen werden sollen.
- **Kategorie für ausführbare Dateien der gewählten Geräte**. Wenn Sie diesen Kategorietyp ausgewählt haben, können Sie beim Schritt "Einstellungen" ein Gerät angeben, dessen ausführbare Dateien in diese Kategorie aufgenommen werden sollen.
- **Automatisch zu erweiternde Kategorie**. Geben Sie einen Ordner an, der ausführbare Dateien enthält, die automatisch in die erstellte Kategorie aufgenommen werden sollen.

  Wenn eine automatisch zu erweiternde Kategorie erstellt wird, führt Kaspersky Security Center die Inventarisierung für Dateien der folgenden Formate aus: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR.

Schritt 2. Geben Sie den Namen der Benutzerkategorie ein.

Geben Sie bei diesem Schritt einen Namen für die Programmkategorie an.

Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**.

Schritt 3. Legen Sie die Bedingungen für die Aufnahme der Programme in die Kategorie fest.

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Manuell zu erweiternde Kategorie** ausgewählt haben.

Wählen Sie bei diesem Schritt in der Dropdown-Liste **Hinzufügen** eines oder mehrere der folgenden Kriterien aus, nach denen Bedingungen für die Aufnahme von Programmen in diese Kategorie hinzugefügt werden sollen:

- **Aus der Liste ausführbarer Dateien**. Fügen Sie Programme aus der Liste für ausführbare Dateien auf dem Client-Gerät zu der benutzerdefinierten Kategorie hinzu.
- **Aus den Dateieigenschaften**. Geben Sie präzise Daten für die ausführbaren Dateien an. Diese Daten dienen als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie.
- **Metadaten der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Metadaten dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.
- **Hash-Werte der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Hash-Werte dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.
- **Zertifikate der Dateien im Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien, die mit Zertifikaten signiert sind, enthält. Kaspersky Security Center gibt die Zertifikate dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

  Es wird davon abgeraten, Bedingungen zu verwenden, in denen der Parameter **Fingerabdruck des Zertifikats** nicht angegeben ist.

- **Metadaten der Dateien des msi-Installers**. Wählen Sie ein MSI-Installationspaket aus. Kaspersky Security Center gibt die Metadaten der ausführbaren Dateien, welche in diesem MSI-Installationspaket enthalten sind, als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.
- **Prüfsummen der Dateien des msi-Installers für das Programm**. Wählen Sie ein MSI-Installationspaket aus. Kaspersky Security Center gibt die Hash-Werte der ausführbaren Dateien, welche in diesem MSI-Installationspaket enthalten sind, als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.
- **KL-Kategorie**. Geben Sie eine KL-Kategorie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

  Eine KL-Kategorie ist eine von den Kaspersky-Lab-Experten erstellte Liste für Programme mit gemeinsamen thematischen Merkmalen. Zur KL-Kategorie "Office-Programme" gehören

beispielsweise Programme aus den Paketen Microsoft Office, Adobe Acrobat und anderen.

Sie können alle KL-Kategorien auswählen, um eine erweiterte Liste mit vertrauenswürdigen Programme zu erstellen.

- **Programmordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus. Kaspersky Security Center nimmt die ausführbaren Dateien aus diesem Ordner in die benutzerdefinierte Kategorie auf.
- **Zertifikate aus der Zertifikatsdatenverwaltung**. Wählen Sie ein Zertifikat aus der Zertifikatsdatenverwaltung als Bedingung für die Aufnahme von Programmen in die benutzerdefinierte Kategorie aus.

  Es wird davon abgeraten, Bedingungen zu verwenden, in denen der Parameter **Fingerabdruck des Zertifikats** nicht angegeben ist.

- **Datenträgertyp**. Geben Sie einen Datenträgertyp (alle Festplatten und Wechseldatenträger, oder nur Wechseldatenträger) als Bedingung für die Aufnahme von Programmen in die benutzerdefinierte Kategorie an.

Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**.

Schritt 4. Legen Sie die Bedingungen für den Ausschluss der Programme aus der Kategorie fest.

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Manuell zu erweiternde Kategorie** ausgewählt haben.

Die Programme, die bei diesem Schritt angegeben werden, werden auch dann aus der Kategorie ausgeschlossen, wenn diese Programme beim Schritt "Legen Sie die Bedingungen für die Aufnahme der Programme in die Kategorie fest" angegeben wurden.

Wählen Sie bei diesem Schritt in der Dropdown-Liste **Hinzufügen** eines der folgenden Kriterien aus, nach dem Bedingungen für den Ausschluss von Programmen aus dieser Kategorie hinzugefügt werden sollen:

- **Aus der Liste ausführbarer Dateien**. Fügen Sie Programme aus der Liste für ausführbare Dateien auf dem Client-Gerät zu der benutzerdefinierten Kategorie hinzu.
- **Aus den Dateieigenschaften**. Geben Sie präzise Daten für die ausführbaren Dateien an. Diese Daten dienen als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie.
- **Metadaten der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Metadaten dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Hash-Werte der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Hash-Werte dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Zertifikate der Dateien im Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien, die mit Zertifikaten signiert sind, enthält. Kaspersky Security Center gibt die Zertifikate dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Metadaten der Dateien des msi-Installers**. Wählen Sie ein MSI-Installationspaket aus. Kaspersky Security Center gibt die Metadaten der ausführbaren Dateien, welche in diesem MSI-Installationspaket enthalten sind, als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Prüfsummen der Dateien des msi-Installers für das Programm**. Wählen Sie ein MSI-Installationspaket aus. Kaspersky Security Center gibt die Hash-Werte der ausführbaren Dateien, welche in diesem MSI-Installationspaket enthalten sind, als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **KL-Kategorie**. Geben Sie eine KL-Kategorie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Programmordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus. Kaspersky Security Center nimmt die ausführbaren Dateien aus diesem Ordner in die benutzerdefinierte Programmkategorie auf.

- **Zertifikate aus der Zertifikatsdatenverwaltung**. Wählen Sie ein Zertifikat aus der Zertifikatsdatenverwaltung als Bedingung für die Aufnahme von Programmen in die benutzerdefinierte Kategorie aus.

- **Datenträgertyp**. Geben Sie einen Datenträgertyp (alle Festplatten und Wechseldatenträger, oder nur Wechseldatenträger) als Bedingung für die Aufnahme von Programmen in die benutzerdefinierte Kategorie an.

Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**.

Schritt 5. Einstellungen

> Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Kategorie für ausführbare Dateien der gewählten Geräte** ausgewählt haben.

Klicken Sie bei diesem Schritt auf **Hinzufügen** und geben Sie die Computer an, deren ausführbare Dateien Kaspersky Security Center in die Programmkategorie aufnehmen soll. Kaspersky Security Center fügt der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzu, die sich im Ordner Ausführbare Dateien befinden.

Bei diesem Schritt können Sie außerdem die folgenden Einstellungen anpassen:

- Algorithmus zur Berechnung der Hash-Funktion durch das Programm Kaspersky Security Center Um einen Algorithmus auszuwählen, muss eines der folgenden Kontrollkästchen aktiviert werden:

- Kontrollkästchen **SHA-256 für die Dateien der Kategorie berechnen (unterstützt für Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)**.

- Kontrollkästchen **MD5 für die Dateien der Kategorie berechnen (unterstützt für Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

- Kontrollkästchen **Mit der Datenverwaltung des Administrationsservers synchronisieren**. Aktivieren Sie dieses Kontrollkästchen, damit Kaspersky Security Center die Programmkategorie regelmäßig bereinigt und zu der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzufügt, die sich im Ordner **Ausführbare Dateien** befinden.

  Ist das Kontrollkästchen **Mit der Datenverwaltung des Administrationsservers synchronisieren** deaktiviert ist, so nimmt Kaspersky Security Center nach der Erstellung der Programmkategorie in dieser Kategorie keine Änderungen vor.

- Feld **Untersuchungsintervall (Std.)**. In diesem Feld können Sie den Zeitraum (in Stunden) angeben, nach dessen Ablauf Kaspersky Security Center die Programmkategorie bereinigt und zu der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzufügt, die sich im Ordner **Ausführbare Dateien** befinden.

  Das Feld ist verfügbar, wenn das Kontrollkästchen **Mit der Datenverwaltung des Administrationsservers synchronisieren** aktiviert ist.

Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**.

Schritt 6. Ordner der Datenverwaltung

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Automatisch zu erweiternde Kategorie** ausgewählt haben.

Klicken Sie bei diesem Schritt auf **Durchsuchen** und geben Sie einen Ordner an, den Kaspersky Security Center nach ausführbaren Dateien durchsuchen soll, um diese automatisch zu der Programmkategorie hinzuzufügen.

Bei diesem Schritt können Sie außerdem die folgenden Einstellungen anpassen:

- Kontrollkästchen **Dynamic Link Libraries (.dll) zur Kategorie hinzufügen**. Aktivieren Sie dieses Kontrollkästchen, damit dynamische Programmbibliotheken (Dateiformat DLL) in die Programmkategorie aufgenommen werden und damit die Komponente Programmkontrolle die Aktionen dieser Bibliotheken, die im System ausgeführt werden, registriert.

  Wenn Dateien im DLL-Format in die Programmkategorie aufgenommen werden, kann sich die Leistungsfähigkeit von Kaspersky Security Center vermindern.

- Kontrollkästchen **Daten zu Skripten in die Kategorie aufnehmen**. Aktivieren Sie dieses Kontrollkästchen, damit Daten über Skripte in die Programmkategorie aufgenommen und damit Skripte von der Komponente Schutz vor Web-Bedrohungen nicht blockiert werden.

Wenn Daten über Skripte in die Programmkategorie aufgenommen werden, kann sich die Leistungsfähigkeit von Kaspersky Security Center vermindern.

- Algorithmus zur Berechnung der Hash-Funktion durch das Programm Kaspersky Security Center Um einen Algorithmus auszuwählen, muss eines der folgenden Kontrollkästchen aktiviert werden:
  - Kontrollkästchen **SHA-256 für die Dateien der Kategorie berechnen (unterstützt für Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)**.
  - Kontrollkästchen **MD5 für die Dateien der Kategorie berechnen (unterstützt für Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.
- Kontrollkästchen **Prüfung des Ordners auf Änderungen erzwingen**. Aktivieren Sie dieses Kontrollkästchen, damit Kaspersky Security Center den Ordner, der zur automatischen Ergänzung der Programmkategorie dient, regelmäßig nach ausführbaren Dateien durchsucht.

  Ist das Kontrollkästchen **Prüfung des Ordners auf Änderungen erzwingen** deaktiviert, so durchsucht Kaspersky Security Center den Ordner, der zur automatischen Ergänzung der Programmkategorie dient, nur dann, wenn der Ordner geändert wurde, ihm Dateien hinzugefügt oder Dateien daraus gelöscht wurden.
- Feld **Untersuchungsintervall (Std.)**. In diesem Feld können Sie angeben, nach welchem Zeitraum (in Stunden) Kaspersky Security Center überprüfen soll, ob der Ordner, der zur automatischen Ergänzung der Programmkategorie dient, verändert wurde.

  Das Feld ist verfügbar, wenn das Kontrollkästchen **Prüfung des Ordners auf Änderungen erzwingen** aktiviert ist.

Um den Installationsassistenten für das Programm fortzusetzen, klicken Sie auf **Weiter**.

Schritt 7. Benutzerkategorie erstellen

Um den Installationsassistenten abzuschließen, klicken Sie auf **Fertig**.

Regeln der Programmkontrolle mithilfe von Kaspersky Security Center hinzufügen und ändern

Um mithilfe von Kaspersky Security Center eine Regel für die Programmkontrolle hinzuzufügen oder zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:

- Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
- Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

6. Wählen Sie im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Programmkontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.

7. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf **Hinzufügen**, wenn Sie eine Regel hinzufügen möchten.
   - Wenn Sie eine vorhandene Regel ändern möchten, wählen Sie in der Liste eine Regel und klicken Sie auf **Ändern**.

   Das Fenster **Regel der Programmkontrolle** wird geöffnet.

8. Wählen Sie in der Dropdown-Liste **Kategorie** die erstellte Programmkategorie, auf deren Basis Sie eine Regel erstellen möchten.

9. Klicken Sie in der Tabelle **Subjekte und deren Rechte** auf **Hinzufügen**.

   Das Windows-Standardfenster **Auswahl: "Benutzer" oder "Gruppen"** wird geöffnet.

10. Legen Sie im Fenster **Auswahl: "Benutzer" oder "Gruppen"** eine Liste mit Benutzern und/oder Benutzergruppen an, für welche Sie die Möglichkeit zum Starten eines Programms anpassen möchten, das zur ausgewählten Kategorie gehört.

11. Gehen Sie in der Tabelle **Subjekte und deren Rechte** wie folgt vor:

    - Um Benutzern und/oder Benutzergruppen den Start von Programmen, die zur ausgewählten Kategorie gehören, zu erlauben, aktivieren Sie das Kontrollkästchen **Erlauben** in den entsprechenden Zeilen.
    - Um Benutzern und/oder Benutzergruppen den Start von Programmen, die zur ausgewählten Kategorie gehören, zu verbieten, aktivieren Sie das Kontrollkästchen **Verbieten** in den entsprechenden Zeilen.

12. Aktivieren Sie das Kontrollkästchen **Für die übrigen Benutzer verbieten**, damit das Programm den Start von Programmen aus der gewählten Kategorie für alle Benutzer verbietet, die nicht in der Spalte **Subjekt** angegeben sind und die nicht zu den in der Spalte **Subjekt** angegebenen Benutzergruppen gehören.

13. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen**, damit Programme, welche die Auslösebedingungen der Regel erfüllen, von Kaspersky Endpoint Security als vertrauenswürdige Programme mit Update-Funktionen betrachtet werden, die berechtigt sind, andere ausführbare Dateien, deren Start künftig zugelassen wird, zu erstellen.

14. Klicken Sie auf **OK**.

15. Klicken Sie im Abschnitt **Programmkontrolle** des Eigenschaftenfensters der Richtlinie auf **Übernehmen**.

Ändern des Status einer Regel der Programmkontrolle mithilfe von Kaspersky Security Center

Um den Status einer Regel der Programmkontrolle zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Programmkontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.
7. Wählen Sie die Regel der Programmkontrolle, deren Status Sie ändern möchten.
8. Öffnen Sie in der Spalte **Status** durch Linksklick das Kontextmenü und wählen Sie einen der folgenden Punkte aus:
   - **Ein**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ verwendet wird.
   - **Aus**. Dieser Status bedeutet, dass die Regel nicht von der Komponente „Programmkontrolle“ verwendet wird.
   - **Test**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, auf welche die Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

     Mithilfe des Status **Test** können Sie für einen Teil der Regeln die Aktion **Benachrichtigen** festlegen, wenn in der Dropdown-Liste **Aktion** die Variante **Blockieren** ausgewählt ist.
9. Klicken Sie auf **Übernehmen**.

Regeln der Programmkontrolle mithilfe von Kaspersky Security Center testen

Um sicherzustellen, dass Programme, die Sie zum Arbeiten benötigen, nicht durch Regeln der Programmkontrolle blockiert werden, wird empfohlen, für neu erstellte Regeln den Testmodus zu aktivieren und ihre Funktion zu analysieren. Wenn der Testmodus aktiviert ist, werden Programme, für welche der Start durch Regeln der Programmkontrolle verboten ist, von Kaspersky Endpoint Security nicht blockiert. Es werden aber Benachrichtigungen über ihren Start an den Administrationsserver gesendet.

Für die Funktionsanalyse von Regeln der Programmkontrolle müssen die Ereignisse aus den Ausführungsresultaten der Komponente Programmkontrolle überprüft werden, die bei Kaspersky Security Center eintreffen. Wenn alle Programme, die der Benutzer zum Arbeiten benötigt, erfolgreich gestartet wurden, sind die Regeln korrekt. Andernfalls sollten die Einstellungen der von Ihnen erstellten Regeln genauer angepasst werden.

Der Testmodus für die Regeln der Programmkontrolle ist standardmäßig deaktiviert.

Um den Testmodus für die Regeln der Programmkontrolle in Kaspersky Security Center zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Programmkontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Programmkontrolle angezeigt.
7. Wählen Sie in der Dropdown-Liste **Modus für die Programmkontrolle** eines der folgenden Elemente aus:
   - **Schwarze Liste**, wenn Sie den Start aller Programme erlauben möchten, unter Ausnahme jener Programme, die in Verbotsregeln angegeben sind.
   - **Weiße Liste**, wenn Sie den Start aller Programme verbieten möchten, unter Ausnahme jener Programme, die in Erlaubnisregeln angegeben sind.
8. Wählen Sie in der Dropdown-Liste **Aktion** eines der folgenden Elemente aus:
   - **Benachrichtigen**. Testmodus für die Regeln der Programmkontrolle aktivieren
   - **Blockieren**. Testmodus für die Regeln der Programmkontrolle deaktivieren

9. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Ereignisse über die Arbeit der Komponente Programmkontrolle im Testmodus anzeigen

Um die Ereignisse anzuzeigen, die aus den Ausführungsresultaten der Komponente Programmkontrolle im Testmodus stammen und bei Kaspersky Security Center eintreffen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse**.
3. Klicken Sie auf **Auswahl erstellen**.

   Das Fenster **Eigenschaften: <Name der Auswahl>** wird geöffnet.
4. Öffnen Sie den Abschnitt **Ereignisse**.
5. Klicken Sie auf **Alle zurücksetzen**.
6. Aktivieren Sie in der Tabelle **Ereignisse** die Kontrollkästchen **Der Programmstart wurde im Testmodus verboten** und **Der Programmstart wurde im Testmodus erlaubt**.
7. Klicken Sie auf **OK**.
8. Wählen Sie in der Liste **Ereignisse für Auswahl** die erstellte Auswahl aus.
9. Klicken Sie auf **Auswahl starten**.

Bericht über Starts, die im Testmodus verboten wurden, anzeigen

Um einen Bericht über im Testmodus verbotene Starts anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte**.
3. Klicken Sie auf **Berichtsvorlage erstellen**.

   Der Assistent für das Erstellen einer Berichtsvorlage wird gestartet.
4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie beim Schritt **Typ der Berichtsvorlage auswählen** im Abschnitt **Sonstiges** den Punkt **Bericht über im Testmodus verbotene Starts** aus.

   Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.

5. Wählen Sie die Berichtsvorlage, die Sie bei den vorherigen Schritten der Anleitung erstellt haben.
6. Wählen Sie im Kontextmenü der Vorlage den Punkt **Bericht anzeigen** aus.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Ereignisse über die Arbeit der Komponente Programmkontrolle anzeigen

Um die Ereignisse anzuzeigen, die aus den Ausführungsresultaten der Komponente Programmkontrolle stammen und bei Kaspersky Security Center eintreffen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse**.
3. Klicken Sie auf **Auswahl erstellen**.

   Das Fenster **Eigenschaften: <Name der Auswahl>** wird geöffnet.
4. Öffnen Sie den Abschnitt **Ereignisse**.
5. Klicken Sie auf **Alle zurücksetzen**.
6. Aktivieren Sie in der Tabelle **Ereignisse** das Kontrollkästchen **Der Programmstart wurde verboten**.
7. Klicken Sie auf **OK**.
8. Wählen Sie in der Liste **Ereignisse für Auswahl** die erstellte Auswahl aus.
9. Klicken Sie auf **Auswahl starten**.

Bericht über verbotene Starts anzeigen

Um einen Bericht über verbotene Starts anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte**.
3. Klicken Sie auf **Berichtsvorlage erstellen**.

   Der Assistent für das Erstellen einer Berichtsvorlage wird gestartet.
4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie beim Schritt **Typ der Berichtsvorlage auswählen** im Abschnitt **Sonstiges** den Punkt **Bericht über verbotene Starts** aus.

Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.

5. Wählen Sie die Berichtsvorlage, die Sie bei den vorherigen Schritten der Anleitung erstellt haben.

6. Wählen Sie im Kontextmenü der Vorlage den Punkt **Bericht anzeigen** aus.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Tipps für die Einführung des Weiße-Liste-Modus

Dieser Abschnitt enthält Empfehlungen für die Einführung des Weiße-Liste-Modus.

Planung der Einführung des Weiße-Liste-Modus

Für die Planung der Einführung des Weiße-Liste-Modus wird folgendes Vorgehen empfohlen:

1. Zusammensetzung der folgenden Kategorien festlegen:

   - Benutzergruppen Gruppen mit Benutzern, für welche die Verwendung unterschiedlicher Sätze von Programmen erlaubt werden soll.

   - Administrationsgruppen Eine oder mehrere Computergruppen, auf welche Kaspersky Security Center den Weiße-Liste-Modus anwendet. Die Erstellung mehrerer Computergruppen ist erforderlich, wenn für diese Gruppen unterschiedliche Einstellungen für den Weiße-Liste-Modus gelten.

2. Liste mit Programmen, deren Start erlaubt werden soll, erstellen

   Bevor diese Liste erstellt wird, sollte die Inventarisierungsaufgabe ausgeführt und die Option aktiviert werden, mit der Informationen über die Programme, welche auf dem Computer gestartet wurden, an den Administrationsserver gesendet werden. Nachdem die Inventarisierungsaufgabe ausgeführt wurde, können Sie eine Liste der ausführbaren Dateien anzeigen. Informationen über die Erstellung, die Einstellungsänderungen und den Start der Inventarisierungsaufgabe sind im Abschnitt Aufgabenverwaltung verfügbar.

Weiße-Liste-Modus anpassen

Um den Weiße-Liste-Modus anzupassen, wird folgendes Vorgehen empfohlen:

1. Erstellung von Programmkategorien, die jene Programme enthalten, deren Start erlaubt werden soll

   Sie können einen der folgenden Typen für die Programmkategorien auswählen:

   - Manuell zu erweiternde Kategorie. Sie können diese Kategorie unter Verwendung der folgenden Bedingungen manuell ergänzen:

     - Metadaten einer Datei. Wenn diese Bedingung verwendet wird, nimmt Kaspersky Security Center alle ausführbaren Dateien, welche die angegebenen Metadaten besitzen, in die Programmkategorie auf.

- Datei-Hash. Wenn diese Bedingung verwendet wird, nimmt Kaspersky Security Center alle ausführbaren Dateien, welche den angegebenen Hash besitzen, in die Programmkategorie auf.

  Wenn diese Bedingung verwendet wird, ist die automatische Installation von Updates nicht möglich, da die Dateien der einzelnen Versionen einen unterschiedlichen Hash besitzen.

- Zertifikat einer Datei. Wenn diese Bedingung verwendet wird, nimmt Kaspersky Security Center alle ausführbaren Dateien, welche mit dem angegebenen Zertifikat signiert sind, in die Programmkategorie auf.

- KL-Kategorie. Wenn diese Bedingung verwendet wird, nimmt Kaspersky Security Center alle ausführbaren Dateien, welche zur angegebenen KL-Kategorie gehören, in die Programmkategorie auf.

- Automatisch zu erweiternde Kategorie. Sie können einen Ordner angeben, der ausführbare Dateien enthält, die automatisch in die erstellte Programmkategorie aufgenommen werden sollen.

  Die Verwendung dieser Kategorie ist riskant, da der Start aller Programme aus dem angegebenen Ordner erlaubt wird.

  In einer Programmkategorie dieses Typs wird nur eine Dateiversion gespeichert – entweder die alte oder die aktualisierte Version. Dies schließt die Möglichkeit einer automatischen Installation von Updates aus, da die Updates nicht gleichzeitig auf den Computern installiert werden.

- Kategorie für ausführbare Dateien der gewählten Geräte. Sie können einen Computer angeben, dessen ausführbare Dateien automatisch in die erstellte Programmkategorie aufgenommen werden sollen.

  Bei Verwendung dieses Typs von Programmkategorien erhält Kaspersky Security Center die Informationen über die Programme auf dem Computer aus der Liste ausführbarer Dateien.

2. Weiße-Liste-Modus für die Komponente Programmkontrolle auswählen

3. Regeln der Programmkontrolle unter Verwendung der erstellten Programmkategorien erstellen

Weiße-Liste-Modus testen

Um den Weiße-Liste-Modus zu testen, wird folgendes Vorgehen empfohlen:

1. Testzeitraum festlegen (von mehreren Tagen bis zu zwei Monaten)

2. Testmodus für die Regeln der Programmkontrolle aktivieren

3. Analyse der Testergebnisse unter Verwendung von Ereignissen und Berichten über die Arbeit der Komponente Programmkontrolle im Testmodus (Ereignisse über die Arbeit der Komponente Programmkontrolle im Testmodus anzeigen, Bericht über Starts, die bei Tests verboten wurden, anzeigen)

   Es wird empfohlen, aufgrund der Testergebnisse jene Programme zu ermitteln, für welche die automatische Update-Installation erlaubt werden muss.

   Sie können die automatische Installation von Updates auf folgende Weise erlauben:

   - Angabe einer erweiterten Liste für erlaubte Programme, indem entweder alle Programme, die zu einer KL-Kategorie gehören, erlaubt werden, oder alle Programme, die mit einem Zertifikat signiert sind, erlaubt werden.

     Um den Start alle Programme die mit einem Zertifikat signiert sind, zu erlauben, können Sie eine Kategorie mit einer Bedingung erstellen, die auf einem Zertifikat basiert und in welcher nur der Parameter **Subjekt** mit dem Wert * verwendet wird.

   - Für die Regel der Programmkontrolle den Parameter **Vertrauenswürdige Programme mit Update-Funktionen** festlegen. Ist das Kontrollkästchen aktiviert, so werden Programme, welche die Auslösebedingungen der Regel erfüllen, von Kaspersky Endpoint Security als vertrauenswürdige Programme mit Update-Funktionen betrachtet, die berechtigt sind, andere ausführbare Dateien, deren Start künftig zugelassen wird, zu erstellen.

   - Programmkategorie auf Basis der Kategorie **Programmordner** erstellen. Bei Verwendung dieser Methode werden alle ausführbaren Dateien, die sich im angegebenen Ordner befinden, zu der Programmkategorie hinzugefügt.

     Die Verwendung dieses Kriteriums ist riskant, da der Start aller Programme aus dem angegebenen Ordner erlaubt wird.

4. Einstellungen für den Weiße-Liste-Modus unter Berücksichtigung der Analyseergebnisse ändern

Unterstützung des Weiße-Liste-Modus

Nachdem der Testmodus für die Regeln der Programmkontrolle deaktiviert wurde, sollte die Unterstützung des Weiße-Liste-Modus fortgesetzt werden. Dazu dient folgendes Vorgehen:

- Funktionsanalyse der Regeln der Programmkontrolle unter Verwendung von Ereignissen und Berichten über die Arbeit der Komponente Programmkontrolle (Bericht über verbotene Starts anzeigen, Ereignisse über die Arbeit der Komponente Programmkontrolle anzeigen), sowie von Benutzeranfragen für den Zugriff auf Programme

- Analyse von unbekannten Dateien durch eine Reputations-Überprüfung in Kaspersky Security Network oder beim Portal Kaspersky Whitelist

- Erforderliche Programme zu Programmkategorien hinzufügen

Gerätekontrolle

Diese Komponente ist verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Dateiserver installiert ist.

Dieser Abschnitt informiert über die Gerätekontrolle und erklärt die Einstellungen der Komponente.

Über die Gerätekontrolle

Die Gerätekontrolle beschränkt den Zugriff von Benutzern auf Geräte, die auf dem Computer installiert oder mit diesem verbunden sind, und gewährleistet somit die Sicherheit vertraulicher Daten:

- Speichergeräte (Festplatten, Wechseldatenträger, Bandlaufwerke, CD/DVD-Laufwerke)
- Datenübertragungsgeräte (Modems, externe Netzwerkkarten)
- Geräte, die Informationen in Druckerzeugnisse umwandeln (Drucker)
- Schnittstellen, mit deren Hilfe Geräte mit einem Computer verbunden werden können (z. B. USB, FireWire und Infrarot)

Die Gerätekontrolle reguliert den Zugriff von Benutzern auf Geräte mithilfe von *Zugriffsregeln für Geräte* (im Folgenden auch "Zugriffsregeln") und *Zugriffsregeln für Schnittstellen*.

Gerätekontrolle aktivieren und deaktivieren

Die Gerätekontrolle ist standardmäßig aktiviert. Bei Bedarf können Sie die Gerätekontrolle deaktivieren.

Um die Gerätekontrolle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Gerätekontrolle aktivieren**, um die Gerätekontrolle einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Gerätekontrolle aktivieren**, um die Gerätekontrolle auszuschalten.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Über die Zugriffsregeln für Geräte und Schnittstellen

Bei der Zugriffsregel für Geräte handelt es sich um eine Kombination von Einstellungen, welche die folgenden Funktionen der Komponente Gerätekontrolle festlegen:

- Zugriff auf Gerätetypen für ausgewählte Benutzer und / oder Benutzergruppen in bestimmten Zeiträumen erlauben

  Sie können einen Benutzer und / oder eine Benutzergruppe wählen und für diese einen Zugriffszeitplan für Geräte erstellen.

- Rechte zum Lesen des Inhalts des Gerätespeichers festlegen

- Rechte zum Ändern des Inhalts des Gerätespeichers festlegen

Standardmäßig sind für alle Gerätetypen aus der Klassifikation der Komponente Gerätekontrolle Zugriffsregeln erstellt, die allen Benutzern jederzeit den vollständigen Zugriff auf alle Geräte erlauben, wenn der Zugriff auf die Schnittstellen für die entsprechenden Gerätetypen erlaubt ist.

Eine Zugriffsregel für eine Schnittstelle definiert die Erlaubnis oder das Verbot für den Zugriff auf eine Schnittstelle.

Für alle Schnittstellen aus der Klassifikation der Komponente Gerätekontrolle sind standardmäßige Regeln erstellt, die den Zugriff auf die Schnittstellen erlauben.

Zugriffsregeln für Geräte und Zugriffsregeln für Schnittstellen können nicht erstellt oder gelöscht, sondern nur geändert werden.

Über vertrauenswürdige Geräte

Vertrauenswürdige Geräte sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Geräts angegeben sind, jederzeit vollständigen Zugriff besitzen.

Für die Arbeit mit vertrauenswürdigen Geräten sind folgende Aktionen verfügbar:

- Hinzufügen des Geräts zur Liste der vertrauenswürdigen Geräte

- Ändern des Benutzers und / oder der Benutzergruppen, denen der Zugriff auf ein vertrauenswürdiges Gerät erlaubt wird

- Löschen eines Geräts aus der Liste der vertrauenswürdigen Geräte

Wenn ein Gerät auf der Liste der vertrauenswürdigen Geräte steht, für Geräte dieses Typs aber eine Regel vorhanden ist, die den Zugriff verbietet oder einschränkt, so besitzt im Hinblick auf eine Zugriffserlaubnis für das Gerät die Zugehörigkeit zur Liste der vertrauenswürdigen Geräte eine höhere Priorität als die Zugriffsregel.

Typische Entscheidungen über den Zugriff auf Geräte

Kaspersky Endpoint Security entscheidet über den Zugriff auf ein Gerät, sobald dieses vom Benutzer an den Computer angeschlossen wird.

Nr.	Ausgangsbedingungen	Zwischenschritte vor der Entscheidung über den Zugriff auf das Gerät			Entscheidung über den Zugriff auf das Gerät
		Prüfung, ob das angeschlossene Gerät in der Liste der vertrauenswürdigen Geräte enthalten ist	Prüfung des Zugriffs auf das Gerät mithilfe einer Zugriffsregel	Prüfung des Zugriffs auf die Schnittstelle mithilfe einer Regel für den Zugriff auf Schnittstellen	
1	Das Gerät ist nicht in der Klassifikation der Komponente Gerätekontrolle enthalten.	Nicht in der Liste der vertrauenswürdigen Geräte.	Keine Zugriffsregel.	Keine Untersuchung.	Zugriff erlaubt.
2	Es handelt sich um ein vertrauenswürdiges Gerät.	In der Liste der vertrauenswürdigen Geräte enthalten.	Keine Untersuchung.	Keine Untersuchung.	Zugriff erlaubt.
3	Zugriff auf das Gerät erlaubt.	Nicht in der Liste der vertrauenswürdigen Geräte.	Zugriff erlaubt.	Keine Untersuchung.	Zugriff erlaubt.
4	Zugriff auf das Gerät hängt von der Schnittstelle ab.	Nicht in der Liste der vertrauenswürdigen Geräte.	Zugriff hängt von der Schnittstelle ab.	Zugriff erlaubt.	Zugriff erlaubt.
5	Zugriff auf das Gerät hängt von der Schnittstelle ab.	Nicht in der Liste der vertrauenswürdigen Geräte.	Zugriff hängt von der Schnittstelle ab.	Zugriff verboten.	Zugriff verboten.
6	Zugriff auf das Gerät erlaubt. Keine Regel für den Zugriff auf Schnittstellen vorhanden.	Nicht in der Liste der vertrauenswürdigen Geräte.	Zugriff erlaubt.	Keine Regel für den Zugriff auf Schnittstellen.	Zugriff erlaubt.
7	Zugriff auf das Gerät verboten.	Nicht in der Liste der vertrauenswürdigen Geräte.	Zugriff verboten.	Keine Untersuchung.	Zugriff verboten.
8	Keine Regel für den Zugriff auf Geräte und keine Regel für den Zugriff auf Schnittstellen vorhanden.	Nicht in der Liste der vertrauenswürdigen Geräte.	Keine Zugriffsregel.	Keine Regel für den Zugriff auf Schnittstellen.	Zugriff erlaubt.

9	Keine Regel für den Zugriff auf Geräte vorhanden.	Nicht in der Liste der vertrauenswürdigen Geräte.	Keine Zugriffsregel.	Zugriff erlaubt.	Zugriff erlaubt.
10	Keine Regel für den Zugriff auf Geräte vorhanden.	Nicht in der Liste der vertrauenswürdigen Geräte.	Keine Zugriffsregel.	Zugriff verboten.	Zugriff verboten.

Sie können die Regeln für den Zugriff auf Geräte nach dem Anschluss des Geräts ändern. Wenn das Gerät angeschlossen wurde und die Zugriffsregel den Zugriff auf das Gerät erlaubt hat, Sie die Zugriffsregel anschließend jedoch geändert und den Zugriff auf das Gerät verboten haben, blockiert Kaspersky Endpoint Security den Zugriff beim nächsten Versuch, zum Zweck der Ausführung einer Dateioperation (Aufruf der Verzeichnisstruktur, Lesen, Schreiben) auf das Gerät zuzugreifen. Geräte ohne Dateisystem werden erst blockiert, wenn sie zum nächsten Mal mit dem Computer verbunden werden.

Wenn der Benutzer eines Computers, auf dem das Programm Kaspersky Endpoint Security installiert ist, den Zugriff auf ein Gerät angefordert hat, das seiner Meinung nach irrtümlicherweise blockiert wurde, so übermitteln Sie ihm eine Anleitung für die Zugriffsanforderung.

Zugriffsregel für ein Gerät ändern

Abhängig vom Gerätetyp können Sie unterschiedliche Zugriffseinstellungen ändern: Liste der Benutzer, für die das Gerät freigegeben ist, Zeitplan für den Zugriff und Erlaubnis/Verbot des Zugriffs.

Gehen Sie folgendermaßen vor, um eine Regel für den Zugriff auf ein Gerät zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.

3. Wählen Sie im rechten Fensterbereich die Registerkarte **Gerätetypen**.

   Auf der Registerkarte **Gerätetypen** befinden sich die Zugriffsregeln für alle Geräte, die in der Klassifikation der Komponente Gerätekontrolle vorhanden sind.

4. Wählen Sie eine Zugriffsregel, die geändert werden soll.

5. Klicken Sie auf **Ändern**. Diese Schaltfläche ist nur für die Gerätetypen verfügbar, die ein Dateisystem besitzen.

   Das Fenster **Regel für den Zugriff auf Geräte anpassen** wird geöffnet.

   Standardmäßig erlaubt eine Zugriffsregel für Geräte allen Benutzern jederzeit den vollständigen Zugriff auf einen Gerätetyp. Eine solche Regel enthält in der Liste **Benutzer und/oder Benutzergruppen** die Gruppe **Alle** und besitzt in der Tabelle **Rechte der gewählten Benutzergruppe nach Zugriffszeitplänen** den Zugriffszeitplan **Standardzeitplan** mit Rechten für alle Vorgänge, die mit Geräten möglich sind.

6. Ändern Sie die Einstellungen der Zugriffsregel für Geräte:

a. Wählen Sie in der Liste **Benutzer und/oder Benutzergruppen** einen Benutzer und / oder eine Benutzergruppe.

   Verwenden Sie die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**, um die Liste **Benutzer und/oder Benutzergruppen** zu ändern.

b. Passen Sie für den gewählten Benutzer und / oder die Benutzergruppe in der Tabelle **Rechte der gewählten Benutzergruppe nach Zugriffszeitplänen** einen Zugriffszeitplan für Geräte an. Aktivieren Sie dazu die Kontrollkästchen für die Zugriffszeitpläne, die in der zu ändernden Zugriffsregel für Geräte verwendet werden sollen.

   Verwenden Sie die Schaltflächen **Erstellen**, **Ändern**, **Kopieren** und **Löschen** in der Tabelle **Rechte der gewählten Benutzergruppe nach Zugriffszeitplänen**, um die Zeitplanliste für den Gerätezugriff zu ändern.

c. Legen Sie für die einzelnen Zugriffszeitpläne, die in der geänderten Regel verwendet werden, jene Vorgänge fest, die bei der Nutzung von Geräten erlaubt sind. Aktivieren Sie dazu in der Tabelle **Rechte der gewählten Benutzergruppe nach Zugriffszeitplänen** die Kontrollkästchen in den Spalten mit den Namen der erforderlichen Vorgänge.

d. Klicken Sie auf **OK**.

Nachdem Sie die ursprünglichen Einstellungswerte einer Zugriffsregel für Geräte geändert haben, erhält die Einstellung für den Zugriff auf den entsprechenden Gerätetyp in der Spalte **Zugriff** in der Tabelle auf der Registerkarte **Gerätetypen** den Wert *Durch Regeln einschränken*.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Ereignisprotokollierung aktivieren und deaktivieren

Die Ereignisprotokollierung ist nur für Vorgänge mit Dateien auf Wechseldatenträgern verfügbar.

Um die Ereignisprotokollierung zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.

3. Wählen Sie im rechten Fensterbereich die Registerkarte **Gerätetypen**.

   Auf der Registerkarte **Gerätetypen** befinden sich die Zugriffsregeln für alle Geräte, die in der Klassifikation der Komponente Gerätekontrolle vorhanden sind.

4. Wählen Sie in der Tabelle für Geräte den Punkt **Wechseldatenträger**.

   Im oberen Bereich der Tabelle wird die Schaltfläche **Ereignisprotokollierung** aktiv.

5. Klicken Sie auf **Ereignisprotokollierung**.

   Das Fenster **Einstellungen für die Ereignisprotokollierung** wird geöffnet.

6. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Ereignisprotokollierung für Vorgänge zum Schreiben und Löschen von Dateien auf Wechseldatenträgern einschalten möchten, aktivieren Sie das Kontrollkästchen **Ereignisprotokollierung aktivieren**.

     Kaspersky Endpoint Security protokolliert ein Ereignis und sendet eine Nachricht an den Administrationsserver für Kaspersky Security Center, wenn der Benutzer auf Wechseldatenträgern einen Vorgang zum Schreiben oder Löschen von Dateien ausführt.

   - Andernfalls deaktivieren Sie das Kontrollkästchen **Ereignisprotokollierung aktivieren**.

7. Legen Sie fest, welche Vorgänge protokolliert werden sollen. Führen Sie dazu eine der folgenden Aktionen aus:

   - Damit Kaspersky Endpoint Security alle Ereignisse protokolliert, aktivieren Sie das Kontrollkästchen **Informationen über alle Dateien speichern**.

   - Damit Kaspersky Endpoint Security nur Informationen über Dateien eines bestimmten Formats protokolliert, aktivieren Sie im Abschnitt **Filter nach Dateiformaten** die Kontrollkästchen für die entsprechenden Dateiformate.

8. Legen Sie fest, für welche Benutzer Kaspersky Endpoint Security die Aktionen protokollieren soll. Gehen Sie dazu folgendermaßen vor:

   a. Klicken Sie im Abschnitt **Benutzer** auf **Auswählen**.

      Das Windows-Standardfenster **Benutzer oder Gruppen wählen** wird geöffnet.

   b. Erstellen oder ändern Sie die Liste für Benutzer und/oder Benutzergruppen

   Wenn Benutzer, die im Abschnitt **Benutzer** angegeben sind, Dateien speichern, die sich auf Wechseldatenträgern befinden, oder Dateien von Wechseldatenträgern löschen, so speichert Kaspersky Endpoint Security im Ereignisprotokoll Informationen über den ausgeführten Vorgang und sendet eine Nachricht an den Administrationsserver für Kaspersky Security Center.

9. Klicken Sie im Fenster **Einstellungen für die Ereignisprotokollierung** auf **OK**.

10. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Ereignisse, die mit Dateien auf Wechseldatenträgern zusammenhängen, können Sie in der Verwaltungskonsole für Kaspersky Security Center im Arbeitsbereich für den Knoten **Administrationsserver** auf der Registerkarte **Ereignisse** einsehen. Damit Ereignisse im lokalen Ereignisprotokoll von Kaspersky Endpoint Security angezeigt werden, muss das Kontrollkästchen **Ein Dateivorgang wurde ausgeführt** in den Benachrichtigungseinstellungen für die Komponente Gerätekontrolle aktiviert werden.

WLAN-Netzwerk zur Liste der vertrauenswürdigen WLAN-Netzwerke hinzufügen

Sie können den Benutzern erlauben, sich mit WLAN-Netzwerken zu verbinden, die Sie für sicher halten, zum Beispiel mit dem WLAN-Netzwerk Ihres Unternehmens. Dazu muss dieses Netzwerk zur Liste der

vertrauenswürdigen WLAN-Netzwerke hinzugefügt werden. Die Gerätekontrolle blockiert den Zugriff auf alle WLAN-Netzwerke, außer jenen, welche auf der Liste der vertrauenswürdigen WLAN-Netzwerke stehen.

Um ein WLAN-Netzwerk zur Liste der vertrauenswürdigen WLAN-Netzwerke hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.

3. Wählen Sie im rechten Fensterbereich die Registerkarte **Gerätetypen**.

   Auf der Registerkarte **Gerätetypen** befinden sich die Zugriffsregeln für alle Geräte, die in der Klassifikation der Komponente Gerätekontrolle vorhanden sind.

4. Klicken Sie in der Spalte **Zugriff** gegenüber des Geräts **WLAN** mit der rechten Maustaste, um das Kontextmenü zu öffnen.

5. Wählen Sie den Punkt **Verbieten mit Ausnahmen**.

6. Wählen Sie in der Geräteliste den Punkt **WLAN** und klicken Sie auf **Ändern**.

   Das Fenster **Vertrauenswürdige WLAN-Netzwerke** wird geöffnet.

7. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Vertrauenswürdiges WLAN-Netzwerk** wird geöffnet.

8. Gehen Sie im Fenster **Vertrauenswürdiges WLAN-Netzwerk** wie folgt vor:

   - Geben Sie im Feld **Netzwerkname** den Namen des WLAN-Netzwerks an, das Sie zur Liste der vertrauenswürdigen WLAN-Netzwerke hinzufügen möchten.
   - Wählen Sie in der Dropdown-Liste **Authentifizierungstyp** den Authentifizierungstyp, der bei einer Verbindung mit dem vertrauenswürdigen WLAN-Netzwerk verwendet werden soll.
   - Wählen Sie in der Dropdown-Liste **Verschlüsselungstyp** den Verschlüsselungstyp, mit dem der Datenverkehr des vertrauenswürdigen WLAN-Netzwerks geschützt werden soll.
   - Im Feld **Kommentar** können Sie beliebige Informationen über das hinzuzufügende WLAN-Netzwerk angeben.

   Ein WLAN-Netzwerk wird als vertrauenswürdig betrachtet, wenn seine Einstellungen mit den in der Regel angegebenen Einstellungen übereinstimmen.

9. Klicken Sie im Fenster **Vertrauenswürdiges WLAN-Netzwerk** auf **OK**.

10. Klicken Sie im Fenster **Vertrauenswürdige WLAN-Netzwerke** auf **OK**.

Zugriffsregel für eine Verbindungsschnittstelle ändern

Gehen Sie folgendermaßen vor, um eine Zugriffsregel für eine Schnittstelle zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.
3. Wählen Sie die Registerkarte **Schnittstellen**.

   Auf der Registerkarte **Schnittstellen** befinden sich Zugriffsregeln für alle Schnittstellen, die in der Klassifikation der Komponente Gerätekontrolle vorhanden sind.
4. Wählen Sie die Zugriffsregel für die Schnittstelle, die geändert werden soll.
5. Ändern Sie die Zugriffseinstellungen:
   - Klicken Sie mit der rechten Maustaste auf die Spalte **Zugriff** und wählen Sie den Punkt **Erlauben**, um den Zugriff auf eine Schnittstelle zu erlauben.
   - Klicken Sie mit der rechten Maustaste auf die Spalte **Zugriff** und wählen Sie den Punkt **Verbieten**, um den Zugriff auf eine Schnittstelle zu verbieten.
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktionen für vertrauenswürdige Geräte

Dieser Abschnitt informiert über die Aktionen mit vertrauenswürdigen Geräten.

Gerät von der Programmoberfläche aus zur Liste der vertrauenswürdigen Geräte hinzufügen

Wird ein Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt, wird der Zugriff auf das Gerät standardmäßig für alle Benutzer erlaubt (Benutzergruppe Jeder).

Gehen Sie folgendermaßen vor, um ein Gerät von der Programmoberfläche aus zur Liste der vertrauenswürdigen Geräte hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.
3. Wählen Sie im rechten Fensterbereich die Registerkarte **Vertrauenswürdige Geräte**.
4. Klicken Sie auf **Auswählen**.

Das Fenster **Vertrauenswürdige Geräte wählen** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen für das Gerät, das zur Liste der vertrauenswürdigen Geräte hinzugefügt werden soll.

   Die Geräteliste in der Spalte **Geräte** ist davon abhängig, welcher Wert in der Dropdown-Liste **Angeschlossene Geräte anzeigen** gewählt wurde.

6. Klicken Sie auf **Auswählen**.

   Das Microsoft-Windows-Fenster **Benutzer oder Gruppen auswählen** wird geöffnet.

7. Legen Sie im Microsoft-Windows-Fenster **Benutzer oder Gruppen wählen** die Benutzer und/oder Benutzergruppen fest, für die Kaspersky Endpoint Security die gewählten Geräte als vertrauenswürdig betrachten soll.

   Die Namen der Benutzer und/oder der Benutzergruppen, die im Microsoft-Windows-Fenster **Benutzer oder Gruppen wählen** festgelegt sind, werden im Feld **Für Benutzer und/oder Benutzergruppen erlauben** angezeigt.

8. Klicken Sie im Fenster **Vertrauenswürdige Geräte wählen** auf **OK**.

   In der Tabelle auf der Registerkarte **Vertrauenswürdige Geräte** des Konfigurationsfensters für die Komponente **Gerätekontrolle** erscheint eine Zeile mit Einstellungen des hinzugefügten vertrauenswürdigen Geräts.

9. Wiederholen Sie die Schritte 4-7 für jedes Gerät, das für bestimmte Benutzer und / oder Benutzergruppen zur Liste der vertrauenswürdigen Geräte hinzugefügt werden soll.

10. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Geräte nach Modell oder ID zur Liste der vertrauenswürdigen Geräte hinzufügen

Wird ein Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt, wird der Zugriff auf das Gerät standardmäßig für alle Benutzer erlaubt (Benutzergruppe Jeder).

Um Geräte nach Modell oder ID zur Liste der vertrauenswürdigen Geräte hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen jener Administrationsgruppe, für welche Sie eine Liste mit vertrauenswürdigen Geräten erstellen möchten.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Wählen Sie die gewünschte Richtlinie aus.

5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:

   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.

- Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

6. Wählen Sie im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.
7. Wählen Sie im rechten Fensterbereich die Registerkarte **Vertrauenswürdige Geräte**.
8. Klicken Sie auf **Hinzufügen**.

   Das Kontextmenü der Schaltfläche wird geöffnet.
9. Führen Sie im Kontextmenü der Schaltfläche **Hinzufügen** eine der folgenden Aktionen aus:

   - Wählen Sie den Punkt **Geräte nach ID** aus, wenn Sie Geräte, deren individuelle IDs bekannt sind, zur Liste der vertrauenswürdigen Geräte hinzufügen möchten.
   - Wählen Sie den Punkt **Geräte nach Modell** aus, wenn Sie vertrauenswürdige Geräte zur Liste hinzufügen möchten, deren VID (Hersteller-ID) und PID (Produkt-ID) bekannt ist.
10. Wählen Sie im folgenden Fenster aus der Dropdown-Liste **Gerätetyp** einen Gerätetyp für die folgende Tabelle aus.
11. Klicken Sie auf **Aktualisieren**.

    Die Tabelle enthält eine Liste der Geräte, deren IDs und/oder Modelle bekannt sind und die zu dem Typ gehören, der in der Dropdown-Liste **Gerätetyp** angegeben ist.
12. Aktivieren Sie die Kontrollkästchen für jene Geräte, die zur Liste der vertrauenswürdigen Geräte hinzugefügt werden sollen.
13. Klicken Sie auf **Auswählen**.

    Das Microsoft-Windows-Fenster **Benutzer oder Gruppen auswählen** wird geöffnet.
14. Legen Sie im Windows-Fenster **Benutzer oder Gruppen wählen** die Benutzer und/oder Benutzergruppen fest, für die Kaspersky Endpoint Security die gewählten Geräte als vertrauenswürdig betrachten soll.

    Die Namen der Benutzer und/oder der Benutzergruppen, die im Microsoft-Windows-Fenster **Benutzer oder Gruppen wählen** festgelegt sind, werden im Feld **Für Benutzer und/oder Benutzergruppen erlauben** angezeigt.
15. Klicken Sie auf **OK**.

    Die Tabelle enthält auf der Registerkarte **Vertrauenswürdige Geräte** Zeilen mit den Einstellungen der hinzugefügten vertrauenswürdigen Geräte.
16. Klicken Sie auf **OK** oder **Übernehmen**, um die Änderungen zu speichern.

Geräte nach einer ID-Maske zur Liste der vertrauenswürdigen Geräte hinzufügen

Wird ein Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt, wird der Zugriff auf das Gerät standardmäßig für alle Benutzer erlaubt (Benutzergruppe Jeder).

Das Hinzufügen von Geräten zur Liste der vertrauenswürdigen Geräte anhand einer ID-Maske ist nur in der Verwaltungskonsole für Kaspersky Security Center möglich.

Gehen Sie wie folgt vor, um Geräte anhand einer ID-Maske zur Liste der vertrauenswürdigen Geräte hinzuzufügen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen jener Administrationsgruppe, für welche Sie eine Liste mit vertrauenswürdigen Geräten erstellen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.
7. Wählen Sie im rechten Fensterbereich die Registerkarte **Vertrauenswürdige Geräte**.
8. Klicken Sie auf **Hinzufügen**.

   Das Kontextmenü der Schaltfläche wird geöffnet.
9. Wählen Sie im Kontextmenü der Schaltfläche **Hinzufügen** den Punkt **Geräte nach ID-Maske** aus.

   Das Fenster **Vertrauenswürdige Geräte nach ID-Maske hinzufügen** wird geöffnet.
10. Tragen Sie im Fenster **Vertrauenswürdige Geräte nach ID-Maske hinzufügen** im Feld **Maske** eine Maske für die Geräte-IDs ein.
11. Klicken Sie auf **Auswählen**.

    Das Microsoft-Windows-Fenster **Benutzer oder Gruppen auswählen** wird geöffnet.
12. Legen Sie im Microsoft Windows-Fenster **Benutzer oder Gruppen wählen** die Benutzer und/oder Benutzergruppen fest, deren Geräte von Kaspersky Endpoint Security Geräte als vertrauenswürdig betrachtet werden sollen, wenn Geräte, Modelle oder IDs mit der festgelegten Maske übereinstimmen.

    Die Namen der Benutzer und/oder der Benutzergruppen, die im Microsoft-Windows-Fenster **Benutzer oder Gruppen wählen** festgelegt sind, werden im Feld **Für Benutzer und/oder Benutzergruppen erlauben** angezeigt.
13. Klicken Sie auf **OK**.

In der Tabelle auf der Registerkarte **Vertrauenswürdige Geräte** des Konfigurationsfensters für die Komponente **Gerätekontrolle** erscheint eine Zeile mit Einstellungen für die Regel. Mit dieser Regel werden Geräte nach einer ID-Maske zur Liste der vertrauenswürdigen Geräte hinzugefügt.

14. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Zugriff von Benutzern auf ein vertrauenswürdiges Gerät anpassen

Wird ein Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt, wird der Zugriff auf das Gerät standardmäßig für alle Benutzer erlaubt (Benutzergruppe Jeder). Sie können den Zugriff von Benutzern (und Benutzergruppen) auf ein vertrauenswürdiges Gerät anpassen.

Um den Zugriff von Benutzern auf ein vertrauenswürdiges Gerät anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.

3. Wählen Sie im rechten Fensterbereich die Registerkarte **Vertrauenswürdige Geräte**.

4. Wählen Sie in der Liste der vertrauenswürdigen Geräte ein Gerät, für das Sie die Zugriffsregeln ändern möchten.

5. Klicken Sie auf **Ändern**.

   Das Fenster **Zugriffsregel für vertrauenswürdige Geräte anpassen** wird geöffnet.

6. Klicken Sie auf **Auswählen**.

   Das Microsoft-Windows-Fenster **Benutzer oder Gruppen auswählen** wird geöffnet.

7. Legen Sie im Microsoft-Windows-Fenster **Benutzer oder Gruppen wählen** die Benutzer und/oder Benutzergruppen fest, für die Kaspersky Endpoint Security die gewählten Geräte als vertrauenswürdig betrachten soll.

8. Klicken Sie auf **OK**.

   Die Namen der Benutzer und/oder Benutzergruppen, die im Microsoft-Windows-Fenster **Benutzer oder Gruppen wählen** festgelegt sind, werden im Fenster **Zugriffsregel für vertrauenswürdige Geräte anpassen** im Feld **Für Benutzer und/oder Benutzergruppen erlauben** angezeigt.

9. Klicken Sie auf **OK**.

10. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Gerät aus der Liste der vertrauenswürdigen Geräte löschen

Gehen Sie folgendermaßen vor, um ein Gerät aus der Liste der vertrauenswürdigen Geräte zu löschen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.
3. Wählen Sie im rechten Fensterbereich die Registerkarte **Vertrauenswürdige Geräte**.
4. Wählen Sie das Gerät, das aus der Liste der vertrauenswürdigen Geräte gelöscht werden soll.
5. Klicken Sie auf **Löschen**.
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Über den Zugriff auf Geräte, die Sie aus der Liste der vertrauenswürdigen Geräte gelöscht haben, entscheidet Kaspersky Endpoint Security auf Basis der Zugriffsregeln für Geräte und der Zugriffsregeln für Schnittstellen.

Liste mit vertrauenswürdigen Geräten importieren

Um eine Liste mit vertrauenswürdigen Geräten zu importieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.
3. Wählen Sie im rechten Fensterbereich die Registerkarte **Vertrauenswürdige Geräte**.
4. Klicken Sie auf **Import**.

   Das Fenster **Konfigurationsdatei wählen** wird geöffnet.
5. Wählen Sie im Fenster **Konfigurationsdatei wählen** eine Datei im XML-Format aus, aus welcher Sie die Liste mit vertrauenswürdigen Geräten importieren möchten, und klicken Sie auf **Öffnen**.

   Wenn die Liste der vertrauenswürdigen Geräte bereits Elemente enthält, öffnet sich das Fenster **Die Liste enthält bereits Elemente**. Dort können Sie eine der folgenden Aktionen ausführen:

   - Um die zu importierenden Elemente zu den vorhandenen Elementen hinzuzufügen, klicken Sie auf **Ja**.
   - Um die vorhandenen Elementen zuerst zu löschen und anschließend die zu importierenden Elemente hinzuzufügen, klicken Sie auf **Nein**.
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Liste mit vertrauenswürdigen Geräten exportieren

Um die Liste mit vertrauenswürdigen Geräten zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.
3. Wählen Sie im rechten Fensterbereich die Registerkarte **Vertrauenswürdige Geräte**.
4. Wählen Sie in der Liste die Elemente aus, die Sie exportieren möchten.
5. Klicken Sie auf **Export**.

   Das Fenster **Konfigurationsdatei wählen** wird geöffnet.
6. Geben Sie im Fenster **Konfigurationsdatei wählen** eine Datei im XML-Format an, in welche Sie die Liste mit vertrauenswürdigen Geräten exportieren möchten, wählen Sie einen Ordner aus, in welchem diese Datei gespeichert werden soll, und klicken Sie auf **Speichern**.

Meldungsvorlagen für die Gerätekontrolle ändern

Versucht ein Benutzer, auf ein blockiertes Gerät zuzugreifen, so meldet Kaspersky Endpoint Security die Sperrung des Geräts oder das Verbot für einen Vorgang mit dem Geräteinhalt. Ist der Benutzer der Meinung, die Zugriffsverweigerung auf ein Gerät oder das Verbot eines Vorgangs mit dem Geräteinhalt sei irrtümlich erfolgt, so kann der Benutzer eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks senden. Dafür ist im Text der Sperrmeldung ein Link vorgesehen.

Für die Meldung über die Sperrung eines Geräts oder über das Verbot eines Vorgangs mit dem Geräteinhalt, sowie für die Nachricht an den Administrator sind Vorlagen vorgesehen. Die Meldungsvorlagen können geändert werden.

Um die Meldungsvorlagen für die Gerätekontrolle zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.
3. Klicken Sie im rechten Fensterbereich auf **Vorlagen**.

   Das Fenster **Vorlagen für Nachrichten** wird geöffnet.
4. Führen Sie eine der folgenden Aktionen aus:

   - Um die Vorlage für die Meldung über die Sperrung eines Geräts oder über das Verbot eines Vorgangs mit dem Geräteinhalt zu ändern, wählen Sie die Registerkarte **Sperrung**.
   - Um die Vorlage für die Nachricht an den Administrator des lokalen Unternehmensnetzwerks zu ändern, wählen Sie die Registerkarte **Nachricht an den Administrator**.

5. Ändern Sie die Meldungsvorlage. Dazu können Sie die Schaltflächen **Variable**, **Standard** und **Link** verwenden (Die Schaltfläche ist nur auf der Registerkarte **Sperrung** verfügbar).

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Anti-Bridging

Dieser Abschnitt informiert über die Funktion Anti-Bridging und erklärt die entsprechenden Einstellungen.

Über Anti-Bridging

Die Funktion Anti-Bridging gewährleistet den Schutz vor Netzwerkbrücken. Dadurch wird verhindert, dass gleichzeitig mehrere Netzwerkverbindungen für den Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, hergestellt werden.

Anti-Bridging aktivieren und deaktivieren

Die Funktion Anti-Bridging ist standardmäßig deaktiviert. Bei Bedarf können Sie diese Funktion aktivieren.

Um die Funktion Anti-Bridging zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.

3. Klicken Sie auf **Anti-Bridging**.

   Das Fenster **Anti-Bridging** wird geöffnet.

4. Führen Sie eine der folgenden Aktionen aus:

   - Um den Schutz vor Netzwerkbrücken einzuschalten, aktivieren Sie das Kontrollkästchen **Anti-Bridging aktivieren**.

     Nachdem die Funktion Anti-Bridging aktiviert wurde, blockiert Kaspersky Endpoint Security die bereits bestehenden Verbindungen gemäß der Verbindungsregeln.

   - Um den Schutz vor Netzwerkbrücken auszuschalten, deaktivieren Sie das Kontrollkästchen **Anti-Bridging aktivieren**.

5. Klicken Sie im Fenster **Anti-Bridging** auf **OK**.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Über die Verbindungsregeln

Für die folgenden vordefinierten Gerätetypen sind bereits Verbindungsregeln vorhanden:

- Netzwerkadapter
- WLAN-Adapter
- Modems

Wenn eine Verbindungsregel aktiviert ist, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

- Wird eine neue Verbindung hergestellt, so wird die aktive Verbindung blockiert, falls für beide Verbindungen der in der Regel angegebene Gerätetyp verwendet wird.
- Verbindungen werden blockiert, wenn Sie mithilfe von Gerätetypen, für die Regeln mit einer niedrigeren Priorität verwendet werden, hergestellt wurden oder hergestellt werden sollen.

Status einer Verbindungsregel ändern

Im den Status einer Verbindungsregel zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.
3. Klicken Sie auf **Anti-Bridging**.

   Das Fenster **Anti-Bridging** wird geöffnet.
4. Wählen Sie die Regel, deren Status Sie ändern möchten.
5. Öffnen Sie in der Spalte **Kontrolle** durch Linksklick das Kontextmenü und führen Sie eine der folgenden Aktionen aus:
   - Um die Verwendung einer Regel zu aktivieren, wählen Sie den Punkt **Ein**.
   - Um die Verwendung einer Regel zu deaktivieren, wählen Sie den Punkt **Aus**.
6. Klicken Sie im Fenster **Anti-Bridging** auf **OK**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Priorität einer Verbindungsregel ändern

Im die Priorität einer Verbindungsregel zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.

3. Klicken Sie auf **Anti-Bridging**.

   Das Fenster **Anti-Bridging** wird geöffnet.

4. Wählen Sie die Regel aus, deren Priorität Sie ändern möchten.

5. Führen Sie eine der folgenden Aktionen aus:

   - Um die Regel in der Regelliste um eine Position nach oben zu verschieben, klicken Sie auf **Aufwärts**.
   - Um die Regel in der Regelliste um eine Position nach unten zu verschieben, klicken Sie auf **Abwärts**.

Je höher die Regel in der Liste der Regeln steht, desto höher ist ihre Priorität. Die Funktion Anti-Bridging blockiert alle Verbindungen, unter Ausnahme der Verbindung, die mithilfe des Gerätetyps hergestellt wurde, für welchen die Regel mit der höchsten Priorität verwendet wird.

1. Klicken Sie im Fenster **Anti-Bridging** auf **OK**.

2. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Freigabe eines blockierten Geräts

Diese Anleitung richtet sich an Benutzer von Client-Computern, auf denen das Programm Kaspersky Endpoint Security installiert ist.

> Die Funktionalität, mit der ein Gerät vorübergehend freigegeben werden kann, ist in Kaspersky Endpoint Security nur dann verfügbar, wenn das Gerät einer Richtlinie für Kaspersky Security Center unterliegt und diese Funktionalität in den Richtlinieneinstellungen aktiviert ist (s. *Administratorhandbuch zu Kaspersky Security Center*).

Um Zugriff auf ein blockiertes Gerät zu erfragen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Gerätekontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Gerätekontrolle angezeigt.

3. Klicken Sie im rechten Fensterbereich auf **Zugriff erfragen**.

   Das Fenster **Zugriff auf ein Gerät erfragen** wird geöffnet.

4. Wählen Sie aus der Liste der angeschlossenen Geräte das Gerät, auf das Sie zugreifen möchten.

5. Klicken Sie auf **Zugriffsanfrage-Datei erstellen**.

   Das Fenster **Zugriffsanfrage-Datei erstellen** wird geöffnet.

6. Geben Sie im Feld **Dauer des Zugriffs auf das Gerät** den Zeitraum an, für den Sie Zugriff auf das Gerät erhalten möchten.

7. Klicken Sie auf **Speichern**.

   Das standardmäßige Microsoft-Windows-Fenster **Zugriffsanfrage-Datei speichern** wird geöffnet.

8. Wählen Sie im Microsoft-Windows-Fenster **Zugriffsanfrage-Datei speichern** den Ordner aus, in dem Sie die Zugriffsanfrage-Datei für den Gerätezugriff speichern möchten, und klicken Sie auf **Speichern**.

9. Senden Sie die Zugriffsanfrage-Datei für das Gerät an den Administrator des lokalen Unternehmensnetzwerks.

10. Fordern Sie beim Administrator des lokalen Unternehmensnetzwerks eine Datei mit einem Zugriffsschlüssel für das Gerät an.

11. Klicken Sie im Fenster **Zugriff auf ein Gerät erfragen** auf **Zugriffsschlüssel aktivieren**.

    Das Microsoft-Windows-Standardfenster **Zugriffsschlüssel laden** wird geöffnet.

12. Wählen Sie im Microsoft-Windows-Fenster **Zugriffsschlüssel laden** die Datei mit einem Zugriffsschlüssel für das Gerät, die Sie vom Administrator des lokalen Unternehmensnetzwerks erhalten haben, und klicken Sie auf **Öffnen**.

    Das Fenster **Zugriffsschlüssel für das Gerät aktivieren** mit Informationen über die Freigabe wird geöffnet.

13. Klicken Sie im Fenster **Zugriffsschlüssel für das Gerät aktivieren** auf **OK**.

Um mit dem Link in der Sperrmeldung Zugriff auf ein blockiertes Gerät zu erfragen, gehen Sie wie folgt vor:

1. Klicken Sie im Fenster der Sperrmeldung für ein Gerät oder für eine Schnittstelle auf den Link **Zugriff erfragen**.

   Das Fenster **Zugriffsanfrage-Datei erstellen** wird geöffnet.

2. Geben Sie im Feld **Dauer des Zugriffs auf das Gerät** den Zeitraum an, für den Sie Zugriff auf das Gerät erhalten möchten.

3. Klicken Sie auf **Speichern**.

   Das standardmäßige Microsoft-Windows-Fenster **Zugriffsanfrage-Datei speichern** wird geöffnet.

4. Wählen Sie im Microsoft-Windows-Fenster **Zugriffsanfrage-Datei speichern** den Ordner aus, in dem Sie die Zugriffsanfrage-Datei für den Gerätezugriff speichern möchten, und klicken Sie auf **Speichern**.

5. Senden Sie die Zugriffsanfrage-Datei für das Gerät an den Administrator des lokalen Unternehmensnetzwerks.

6. Fordern Sie beim Administrator des lokalen Unternehmensnetzwerks eine Datei mit einem Zugriffsschlüssel für das Gerät an.

7. Klicken Sie im Fenster **Zugriff auf ein Gerät erfragen** auf **Zugriffsschlüssel aktivieren**.

   Das Microsoft-Windows-Standardfenster **Zugriffsschlüssel laden** wird geöffnet.

8. Wählen Sie im Microsoft-Windows-Fenster **Zugriffsschlüssel laden** die Datei mit einem Zugriffsschlüssel für das Gerät, die Sie vom Administrator des lokalen Unternehmensnetzwerks erhalten haben, und klicken Sie auf **Öffnen**.

   Das Fenster **Zugriffsschlüssel für das Gerät aktivieren** mit Informationen über die Freigabe wird geöffnet.

9. Klicken Sie im Fenster **Zugriffsschlüssel für das Gerät aktivieren** auf **OK**.

Der Zeitraum, für den Zugriff auf ein Gerät gewährt wird, kann von dem Zeitraum abweichen, den Sie beantragt haben. Ein Gerät wird für jenen Zeitraum freigegeben, den der Administrator des lokalen Unternehmensnetzwerks im Zugriffsschlüssel für das Gerät festlegt.

Mithilfe von Kaspersky Security Center einen Zugriffsschlüssel für ein blockiertes Gerät erstellen

Um einem Benutzer temporären Zugriff auf ein blockiertes Gerät zu gewähren, wird ein Zugriffsschlüssel für dieses Gerät benötigt. Sie können mithilfe von Kaspersky Security Center einen Zugriffsschlüssel erstellen.

Um einen Zugriffsschlüssel für ein blockiertes Gerät zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.

4. Wählen Sie in der Liste der Client-Computer den Computer aus, dessen Benutzer temporären Zugriff auf ein gesperrtes Gerät erhalten soll.

5. Wählen Sie im Kontextmenü des Computers den Punkt **Freigabe im Offline-Modus** aus.

   Das Fenster **Freigabe im Offline-Modus** wird geöffnet.

6. Wählen Sie die Registerkarte **Gerätekontrolle**.

7. Klicken Sie auf der Registerkarte **Gerätekontrolle** auf **Durchsuchen**.

   Das standardmäßige Windows-Fenster **Zugriffsanfrage-Datei auswählen** wird geöffnet.

8. Wählen Sie im Windows-Fenster **Zugriffsanfrage-Datei auswählen** die Zugriffsanfrage-Datei aus, die Sie von einem Benutzer erhalten haben, und klicken Sie auf **Öffnen**.

   Auf der Registerkarte **Gerätekontrolle** werden Informationen über das gesperrte Gerät angezeigt, auf das der Zugriff erfragt wurde.

9. Geben Sie einen Wert für **Dauer des Zugriffs auf das Gerät** an.

   Diese Einstellung enthält den Zeitraum, für den Sie einem Benutzer den Zugriff auf ein gesperrtes Gerät gewähren. Standardmäßig ist der Wert ausgewählt, den der Benutzer beim Erstellen der

Zugriffsanfrage-Datei angegeben hat.

10. Geben Sie einen Wert für **Aktivierungsfrist** an.

    Diese Einstellung enthält den Zeitraum, während dem der Benutzer mithilfe des Zugriffsschlüssels den Zugriff auf das blockierte Gerät aktivieren kann.

11. Klicken Sie auf **Speichern**.

    Das Windows-Standardfenster **Zugriffsschlüssel speichern** wird geöffnet.

12. Geben Sie an, in welchem Ordner die Zugriffsschlüsseldatei für das blockierte Gerät gespeichert werden soll.

13. Klicken Sie auf **Speichern**.

Web-Kontrolle

> Diese Komponente ist verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Dateiserver installiert ist.

Dieser Abschnitt informiert über die Funktionen von Web-Kontrolle und erklärt die Einstellungen der Komponente.

Über die Web-Kontrolle

Die Komponente Web-Kontrolle dient dazu, die Aktionen der Benutzer eines lokalen Firmennetzwerks zu kontrollieren. Dazu wird der Zugriff auf Webressourcen eingeschränkt oder verboten.

> Der Begriff Webressource bezieht sich sowohl auf eine bestimmte Webseite oder mehrere Webseiten, als auch auf eine oder mehrere Websites, die ein gemeinsames Merkmal aufweisen.

Die Web-Kontrolle bietet folgende Features:

- Einsparung von Datenverkehr

  Das Volumen des Datenverkehrs wird durch Beschränkung oder Verbot des Downloads von Multimedia-Dateien und durch Beschränkung oder Verbot für den Zugriff auf Webressourcen, die nicht mit beruflichen Aufgaben zusammenhängen, kontrolliert.

- Abgrenzung des Zugangs nach Inhaltskategorien der Webressourcen

  Um den Datenverkehr und potenzielle Verluste durch zweckentfremdete Nutzung der Arbeitszeit zu reduzieren, können Sie den Zugriff auf bestimmte Webressourcen-Kategorien beschränken oder verbieten (beispielsweise den Zugriff auf Webressourcen der Kategorie "Kommunikation im Internet").

- Zentralisierte Verwaltung desZugriffs auf Webressourcen

Bei Verwendung von Kaspersky Security Center stehen individuelle und gruppenbezogene Einstellungen für den Zugriff auf Webressourcen zur Verfügung.

Alle Einschränkungen und Verbote für den Zugriff auf Webressourcen werden als Zugriffsregeln für Webressourcen realisiert.

Web-Kontrolle aktivieren und deaktivieren

Die Web-Kontrolle ist standardmäßig aktiviert. Bei Bedarf können Sie die Web-Kontrolle deaktivieren.

Um die Web-Kontrolle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Web-Kontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Web-Kontrolle angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Web-Kontrolle aktivieren**, um die Web-Kontrolle einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Web-Kontrolle aktivieren**, um die Web-Kontrolle auszuschalten.

   Ist die Web-Kontrolle deaktiviert, kontrolliert Kaspersky Endpoint Security den Zugriff auf Webressourcen nicht.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Inhaltskategorien für Webressourcen

In der folgenden Liste wurden die Inhaltskategorien für Webressourcen (im Folgenden auch "Kategorien" genannt) so gewählt, dass sie die in Webressourcen enthaltenden Informationsblöcke möglichst vollständig beschreiben. Dabei wurden funktionelle und thematische Besonderheiten berücksichtigt. Die Reihenfolge, nach der die Kategorien in der Liste angeordnet sind, sagt nichts über die Wichtigkeit oder Verbreitung der Kategorien im Internet aus. Die Bezeichnungen der Kategorien sind nicht allgemeingültig und werden nur für die Programme und Websites von Kaspersky Lab verwendet. Die Bezeichnungen können sich in ihrer Bedeutung durchaus von den Definitionen der geltenden Gesetzgebung unterscheiden. Webressourcen können gleichzeitig mehreren Kategorien angehören.

Für Erwachsene

Diese Kategorie beinhaltet die folgenden Arten von Webressourcen:

- Webressourcen, die beliebiges Foto- oder Videomaterial mit Darstellungen von Geschlechtsorganen, Geschlechtsverkehr oder Selbstbefriedigung von Menschen oder humanoiden Wesen beinhalten.
- Webressourcen, die beliebige Texte, literarisches und künstlerisches Material eingeschlossen, mit Beschreibungen von Geschlechtsorganen, Geschlechtsverkehr oder Selbstbefriedigung von Menschen oder humanoiden Wesen beinhalten.

- Webressourcen, die der Diskussion über den sexuellen Aspekt menschlicher Beziehungen gewidmet sind.
- Webressourcen mit erotischen Inhalten und Werken, die eine realitätsnahe Betrachtung des menschlichen Sexuallebens beinhalten, oder Kunstwerke, die darauf ausgerichtet sind, sexuelle Erregung hervorzurufen.
- Webressourcen offizieller Medien und Internet-Gemeinschaften mit einem festen Zielpublikum, die spezielle Bereiche und/oder gesonderte Artikel beinhalten, die den sexuellen Aspekten zwischenmenschlicher Beziehungen gewidmet sind.
- Webressourcen, die sexuellen Perversionen gewidmet sind.
- Webressourcen, die der Bewerbung oder dem Verkauf von Gegenständen, die für sexuelle Handlungen oder die sexuelle Stimulation bestimmt sind, von sexuellen Dienstleistungen und intimen Treffen, u. a. virtueller Art im Rahmen von erotischen Videochats, Telefonsex und Schriftverkehr sexuellen Inhalts gewidmet sind ("virtueller Sex").
- Webressourcen mit folgendem Inhalt:
  - Artikel und die Blogs zum Thema der wissenschaftlichen und populären Sexualerziehung
  - Medizinische Enzyklopädien, insbesondere Abschnitte über sexuelle Fortpflanzung
  - Ressourcen von medizinischen Institutionen, insbesondere Abschnitte über die Behandlung von Geschlechtsorganen

Software, Audio, Video

Die Kategorie umfasst folgende Unterkategorien, die einzeln gewählt werden können:

- Audio und Video

  Diese Unterkategorie umfasst Webressourcen, die Audio- und Videomaterialen verbreiten: z. B. Filme, Aufzeichnungen von Sportübertragungen, Konzertmitschnitte, Lieder, Clips, Videoclips und audiovisuelle Lehrmaterialen.

- Torrents

  Diese Unterkategorie umfasst Websites für Torrent-Tracker, die dem Austausch von Dateien beliebiger Größe dienen.

- Filehosting-Anbieter

  Diese Unterkategorie umfasst Filesharing-Websites, unabhängig davon, wo sich die verbreiteten Dateien tatsächlich befinden.

Alkohol, Tabak, Drogen und psychotrope Substanzen

Diese Kategorie beinhaltet Webressourcen, deren Inhalt direkt oder indirekt mit alkoholischen und alkoholhaltigen Produkten, Tabakwaren, Drogen sowie psychotropen Stoffen und / oder Betäubungsmitteln in Zusammenhang steht:

- Webressourcen, die der Bewerbung und dem Verkauf der vorgenannten Stoffe sowie von Gegenständen zu deren Konsum gewidmet sind.

- Webressourcen mit Anleitungen zum Konsum oder zur Herstellung von Drogen sowie psychotropen Stoffen und/oder Betäubungsmitteln.

Zu dieser Kategorie gehören Webressourcen zu wissenschaftlichen und medizinischen Themen.

Gewalt

Zu dieser Kategorie gehören Webressourcen mit beliebigen Foto-, Video- und Textinhalten, die psychische oder physische Gewalt gegen Menschen sowie Tierquälerei darstellen bzw. beschreiben:

- Webressourcen, die Darstellungen / Beschreibungen von Hinrichtungen, Folter und Misshandlung sowie von hierfür bestimmtem Instrumentarium enthalten.

  Überschneidung mit der Kategorie "Waffen, Sprengstoffe, Pyrotechnik".

- Webressourcen mit Darstellungen / Beschreibungen von Mordszenen, Schlägereien, Vergewaltigungen und anderen Gewalttaten, Mobbing und Quälereien an bzw. von Menschen, Tieren oder Fantasiewesen.

- Webressourcen mit Informationen, die zu Taten animieren, die eine Gefahr für Leib und Leben darstellen, Aufrufe zu Selbstverletzung und Selbstmord eingeschlossen.

- Webressourcen, die Informationen enthalten, welche Gewalt und / oder Grausamkeiten rechtfertigen oder gutheißen oder zu Gewalt gegenüber Menschen oder Tieren aufrufen.

- Webressourcen, die besonders realistische Darstellungen/Beschreibungen der Opfer und Schrecken von Kriegen, bewaffneten Konflikten und Kampfhandlungen, Unglücken, Unfällen, Naturkatastrophen, Havarien, Unruhen und menschlichem Leid enthalten.

- Browserspiele mit Gewaltszenen und Grausamkeiten, darunter u. a. so genannte Ego-Shooter sowie Fighter- und Slasher-Spiele.

  Überschneidung mit der Kategorie "Computerspiele".

Waffen, Sprengstoffe, Pyrotechnik

Diese Kategorie beinhaltet Webressourcen mit Informationen über Waffen, Sprengstoffe und pyrotechnische Produkte:

- Webseiten von Herstellern und Verkäufern von Waffen, Sprengstoffen und pyrotechnischen Produkten.

- Webressourcen, die der Herstellung und Verwendung von Waffen, Sprengstoffen und pyrotechnischen Produkten gewidmet sind.

- Webressourcen mit analytischen, historischen, herstellungstechnischen und enzyklopädischen Inhalten zu den Themenbereichen Waffen, Sprengstoffe und pyrotechnische Produkte.

Unter "Waffen" sind Vorrichtungen, Gegenstände und Mittel zu verstehen, die von ihrer Konstruktion her dazu vorgesehen sind, Leib und Leben von Menschen und Tieren Schaden zuzufügen und / oder technische Anlagen und sonstige Objekte außer Betrieb zu setzen.

Obszönität

Diese Kategorie beinhaltet Webressourcen, auf denen Elemente anstößiger Lexik festgestellt wurden.

Überschneidung mit der Kategorie "Für Erwachsene".

Zu dieser Kategorie gehören auch Webressourcen mit linguistischen und philologischen Materialien, die anstößige Lexik zum Thema haben.

Kommunikation im Internet

Diese Kategorie beinhaltet Webressourcen, die es registrierten oder nicht registrierten Benutzern ermöglichen, persönliche Nachrichten an andere Nutzer dieser Webressourcen oder anderer Internet-Dienste zu versenden und / oder unter bestimmten Bedingungen an der Ergänzung der allgemein oder teilweise zugänglichen Inhalte der entsprechenden Webressourcen mitzuwirken. Folgende Unterkategorien können separat gewählt werden:

- Chats und Foren

  Diese Unterkategorie umfasst Webressourcen, welche für die öffentliche Diskussion unterschiedlicher Themen mithilfe spezieller Webanwendungen dienen, sowie Webressourcen, welche für die Verbreitung und Unterstützung von Instant-Messaging-Anwendungen dienen, mit denen Konversationen in Echtzeit möglich sind.

- Blogs

  Diese Unterkategorie umfasst Blog-Plattformen. Dies sind Websites, die kostenpflichtige oder kostenlose Dienste anbieten, mit denen Blogs erstellt und verwaltet werden können.

- Soziale Netzwerke

  Diese Unterkategorie umfasst Websites, mit denen Kontakte zwischen Menschen, Organisationen und Staaten hergestellt, angezeigt und organisiert werden können. Teilnahmevoraussetzung ist die Registrierung mit einem Benutzerkonto.

- Partnerbörsen

  Diese Unterkategorie umfasst Webressourcen, die eine Variante der sozialen Netzwerke sind. Sie bieten kostenpflichtige oder kostenlose Dienste an.

  Überschneidet sich mit den Kategorien "Inhalte für Erwachsene".

- Web-Mail

Diese Unterkategorie umfasst ausschließlich Login-Seiten für E-Mail-Dienste und Seiten für E-Mail-Postfächer, die E-Mail-Nachrichten und entsprechende Daten (z. B. persönliche Kontakte) enthalten. Andere Webseiten von Internet-Providern, die einen Maildienst anbieten, gehören nicht zu dieser Kategorie.

Glücksspiel, Lotterien, Wetten

Diese Kategorie beinhaltet Webressourcen, die ihren Besuchern die kostenpflichtige Teilnahme an Spielen anbieten, selbst wenn diese keine obligatorische Bedingung für die Nutzung der Webressourcen darstellt. Diese Kategorie umfasst Webressourcen folgenden Inhalts:

- Glücksspiele mit Geldeinsatz.

  > Überschneidung mit der Kategorie "Computerspiele".

- Geldwetten.
- Lotterien, die den Kauf von Lotterielosen / Losnummern vorsehen.
- Informationen, die dazu geeignet sind, den Wunsch zur Teilnahme an Glücksspielen, Wetten und Lotterien zu wecken.

> Zu dieser Kategorie gehören Spiele, die gesondert eine kostenlose Teilnahme anbieten, sowie Webressourcen, die bei ihren Nutzern aktiv für den Besuch von Webressourcen der oben genannten Kategorie werben.

Online-Shops, Banken, Zahlungssysteme

Diese Kategorie beinhaltet Webressourcen, die für die Vornahme beliebiger bargeldloser Online-Transaktionen mithilfe spezieller Web-Anwendungen vorgesehen sind. Folgende Unterkategorien können separat gewählt werden:

- Online-Shops

  Diese Unterkategorie umfasst Online-Shops und Online-Auktionen, die für den Verkauf beliebiger Waren, Arbeiten oder Dienstleistungen an natürliche und/oder juristische Personen bestimmt sind. Dazu zählen sowohl Websites reiner Online-Shops als auch Online-Filialen gewöhnlicher Geschäfte, in denen online bezahlt werden kann.

- Banken

  Diese Unterkategorie umfasst spezielle Webseiten von Banken, die Dienstleistungen für das Online-Banking anbieten. Dazu zählen u. a. bargeldlose (elektronische) Überweisungen zwischen Bankkonten, Eröffnung von Anlagekonten, Umtausch von Geldmitteln und Bezahlung der Leistungen von Drittunternehmen.

- Zahlungssysteme

  Diese Unterkategorie umfasst Webseiten elektronischer Zahlungssysteme, die dem Zugang zu einem persönlichen Benutzerkonto dienen.

In technischer Hinsicht können sowohl Bankkarten aller Art (Plastikkarten und virtuelle Karten, EC-Karten und Kreditkarten, regionale und internationale Karten) als auch elektronisches Geld als Zahlungsmittel dienen. Zur Ermittlung der Kategorie von Webressourcen ist es unerheblich, ob gewisse technische Aspekte, wie die Datenübertragung per SSL-Protokoll, die Nutzung von Sicherheitsstandards wie "3D Secure" usw. gegeben sind.

Karriere-Netzwerk

Diese Kategorie beinhaltet Webressourcen, die für die Kontaktaufnahme zwischen Arbeitgebern und Arbeitnehmern vorgesehen sind:

- Webseiten von Personalagenturen (Arbeitsvermittlungen und / oder Zeitarbeitsfirmen).
- Webseiten von Arbeitgebern mit Beschreibungen von freien Stellen und deren Vorteilen.
- Unabhängige Portale mit Stellenangeboten von Arbeitgebern und Personalagenturen.
- Soziale Netzwerke mit professioneller Orientierung, die unter anderem die Veröffentlichung und Suche von Daten über Fachleute ermöglichen, die aktiv nach Arbeit suchen.

Anonymisierungs-Tools

Diese Kategorie beinhaltet Webressourcen, die als Bindeglied für das Herunterladen von Inhalten anderer Webressourcen mithilfe spezieller Web-Anwendungen dienen, wobei folgende Ziele verfolgt werden:

- Umgehung von Zugangsbeschränkungen des lokalen Netzwerkadministrators für URL- oder IP-Adressen.
- Anonymer Zugriff auf Webressourcen, so auch auf Webressourcen, die HTTP-Anfragen von bestimmten IP-Adressen oder IP-Adressgruppen (beispielsweise aus bestimmten Ländern) nicht akzeptieren.

Zu dieser Kategorie gehören sowohl Webressourcen, die ausschließlich für die vorgenannten Zwecke bestimmt sind ("Anonymizer"), als auch Webressourcen, mit in technischer Hinsicht ähnlichen Funktionen.

Computerspiele

Diese Kategorie beinhaltet Webressourcen, die Computerspielen unterschiedlicher Art gewidmet sind:

- Webseiten von Computerspiel-Entwicklern.
- Webressourcen, die Diskussionen über Computerspiele gewidmet sind.
- Webressourcen, welche die technischen Möglichkeiten zur Teilnahme an Online-Spielen bieten, bei denen man alleine oder gegen andere Spieler antreten kann, unabhängig davon, ob eine lokale Installation von Anwendungen erforderlich ist oder nicht ("Browserspiele").

- Webressourcen zur Bewerbung und Verbreitung sowie zum Support von Computerspielen.

Religion, religiöse Vereinigungen

Diese Kategorie beinhaltet Webressourcen mit Material zu gesellschaftlichen Strömungen (Bewegungen), Vereinigungen (Gemeinschaften) und Organisationen, die auf religiösen Ideologien und / oder kultischen Handlungen beliebiger Ausprägung basieren:

- Webseiten offizieller religiöser Organisationen unterschiedlicher Ebenen, von internationalen Konfessionen bis hin zu lokal begrenzten Religionsgemeinschaften.
- Webseiten nicht registrierter religiöser Vereinigungen und Gemeinschaften, die geschichtlich durch die Abspaltung der vorherrschenden religiösen Vereinigungen oder Gemeinschaften entstanden sind.
- Websites religiöser Vereinigungen und Gemeinschaften, die unabhängig von den traditionellen religiösen Strömungen/Bewegungen entstanden sind, unter anderem auf Initiative eines konkreten Gründers.
- Webseiten konfessionsübergreifender Organisationen im Dienste der Zusammenarbeit von Vertretern unterschiedlicher traditioneller Religionen.
- Webressourcen, die wissenschaftliche, historische und enzyklopädische Inhalte zum Thema Religion anbieten.
- Webressourcen, die detaillierte Darstellungen / Beschreibungen religiöser Kulthandlungen, wie Zeremonien und Rituale, enthalten, die mit der Verehrung eines Gottes oder von Wesen bzw. Gegenständen im Zusammenhang stehen, denen übersinnliche Kräfte zugeschrieben werden.

Nachrichtenportale

Diese Kategorie beinhaltet Webressourcen mit öffentlichen Nachrichteninhalten, die durch Medien oder Internet-Verlage zusammengestellt werden und das Hinzufügen von Nachrichten durch die Benutzer vorsehen:

- Webseiten offizieller Medien.
- Webseiten, die Informationsdienste unter Berufung auf offizielle Informationsquellen zur Verfügung stellen.
- Webseiten, die Nachrichtenüberblicke bieten, also eine Auswahl von Nachrichten aus verschiedenen offiziellen und/oder inoffiziellen Quellen.
- Webseiten, deren Nachrichteninhalte durch die Benutzer selbst zusammengestellt werden ("Social News Webseiten").

Banner

Diese Kategorie umfasst Webressourcen, die Banner enthalten. Auf Bannern platzierte Werbung kann die Benutzer von ihrer Arbeit ablenken. Außerdem erhöhen Banner den Datenverkehr.

Regionale gesetzliche Beschränkungen

Diese Kategorie umfasst die Unterkategorie **Blockiert gemäß der Gesetzgebung der Russischen Föderation**. Zu dieser Kategorie gehören Webressourcen, die gemäß den Vorschriften der Gesetzgebung der Russischen Föderation blockiert werden.

Über die Zugriffsregeln für Webressourcen

Es wird davon abgeraten, mehr als 1.000 Zugriffsregeln für Webressourcen zu erstellen, da es andernfalls zu Systeminstabilität kommen kann.

Eine Zugriffsregel für Webressourcen besteht aus einer Auswahl von Filtern und aus einer Aktion, die Kaspersky Endpoint Security ausführt, wenn ein Benutzer die in der Regel beschriebenen Webressourcen zur im Regelzeitplan festgelegten Zeit besucht. Mithilfe von Filtern kann der Bereich der Webressourcen genau festgelegt werden, auf die der Zugriff durch die Komponente Web-Kontrolle kontrolliert wird.

Folgende Filter sind verfügbar:

- **Inhaltsfilter**. Die Web-Kontrolle unterteilt die Webressourcen nach Inhaltskategorien und Datentypkategorien. Sie können den Zugriff der Benutzer auf jene Daten kontrollieren, die sich in Webressourcen befinden, welche zu den durch diese Kategorien definierten Datentypen gehören. Wenn ein Benutzer Webressourcen besucht, die zu einer gewählten Inhaltskategorie und / oder Datentypkategorie gehören, führt Kaspersky Endpoint Security die in der Regel festgelegte Aktion aus.

- **Filter für Adressen von Webressourcen**. Sie können den Zugriff der Benutzer auf alle Adressen von Webressourcen oder auf bestimmte Adressen von Webressourcen und / oder Adressgruppen von Webressourcen kontrollieren.

  Wenn gleichzeitig ein Inhaltsfilter und ein Filter für Adressen von Webressourcen angegeben wurden und die festgelegten Adressen von Webressourcen und / oder Adressgruppen von Webressourcen einer gewählten Inhaltskategorien oder Datentypkategorien angehören, kontrolliert Kaspersky Endpoint Security nicht den Zugriff auf alle Webressourcen der gewählten Inhaltskategorie und / oder Datentypkategorie, sondern nur auf die festgelegten Adressen von Webressourcen und / oder Adressgruppen von Webressourcen.

- **Filter für Namen von Benutzern und Benutzergruppen**. Sie können Benutzer und / oder Benutzergruppen festlegen, für die der Zugriff auf Webressourcen nach der Regel kontrolliert werden soll.

- **Zeitplan für die Regel**. Sie können einen Zeitplan für die Regel erstellen. Der Zeitplan für eine Regel bestimmt die Zeit, in der Kaspersky Endpoint Security den Zugriff auf die in einer Regel festgelegten Webressourcen kontrolliert.

Nach der Installation von Kaspersky Endpoint Security ist die Regelliste der Komponente Web-Kontrolle nicht leer. Es sind zwei Regeln vordefiniert:

- Regel "Skripte und Stylesheets", die allen Benutzern jederzeit den Zugriff auf alle Webressourcen erlaubt, in deren Adressen Dateinamen mit der Endung css, js oder vbs vorkommen. Beispiele: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- "Standardregel", die allen Benutzern jederzeit den Zugriff auf alle Webressourcen erlaubt.

Aktionen für die Zugriffsregeln für Webressourcen

Für die Zugriffsregeln für Webressourcen stehen Ihnen die folgenden Aktionen zur Verfügung:

- Hinzufügen einer neuen Regel
- Ändern einer Regel
- Zuweisen einer Priorität für die Regel

  Die Priorität einer Regel wird durch die Position bestimmt, an welcher die Zeile mit der Kurzbeschreibung der Regel in der Tabelle für Zugriffsregeln im Konfigurationsfenster der Komponente Web-Kontrolle steht. Das bedeutet, dass eine Regel, die in der Tabelle weiter oben steht als andere Regeln, eine höhere Priorität besitzt.

  Fällt eine Webressource, auf die ein Benutzer zuzugreifen versucht, unter mehrere Regeln, ermittelt Kaspersky Endpoint Security die Regel mit der höchsten Priorität.
- Testen der Regel

  Mit der Funktion "Regeldiagnose" können Sie testen, ob die Regeln korrekt funktionieren.
- Aktivieren und Deaktivieren der Regel

  Eine Zugriffsregel für Webressourcen kann aktiviert (Status *Ein*) oder deaktiviert werden (Status *Aus*). Eine neu erstellte Regel ist standardmäßig aktiviert (sie besitzt den Status *Ein).* Sie können die Regel deaktivieren.
- Regel löschen

Zugriffsregel für Webressourcen hinzufügen und ändern

Gehen Sie folgendermaßen vor, um eine Regel für den Zugriff auf Webressourcen hinzuzufügen oder zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Web-Kontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Web-Kontrolle angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, wenn Sie eine Regel hinzufügen möchten.
   - Um eine Regel zu ändern, wählen Sie in der Tabelle eine Regel und klicken Sie auf **Ändern**.

   Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.
4. Geben Sie die Einstellungen für die Regel an oder ändern Sie sie. Gehen Sie dazu folgendermaßen vor:
   a. Tragen Sie im Feld **Name** einen Namen für die Regel ein oder ändern Sie den Namen.
   b. Wählen Sie in der Dropdown-Liste **Inhalt filtern** das entsprechende Element aus:
      - **Beliebiger Inhalt**.

- Nach Inhaltskategorien.
- Nach Datentypen.
- Nach Inhaltskategorien und Datentypen

c. Wenn Sie ein anderes Element als **Beliebiger Inhalt** ausgewählt ist, werden Abschnitte für die Auswahl von Inhaltskategorien und/oder Datentypen geöffnet. Aktivieren Sie die Kontrollkästchen für die entsprechenden Inhaltskategorien und/oder Datentypen.

Ist das Kontrollkästchen für eine Inhaltskategorie und/oder einen Datentyp aktiviert, so verwendet Kaspersky Endpoint Security die Regel, um den Zugriff auf die Webressourcen zu kontrollieren, die den gewählten Inhaltskategorien und/oder Dateitypen angehören.

d. Wählen Sie in der Dropdown-Liste **Auf Adressen anwenden** das entsprechende Element aus:

- Auf alle Adressen.
- Auf bestimmte Adressen.

e. Bei Auswahl des Elements **Auf bestimmte Adressen** öffnet sich ein Abschnitt, in dem eine Adressliste für Webressourcen erstellt werden muss. Sie können die Adresse und/oder die Adressgruppe einer Webressource hinzufügen oder ändern. Dazu dienen die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**.

f. Aktivieren Sie das Kontrollkästchen **Benutzer und/oder Gruppen angeben**.

g. Klicken Sie auf **Auswählen**.

Das Microsoft-Windows-Fenster **Benutzer oder Gruppen auswählen** wird geöffnet.

h. Erstellen oder ändern Sie die Liste der Benutzer und / oder der Benutzergruppen, für die der Zugriff auf die in der Regel beschriebenen Webressourcen erlaubt oder verboten werden soll.

i. Wählen Sie in der Dropdown-Liste **Aktion** das entsprechende Element aus:

- **Erlauben**. Wenn dieser Wert gewählt wird, erlaubt Kaspersky Endpoint Security den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
- **Verbieten**. Wenn dieser Wert gewählt wird, verbietet Kaspersky Endpoint Security den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
- **Warnen**. Ist dieser Wert gewählt, so warnt Kaspersky Endpoint Security bei einem Zugriffsversuch auf Webressourcen, welche dieser Regel entsprechen, vor dem Besuch der Webressource. Die Warnmeldung enthält Links, über die der Benutzer auf die angeforderte Webressource zugreifen kann.

j. Wählen Sie entweder aus der Dropdown-Liste **Zeitplan für die Regel** den Namen des entsprechenden Zeitplans oder erstellen Sie auf Basis des gewählten Regelzeitplans einen neuen Zeitplan. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche **Einstellungen** neben der Dropdown-Liste **Zeitplan für die Regel**.

   Das Fenster **Zeitplan für die Regel** wird geöffnet.

2. Um dem Regelzeitplan einen Zeitraum hinzuzufügen, in dem die Regel nicht gelten soll, wählen Sie in der Zeitplantabelle mit der linken Maustaste die Tabellenzellen für den entsprechenden Zeitraum und Wochentag.

   Die Farbe der Zellen ändert sich in Grau.

3. Um im Regelzeitplan einen Zeitraum, für welchen die Regel gilt, in einen Zeitraum zu ändern, für welchen die Regel nicht gilt, wählen Sie mit der linken Maustaste die grauen Tabellenzellen für den entsprechenden Zeitraum und Wochentag.

   Die Farbe der Zellen ändert sich in Grün.

4. Klicken Sie auf **Speichern unter**.

   Das Fenster **Name des Regelzeitplans** wird geöffnet.

5. Geben Sie einen Namen für den Regelzeitplan an oder behalten Sie den Standardnamen bei.

6. Klicken Sie auf **OK**.

5. Klicken Sie im Fenster **Regel für den Zugriff auf Webressourcen** auf **OK**.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Zugriffsregeln für Webressourcen eine Priorität zuweisen

Sie können jeder Regel aus der Liste eine bestimmte Priorität zuweisen, indem Sie die Regeln entsprechend anordnen.

Gehen Sie folgendermaßen vor, um Regeln für den Zugriff auf Webressourcen eine Priorität zuzuweisen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Web-Kontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Web-Kontrolle angezeigt.

3. Wählen Sie im rechten Fensterbereich eine Regel, deren Priorität geändert werden soll.

4. Verschieben Sie die Regel mit den Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Position in der Regelliste.

5. Wiederholen Sie die Punkte 3-4 für jene Regeln, deren Priorität geändert werden soll.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Zugriffsregeln für Webressourcen testen

Sie können die Regeln der Web-Kontrolle bewerten, um festzustellen, inwieweit sie aufeinander abgestimmt sind. Dazu dient in der Komponente Web-Kontrolle die Funktion "Regeldiagnose".

Gehen Sie folgendermaßen vor, um die Regeln für den Zugriff auf Webressourcen zu testen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Web-Kontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Web-Kontrolle angezeigt.

3. Klicken Sie im rechten Fensterbereich auf **Diagnose**.

   Das Fenster **Regeldiagnose** wird geöffnet.

4. Füllen Sie die Felder im Abschnitt **Bedingungen** aus:

   a. Aktivieren Sie das Kontrollkästchen **Geben Sie eine Adresse an**, um Regeln zu prüfen, nach denen Kaspersky Endpoint Security den Zugriff auf eine bestimmte Webressource kontrolliert. Tragen Sie im Feld die Adresse einer Webressource ein.

   b. Erstellen Sie eine Liste der Benutzer und/oder Benutzergruppen, um die Regeln zu überprüfen, nach denen Kaspersky Endpoint Security den Zugriff auf Webressourcen für bestimmte Benutzer und/oder Benutzergruppen kontrolliert.

   c. Wählen Sie in der Dropdown-Liste **Inhalt filtern** das entsprechende Element (**Nach Inhaltskategorien**, **Nach Datentypen** oder **Nach Inhaltskategorien und Datentypen**), um Regeln zu prüfen, nach denen Kaspersky Endpoint Security den Zugriff auf Webressourcen für bestimmte Inhaltskategorien und/oder Kategorien für Datentypen kontrolliert.

   d. Aktivieren Sie das Kontrollkästchen **Zeitpunkt des Zugriffsversuchs berücksichtigen**, wenn bei der Regelprüfung der Zeitpunkt (Wochentag und Uhrzeit) berücksichtigt werden soll, zu dem ein Zugriffsversuch auf die Webressourcen erfolgt, die in den Bedingungen für die Regeldiagnose festgelegt wurden. Geben Sie nun einen Wochentag und eine Uhrzeit an.

5. Klicken Sie auf die Schaltfläche **Prüfen**.

Nach der Überprüfung wird eine Meldung über die Aktion angezeigt, die Kaspersky Endpoint Security bei einem Zugriffsversuch auf die angegebene Webressource in Übereinstimmung mit der zuerst ausgelösten Regel ausführen würde (Erlaubnis, Verbot, Warnung). Die zuerst ausgelöste Regel ist jene Regel, die in der Regelliste der Web-Kontrolle unter jenen Regeln, welche die Diagnosebedingungen erfüllen, an erster Stelle steht. Die Meldung wird rechts von der Schaltfläche **Prüfen** angezeigt. Die darunter angezeigte Tabelle enthält eine Liste der übrigen ausgelösten Regeln mit Angabe der Aktion, die Kaspersky Endpoint Security ausführt. Die Regeln sind in absteigender Reihenfolge nach der Priorität angeordnet.

Zugriffsregel für Webressourcen aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um eine Zugriffsregel für Webressourcen zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Web-Kontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Web-Kontrolle angezeigt.

3. Wählen Sie im rechten Fensterbereich eine Regel, die sie aktivieren oder deaktivieren möchten.

4. Führen Sie in der Spalte **Status** folgende Schritte aus:

   - Wählen Sie den Wert *Ein*, um die Verwendung einer Regel zu aktivieren.

   - Wählen Sie den Wert *Aus*, um die Verwendung einer Regel zu deaktivieren.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Migration von Zugriffsregeln für Webressourcen aus Vorgängerversionen des Programms

Beim Programm-Upgrade von der Version Kaspersky Endpoint Security 10 Service Pack 2 für Windows und von älteren Versionen auf Kaspersky Endpoint Security 11 für Windows werden die Zugriffsregeln für Webressourcen, die auf Inhaltskategorien für Webressourcen basieren, nach folgenden Regeln migriert:

- Regeln für den Zugriff auf Webressourcen, die auf einer oder mehreren Inhaltskategorien für Webressourcen aus der Liste "Chats und Foren", "Web-Mail", "Soziale Netzwerke" basieren, werden der Inhaltskategorie für Webressourcen "Kommunikation im Internet" zugeordnet.

- Regeln für den Zugriff auf Webressourcen, die auf einer oder mehreren Inhaltskategorien für Webressourcen aus der Liste "Online-Shops" und "Zahlungssysteme" basieren, werden der Inhaltskategorie für Webressourcen "Online-Shops, Banken, Zahlungssysteme" zugeordnet.

- Regeln für den Zugriff auf Webressourcen, die auf der Inhaltskategorie "Glücksspiel" basieren, werden der Inhaltskategorie für Webressourcen "Glücksspiel, Lotterien, Wetten" zugeordnet.

- Regeln für den Zugriff auf Webressourcen, die auf der Inhaltskategorie "Browserspiele" basieren, werden der Inhaltskategorie für Webressourcen "Computerspiele" zugeordnet.

- Regeln für den Zugriff auf Webressourcen, die auf Inhaltskategorien basieren, die nicht in den vorstehenden Punkten der Liste enthalten sind, werden unverändert übernommen.

Adressliste für Webressourcen exportieren und importieren

Wenn Sie in einer Zugriffsregel bereits eine Adressliste für Webressourcen angelegt haben, kann die Liste in eine txt-Datei exportiert werden. Die Liste kann später aus dieser Datei importiert werden, um beim Anpassen von Regeln keine neue Adressliste für Webressourcen manuell erstellen zu müssen. Die Möglichkeit zum Export und Import einer Adressliste für Webressourcen ist beispielsweise vorteilhaft, wenn Sie Regeln mit ähnlichen Einstellungen erstellen möchten.

Gehen Sie folgendermaßen vor, um eine Adressliste für Webressourcen zu exportieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Web-Kontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Web-Kontrolle angezeigt.

3. Wählen Sie die Regel, deren Adressliste für Webressourcen in eine Datei exportiert werden soll.

4. Klicken Sie auf **Ändern**.

   Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.

5. Wenn Sie nicht die gesamte Adressliste für Webressourcen, sondern nur einen Teil davon exportieren möchten, dann markieren Sie die betreffenden Adressen für Webressourcen.

6. Klicken Sie auf die Schaltfläche  , die sich rechts von der Adressliste für Webressourcen befindet.

   Ein Fenster zur Bestätigung der Aktion wird geöffnet.

7. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Bestätigungsfenster auf **Ja**, wenn Sie nur die markierten Elemente aus der Adressliste für Webressourcen exportieren möchten.

   - Klicken Sie im Bestätigungsfenster auf **Nein**, wenn Sie alle Elemente aus der Adressliste für Webressourcen exportieren möchten.

     Das Standardfenster **Speichern unter** von Microsoft Windows wird geöffnet.

8. Wählen Sie im Microsoft-Windows-Fenster **Speichern unter** die Datei, in welche die Adressliste für Webressourcen exportiert werden soll, und klicken Sie auf **Speichern**.

Gehen Sie folgendermaßen vor, um eine Adressliste für Webressourcen aus einer Datei in die Regel zu importieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Web-Kontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Web-Kontrolle angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf **Hinzufügen**, um eine neue Zugriffsregel für Webressourcen zu erstellen.

   - Wählen Sie die Zugriffsregel für Webressourcen, die geändert werden soll. Klicken Sie auf **Ändern**.

   Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.

4. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine neue Zugriffsregel für Webressourcen erstellen, wählen Sie in der Dropdown-Liste **Auf Adressen anwenden** das Element **Auf bestimmte Adressen**.

   - Wenn Sie eine Zugriffsregel für Webressourcen ändern, gehen Sie weiter zu Punkt 5 der Anleitung.

5. Klicken Sie auf die Schaltfläche  , die sich rechts von der Adressliste für Webressourcen befindet.

   Wenn Sie eine neue Regel erstellen, wird das Standardfenster **Datei öffnen** von Microsoft Windows geöffnet.

Wenn Sie eine Regel ändern, öffnet sich ein Bestätigungsfenster.

6. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine neue Zugriffsregel für Webressourcen erstellen, gehen Sie weiter zu Punkt 7 der Anleitung.
   - Wenn Sie eine Zugriffsregel für Webressourcen ändern, führen Sie im Bestätigungsfenster eine der folgenden Aktionen aus:
     - Klicken Sie auf **Ja**, um die importierten Elemente zu einer bereits vorhandenen Adressliste für Webressourcen hinzuzufügen.
     - Klicken Sie auf **Nein**, um die vorhandenen Elemente der Adressliste für Webressourcen zu löschen und die importierten Elemente hinzuzufügen.

   Das Standardfenster **Datei öffnen** von Microsoft Windows wird geöffnet.

7. Wählen Sie im Microsoft-Windows-Fenster **Datei öffnen** eine Datei, aus der die Adressliste für Webressourcen importiert werden soll.

8. Klicken Sie auf **Öffnen**.

9. Klicken Sie im Fenster **Regel für den Zugriff auf Webressourcen** auf **OK**.

Regeln für das Erstellen von Adressmasken für Webressourcen

Die Verwendung einer *Adressmaske für eine Webressource* (im Folgenden "Adressmaske") bietet sich an, wenn eine Zugriffsregel für Webressourcen erstellt wird, für die eine hohe Anzahl ähnlicher Adressen für Webressourcen angegeben werden soll. Eine korrekt formulierte Adressmaske kann eine Vielzahl von Webressourcen ersetzen.

Für das Erstellen einer Adressmaske sind folgende Regeln zu beachten:

1. Das Zeichen `*` ersetzt eine beliebige Abfolge aus null oder mehr Zeichen.

   Beispielsweise wird bei Angabe der Adressmaske *abc* die Zugriffsregel für Webressourcen auf alle Adressen angewendet, welche die Zeichenfolge abc enthalten. Beispiel: http://www.example.com/page_0-#9abcdefl.

   Um das Symbol `*` in eine Maske aufzunehmen, muss das Symbol `*` in der Maske doppelt angegeben werden.

2. Die Zeichenfolge `www.` zu Beginn der Adressmaske wird wie `*.` behandelt.

   Beispiel: Die Adressmaske www.example.com wird wie *.example.com behandelt.

3. Beginnt eine Adressmaske nicht mit dem Zeichen `*`, entspricht der Inhalt dieser Adressmaske dem gleichen Inhalt mit dem Präfix `*.`.

4. Die Zeichenfolge `*.` am Anfang einer Maske wird wie `*.` oder als leere Zeile behandelt.

   Beispiel: Die Adressmaske http://www.*.example.com schließt die Adresse http://www2.example.com ein.

5. Endet eine Adressmaske mit einem anderen Zeichen als `/` oder `*`, so entspricht der Inhalt dieser Adressmaske dem gleichen Inhalt mit dem Postfix `/*`.

   Beispiel: Die Adressmaske http://www.example.com schließt Adressen der Form http://www.example.com/abc ein, wobei a, b, c für beliebige Zeichen stehen.

6. Endet eine Adressmaske mit dem Zeichen `/`, entspricht der Inhalt dieser Adressmaske dem gleichen Inhalt mit dem Postfix `/*`.

7. Die Zeichenfolge `/*` am Ende einer Adressmaske wird wie `/*` oder als leere Zeile behandelt.

8. Eine Untersuchung von Adressen für Webressourcen nach einer Adressmaske erfolgt unter Berücksichtigung des Schemas (http oder https):

   - Enthält eine Adressmaske kein Netzwerkprotokoll, erstreckt sich die Adressmaske auf eine Adresse mit beliebigem Netzwerkprotokoll.

     Beispiel: Die Adressmaske example.com schließt die Adressen http://example.com und https://example.com ein.

   - Enthält eine Adressmaske ein Netzwerkprotokoll, erstreckt sich die Adressmaske nur auf Adressen mit dem in der Adressmaske genannten Netzwerkprotokoll.

     Beispiel: Die Adressmaske http://*.example.com schließt die Adresse http://www.example.com ein, während die Adresse https://www.example.com nicht darunter fällt.

9. Eine Adressmaske, die in doppelten Anführungszeichen steht, wird ungeachtet zusätzlicher Substitutionen behandelt. Eine Ausnahme bildet das Zeichen `*`, falls es in der Adressmaske enthalten ist. Für Adressmasken, die in doppelten Anführungszeichen stehen, werden die Regeln 5 und 7 nicht ausgeführt (s. Beispiele 14 – 18 in folgender Tabelle).

10. Beim Vergleich mit der Adressmaske für eine Webressource bleiben Benutzername und Kennwort, Verbindungsport sowie Groß- und Kleinschreibung unberücksichtigt.

Praktische Beispiele für die Regeln zum Erstellen von Adressmasken

Nr.	Adressmaske	Zu untersuchende Adresse für eine Webressource	Die zu untersuchende Adresse entspricht der Adressmaske	Komr
1	*.example.com	http://www.123example.com	Nein	Siehe Reg
2	*.example.com	http://www.123.example.com	Ja	Siehe Reg
3	*example.com	http://www.123example.com	Ja	Siehe Reg
4	*example.com	http://www.123.example.com	Ja	Siehe Reg
5	http://www.*.example.com	http://www.123example.com	Nein	Siehe Reg
6	www.example.com	http://www.example.com	Ja	Siehe Reg 1.
7	www.example.com	https://www.example.com	Ja	Siehe Reg

				1.
8	http://www.*.example.com	http://123.example.com	Ja	Siehe Reg und 1.
9	www.example.com	http://www.example.com/abc	Ja	Siehe Reg und 1.
10	example.com	http://www.example.com	Ja	Siehe Reg 1.
11	http://example.com/	http://example.com/abc	Ja	Siehe Reg
12	http://example.com/*	http://example.com	Ja	Siehe Reg
13	http://example.com	https://example.com	Nein	Siehe Reg
14	"example.com"	http://www.example.com	Nein	Siehe Reg
15	"http://www.example.com"	http://www.example.com/abc	Nein	Siehe Reg
16	"*.example.com"	http://www.example.com	Ja	Siehe Reg 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Ja	Siehe Reg 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Ja	Siehe Reg 8.
19	www.example.com/abc/123	http://www.example.com/abc	Nein	Eine Adressma mehr Info als die Adı Webresso

Meldungsvorlagen für die Web-Kontrolle ändern

Abhängig davon, welche Aktion in den Eigenschaften der Regeln für die Web-Kontrolle festgelegt ist, zeigt Kaspersky Endpoint Security beim Versuch eines Benutzers, Zugriff auf Webressourcen zu erhalten, eine Meldung an (die Antwort des HTTP-Servers wird durch eine HTML-Seite mit einer Meldung ersetzt). Folgende Meldungstypen sind möglich:

- Warnmeldung. Eine solche Meldung warnt den Benutzer, dass vom Besuch einer Webressource abgeraten wird und/oder der Besuch gegen die Sicherheitsrichtlinie des Unternehmens verstößt. Kaspersky Endpoint Security zeigt eine Warnmeldung an, wenn in den Einstellungen der Regel, welche diese Webressource beschreibt, in der Dropdown-Liste **Aktion** das Element **Warnen** gewählt ist.

  Hält der Benutzer die Warnung für einen Irrtum, so kann der Benutzer mit einem Link aus der Warnung eine vorgefertigte Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken.

- Meldung über die Sperrung einer Webressource. Kaspersky Endpoint Security zeigt eine Meldung über die Sperrung einer Webressource an, wenn in den Einstellungen der Regel, welche

diese Webressource beschreibt, in der Dropdown-Liste **Aktion** das Element **Verbieten** gewählt ist.

Hält der Benutzer die Zugriffssperre auf eine Webressource für einen Irrtum, so kann der Benutzer mit einem Link aus der Sperrmeldung eine vorgefertigte Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken.

Für die Warnmeldung, für die Meldung über die Sperrung einer Webressource und für die Nachricht an den Administrator des lokalen Unternehmensnetzwerks sind Vorlagen vorgesehen. Der Inhalt dieser Vorlagen kann geändert werden.

Gehen Sie folgendermaßen vor, um die Meldungsvorlage für die Web-Kontrolle zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Sicherheitskontrolle** den Unterabschnitt **Web-Kontrolle**.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente Web-Kontrolle angezeigt.
3. Klicken Sie im rechten Fensterbereich auf **Vorlagen**.

   Das Fenster **Vorlagen für Nachrichten** wird geöffnet.
4. Führen Sie eine der folgenden Aktionen aus:
   - Um die Vorlage für die Meldung zu ändern, die den Benutzer darüber informiert, dass vom Besuch einer Webressource abgeraten wird, wählen Sie die Registerkarte **Warnung**.
   - Um die Vorlage für die Meldung über die Zugriffsverweigerung für eine Webressource zu ändern, wählen Sie die Registerkarte **Sperrung**.
   - Um die Vorlage für die Nachricht an den Administrator zu ändern, wählen Sie die Registerkarte **Nachricht an den Administrator**.
5. Ändern Sie die Meldungsvorlage. Dazu können Sie die Dropdown-Liste **Variable** sowie die Schaltflächen **Standard** und **Link** verwenden (Die Schaltfläche ist auf der Registerkarte **Nachricht an den Administrator** nicht verfügbar).
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Datenverschlüsselung

Ist das Programm Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Workstation installiert, so ist die Funktionalität zur Datenverschlüsselung in vollem Umfang verfügbar. Ist das Programm Kaspersky Endpoint Security auf einem Computer mit einem Betriebssystem von Microsoft Windows für Dateiserver installiert, so ist nur die vollständige Festplattenverschlüsselung mithilfe der Technologie BitLocker-Laufwerkverschlüsselung verfügbar.

Dieser Abschnitt informiert über die Verschlüsselung und Entschlüsselung von Dateien auf lokalen Computerlaufwerken, Festplatten und Wechseldatenträgern. Außerdem wird hier erklärt, wie die

Verschlüsselung und Entschlüsselung von Daten mithilfe von Kaspersky Endpoint Security und des Verwaltungs-Plug-ins für Kaspersky Endpoint Security angepasst und ausgeführt wird.

Wenn der Zugriff auf verschlüsselte Daten nicht möglich ist, folgen Sie den entsprechenden Anleitungen für die Arbeit mit verschlüsselten Daten (Mit verschlüsselten Dateien arbeiten, wenn die Dateiverschlüsselungsfunktion eingeschränkt ist, Mit verschlüsselten Geräten arbeiten, wenn kein Zugriff besteht).

Über die Datenverschlüsselung

Kaspersky Endpoint Security erlaubt die Verschlüsselung von Dateien und Ordnern, die auf lokalen Laufwerken und Wechseldatenträgern gespeichert sind, sowie die Verschlüsselung kompletter Wechseldatenträger und Festplatten. Die Datenverschlüsselung reduziert das Risiko eines Informationsdiebstahls, falls ein Laptop, ein Wechseldatenträger oder eine Festplatte gestohlen wird oder verloren geht, oder falls Dritte oder andere Programme auf Daten zugreifen.

Wenn die Lizenz abgelaufen ist, verschlüsselt das Programm neue Daten nicht mehr. Bereits verschlüsselte Daten bleiben verschlüsselt und es kann weiterhin damit gearbeitet werden. Um neue Daten zu verschlüsseln, muss das Programm mit einer neuen Lizenz aktiviert werden, welche die Verwendung der Verschlüsselung vorsieht.

> Wenn die Lizenz abgelaufen ist, der Lizenzvertrag verletzt wurde, der Schlüssel entfernt wurde, oder das Programm Kaspersky Endpoint Security oder die Verschlüsselungskomponenten vom Computer des Benutzers entfernt wurde, kann nicht garantiert werden, dass zuvor verschlüsselte Dateien auch weiterhin verschlüsselt bleiben. Das hängt damit zusammen, dass manche Programme, wie z. B. Microsoft Office Word, bei der Bearbeitung einer Datei eine temporäre Kopie anlegen, mit der sie die Originaldatei beim Speichern ersetzen. Ist die Verschlüsselungsfunktionalität auf dem Computer nicht vorhanden oder nicht verfügbar, so bleibt die Datei unverschlüsselt.

Kaspersky Endpoint Security bietet folgende Datenschutzmaßnahmen:

- **Dateiverschlüsselung auf lokalen Festplatten des Computers**. Sie können folgende Listen anlegen: Listen mit Dateien nach Erweiterung oder Erweiterungsgruppen, und Listen mit Ordnern, die sich auf lokalen Laufwerken des Computers befinden. Außerdem können Sie Verschlüsselungsregeln für Dateien definieren, die von bestimmten Programmen erstellt werden. Nachdem die Richtlinie für Kaspersky Security Center übernommen wurde, verschlüsselt und entschlüsselt Kaspersky Endpoint Security folgende Dateien:
  - Dateien, die einzeln zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
  - Dateien, die in Ordnern gespeichert sind, welche zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
  - Dateien, die von bestimmten Programmen erstellt werden

  Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.
- **Wechseldatenträger verschlüsseln**. Sie können eine Standard-Verschlüsselungsregel festlegen, nach der das Programm für alle Wechseldatenträger die gleiche Aktion ausführt. Außerdem können Sie Verschlüsselungsregeln für bestimmte Wechseldatenträger erstellen.

Die Standard-Verschlüsselungsregel besitzt eine niedrigere Priorität als die Verschlüsselungsregeln, die für bestimmte Wechseldatenträger erstellt wurden. Verschlüsselungsregeln, die für bestimmte Wechseldatenträger unter Angabe eines Gerätemodells erstellt wurden, besitzen eine niedrigere Priorität als Verschlüsselungsregeln, die für Wechseldatenträger unter Angabe einer Geräte-ID erstellt wurden.

Um zu wählen, welche Regel für die Dateiverschlüsselung auf einem Wechseldatenträger gilt, überprüft Kaspersky Endpoint Security, ob Gerätemodell und Geräte-ID bekannt sind. Anschließend führt das Programm eine der folgenden Aktionen aus:

- Ist nur das Gerätemodell bekannt, so wendet das Programm jene Verschlüsselungsregel an, die für Wechseldatenträger mit diesem Gerätemodell erstellt wurde, falls eine solche Regel vorhanden ist.
- Ist nur die Geräte-ID bekannt, so wendet das Programm jene Verschlüsselungsregel an, die für Wechseldatenträger mit dieser Geräte-ID erstellt wurde, falls eine solche Regel vorhanden ist.
- Sind Gerätemodell und Geräte-ID bekannt, so wendet das Programm jene Verschlüsselungsregel an, die für Wechseldatenträger mit dieser Geräte-ID erstellt wurde, falls eine solche Regel vorhanden ist. Ist eine solche Regel nicht vorhanden, es gibt aber eine Verschlüsselungsregel, die für Wechseldatenträger mit diesem Gerätemodell erstellt wurde, so verwendet das Programm diese Regel. Wurde weder für diese Geräte-ID noch für dieses Gerätemodell eine Verschlüsselungsregel festgelegt, so verwendet das Programm die standardmäßige Verschlüsselungsregel.
- Wenn weder das Gerätemodell noch die Geräte-ID bekannt ist, wendet das Programm die Standard-Verschlüsselungsregel an.

Ein Wechseldatenträger kann vom Programm so vorbereitet werden, dass die darauf verschlüsselten Dateien im portablen Modus verwendet werden können. Ist der portable Modus aktiviert, so können verschlüsselte Dateien auf Wechseldatenträgern auch dann verwendet werden, wenn der Wechseldatenträger mit einem Computer verbunden ist, auf dem die Verschlüsselungsfunktion nicht verfügbar ist.

Das Programm führt bei der Übernahme der Richtlinie für Kaspersky Security Center die in der Verschlüsselungsregel angegebene Aktion durch.

- **Verwaltung von Regeln für den Zugriff von Programmen auf verschlüsselte Dateien**. Sie können für ein beliebiges Programm eine Regel für den Zugriff auf verschlüsselte Dateien erstellen. Diese Regel kann entweder den Zugriff auf verschlüsselte Dateien verbieten oder nur den Zugriff auf den verschlüsselten Text erlauben, also auf eine Zeichenfolge, die aus der Verschlüsselung hervorgeht.
- **Verschlüsselte Archive erstellen**. Sie können verschlüsselte Archive erstellen und den Zugriff darauf mit einem Kennwort schützen. Der Zugriff auf den Inhalt verschlüsselter Archive wird erst nach Eingabe der Kennwörter gewährt, mit denen Sie den Zugriff auf diese Archive geschützt haben. Solche Archive können gefahrlos über das Internet oder auf Wechseldatenträgern übertragen werden.
- **Vollständige Festplattenverschlüsselung**. Sie können ein Verschlüsselungsverfahren wählen: Kaspersky-Festplattenverschlüsselung oder BitLocker-Laufwerkverschlüsselung (im Folgenden auch "BitLocker" genannt).

  Die BitLocker-Technologie ist Bestandteil des Betriebssystems Windows. Wenn ein Computer mit Trusted Platform Module (TPM) ausgerüstet ist, verwendet BitLocker das TPM zur Speicherung von Wiederherstellungsschlüsseln, die zur Freigabe verschlüsselter Festplatten dienen. Beim Hochfahren des Computers fragt BitLocker bei Trusted Platform Module die Wiederherstellungsschlüssel für die

Festplatte ab und entsperrt die Festplatte. Sie können die Verwendung eines Kennworts und/oder eines PIN-Codes für den Zugriff auf die Wiederherstellungsschlüssel festlegen.

Sie können eine standardmäßige Regel für die vollständige Festplattenverschlüsselung festlegen und eine Liste mit Festplatten erstellen, die von der Verschlüsselung ausgeschlossen werden sollen. Nachdem die Richtlinie für Kaspersky Security Center übernommen wurde, führt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung sektorbasiert aus. Das Programm verschlüsselt alle logischen Partitionen der Festplatten auf einmal. Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Nach der Verschlüsselung von Systemfestplatten und einem nachfolgenden Neustart des Computers, sind der Zugriff auf die Festplatten und das Laden des Betriebssystems erst möglich, nachdem der Benutzer sich mithilfe des Authentifizierungsagenten authentifiziert hat. Dazu ist entweder die Eingabe des Kennworts für den Token oder die Smartcard, die an den Computer angeschlossen sind, oder die Eingabe der Anmeldedaten des Benutzerkontos für den Authentifizierungsagenten erforderlich. Dieses Benutzerkonto wird vom Systemadministrator des lokalen Unternehmensnetzwerks mithilfe der Verwaltungsaufgaben für die Benutzerkonten des Authentifizierungsagenten erstellt. Diese Konten basieren auf den Benutzerkonten von Microsoft Windows, mit denen sich die Benutzer im Betriebssystem anmelden. Sie können die Benutzerkonten des Authentifizierungsagenten verwalten und das Verfahren zur einmaligen Anmeldung (SSO, Single Sign-On) nutzen, das eine automatische Anmeldung im Betriebssystem mit dem Benutzernamen und dem Kennwort des Benutzerkontos für den Authentifizierungsagenten ermöglicht.

> Wenn für den Computer eine Sicherungskopie erstellt wurde, die Computerdaten dann verschlüsselt wurden, anschließend die Sicherungskopie des Computers wiederhergestellt wurde und die Computerdaten erneut verschlüsselt wurden, so erstellt Kaspersky Endpoint Security Duplikate der Benutzerkonten für den Authentifizierungsagenten. Um die Duplikate zu löschen, muss das Dienstprogramm klmover mit dem Parameter `dupfix` verwendet werden. Das Tool gehört zum Lieferumfang von Kaspersky Security Center. Weitere Informationen dazu finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

> Beim Upgrade des Programms auf Kaspersky Endpoint Security 11 für Windows wird die Liste der Benutzerkonten für den Authentifizierungsagenten nicht gespeichert.

Der Zugriff auf verschlüsselte Festplatten ist nur von jenen Computern möglich, auf denen das Programm Kaspersky Endpoint Security installiert und die vollständige Festplattenverschlüsselung verfügbar ist. Diese Bedingung gewährleistet ein minimales Risiko von Datendiebstahl von der verschlüsselten Festplatte, falls diese außerhalb des lokalen Unternehmensnetzwerks verwendet wird.

Um Festplatten und Wechseldatenträger zu verschlüsseln, können Sie die Funktion **Nur belegten Speicherplatz verschlüsseln** verwenden. Es wird empfohlen, diese Funktion nur für neue Geräte zu verwenden, die bisher noch nicht benutzt worden sind. Wenn Sie die Verschlüsselung auf einem Gerät verwenden möchten, das bereits benutzt wurde, so sollte das gesamte Gerät verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, aus denen noch Informationen entnommen werden können.

Vor dem Beginn der Verschlüsselung erhält Kaspersky Endpoint Security eine Sektorenkarte des Dateisystems. Im ersten Datenstrom werden die Sektoren verschlüsselt, die beim Start der Verschlüsselung mit Dateien belegt sind. Im zweiten Datenstrom werden die Sektoren verschlüsselt, die nach dem Beginn der Verschlüsselung geschrieben wurden. Nach dem Abschluss der Verschlüsselung sind alle Sektoren verschlüsselt, die Daten enthalten.

Löscht der Benutzer nach dem Abschluss der Verschlüsselung eine Datei, so werden die Sektoren, in denen diese Datei gespeichert waren, frei und dort können auf Dateisystemebene Informationen geschrieben werden. Dabei bleiben die Sektoren weiterhin verschlüsselt. Wird die Verschlüsselung regelmäßig ausgeführt und die Funktion **Nur belegten Speicherplatz verschlüsseln** ist aktiviert, so werden durch die kontinuierliche Speicherung von Dateien nach und nach alle Sektoren auf dem neuen Gerät verschlüsselt.

Die Daten, die zur Entschlüsselung von Objekten erforderlich sind, werden vom Administrationsserver für Kaspersky Security Center zur Verfügung gestellt, der den Computer zum Zeitpunkt der Verschlüsselung verwaltet. Falls ein Computer mit verschlüsselten Objekten inzwischen von einem anderen Administrationsserver verwaltet wird und noch nie auf die verschlüsselten Objekte zugegriffen wurde, so kann die Freigabe wie folgt erreicht werden:

- Administrator des lokalen Unternehmensnetzwerks um die Freigabe der verschlüsselten Objekte bitten
- Daten auf verschlüsselten Geräten mithilfe des Reparatur-Tools wiederherstellen
- Aus einer Sicherungskopie die Konfiguration des Administrationsservers für Kaspersky Security Center wiederherstellen, von welchem der Computer bei der Verschlüsselung verwaltet wurde, und diese Konfiguration auf dem Administrationsserver verwenden, welcher den Computer mit den verschlüsselten Objekten verwaltet

Im Verlauf der Verschlüsselung legt das Programm Verwaltungsdateien an. Für deren Speicherung sind etwa 0,5% unfragmentierter freier Speicherplatz auf der Festplatte des Computers erforderlich. Ist auf der Festplatte zu wenig unfragmentierter Speicherplatz verfügbar, so wird die Verschlüsselung erst gestartet, wenn entsprechende Bedingungen vorliegen.

Die Kompatibilität zwischen der Verschlüsselungsfunktion von Kaspersky Endpoint Security und Kaspersky Anti-Virus für UEFI wird nicht unterstützt. Die Verschlüsselung von Computerlaufwerken, auf denen Kaspersky Anti-Virus für UEFI installiert ist, führt zur Funktionsunfähigkeit von Kaspersky Anti-Virus für UEFI.

Beschränkungen der Verschlüsselungsfunktionalität

Die Funktionalität zur vollständigen Festplattenverschlüsselung mit dem Verfahren Kaspersky-Festplattenverschlüsselung ist nicht verfügbar für Festplatten, welche die Hard- und Softwarevoraussetzungen nicht erfüllen.

Folgende Konfigurationen werden von Endpoint Security nicht unterstützt:

- Schema, bei dem sich Ladeprogramm und Betriebssystem auf unterschiedlichen Laufwerken befinden
- integrierte Software des Standards UEFI 32
- System mit der Technologie Intel Rapid Start Technology und Laufwerke mit einer Hibernation-Partition, auch wenn die Nutzung von Intel Rapid Start Technology deaktiviert ist
- Laufwerke im MBR-Format, die über mehr als vier erweiterte Partitionen (extended partitions) verfügen
- System, in dem eine Auslagerungsdatei vorhanden ist, die sich nicht auf dem Systemlaufwerk befindet

- Multi-Boot-System mit mehreren gleichzeitig installierten Betriebssystemen
- dynamische Partitionen (nur primäre Partitionen werden unterstützt)
- Laufwerke, auf denen weniger als 0,5% freier unfragmentierter Speicherplatz vorhanden ist
- Laufwerke mit einer anderen Sektorgröße als 512 Byte oder 4096 Byte mit 512-Byte-Emulation
- Hybridlaufwerke

Verschlüsselungsalgorithmus ändern

Der Verschlüsselungsalgorithmus, den Kaspersky Endpoint Security für die Datenverschlüsselung verwendet, ist von der Verschlüsselungsbibliothek abhängig, die zum Programmpaket gehört.

Gehen Sie folgendermaßen vor, um den Verschlüsselungsalgorithmus zu ändern:

1. Entschlüsseln Sie die Objekte, die mit dem Programm Kaspersky Endpoint Security verschlüsselt wurden, bevor der Verschlüsselungsalgorithmus geändert wird.

   Nach einer Änderung des Verschlüsselungsalgorithmus sind Objekte, die früher verschlüsselt wurden, nicht mehr verfügbar.

2. Entfernen Sie Kaspersky Endpoint Security.
3. Installieren Sie Kaspersky Endpoint Security aus dem Programmpaket für Kaspersky Endpoint Security mit dem Verschlüsselungsalgorithmus für eine andere Bit-Version.

Verwendung der Technologie zur Einmalanmeldung (SSO) aktivieren

Das Verfahren zur Einmalanmeldung (SSO) ist inkompatibel mit Drittanbietern von Anmeldedaten.

Gehen Sie wie folgt vor, um die Technologie des einmaligen Anmeldens (SSO) zu aktivieren:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Verwendung der Einmalanmeldung (SSO) aktivieren möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:

- Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
- Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Allgemeine Verschlüsselungseinstellungen**.
7. Klicken Sie im Unterabschnitt **Allgemeine Verschlüsselungseinstellungen** im Block **Einstellungen für Kennwörter** auf die Schaltfläche **Einstellungen**.

   Die Registerkarte **Authentifizierungsagent** im Fenster **Einstellungen für Verschlüsselungskennwörter** wird geöffnet.
8. Aktivieren Sie das Kontrollkästchen **Technologie zur Einmalanmeldung (SSO) verwenden**.
9. Klicken Sie auf **OK**.
10. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf die Schaltfläche **OK**, um die vorgenommenen Änderungen zu speichern.
11. Wenden Sie die Richtlinie an.

    Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Besonderheiten der Dateiverschlüsselung

Bitte beachten Sie folgende Besonderheiten bei der Nutzung der Dateiverschlüsselungsfunktion:

- Die Richtlinie für Kaspersky Security Center mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger wird für eine bestimmte Gruppe verwalteter Computer erstellt. Deshalb ist das Ergebnis, das durch das Übernehmen der Richtlinie für Kaspersky Security Center mit angepasster Verschlüsselung/Entschlüsselung von Wechseldatenträgern erreicht wird, davon abhängig, mit welchen Computern ein Wechseldatenträger verbunden ist.
- Für Dateien mit dem Zugriffsstatus "nur Lesen", die auf Wechseldatenträgern gespeichert sind, führt Kaspersky Endpoint Security keine Dateiverschlüsselung/-entschlüsselung durch.
- Kaspersky Endpoint Security verschlüsselt / entschlüsselt Standardordner nur für die lokalen Benutzerprofile (local user profiles) des Betriebssystems. Kaspersky Endpoint Security verschlüsselt und entschlüsselt keine Standardordner für servergespeicherte Benutzerprofile (roaming user profiles), verbindliche Benutzerprofile (mandatory user profiles), temporäre Benutzerprofile (temporary user profiles) und Ordnerumleitung (folder redirection). Folgende Ordner gehören zur Liste der Standardordner, die von Kaspersky Lab für die Verschlüsselung empfohlen werden:
  - Eigene Dateien
  - Favoriten
  - Cookies-Dateien
  - Desktop

- Temporäre Dateien für Internet Explorer
- Temporäre Dateien
- Outlook-Dateien

- Für Dateien, deren Veränderung die Funktionsfähigkeit des Betriebssystems und der installierten Programme beeinträchtigen kann, führt Kaspersky Endpoint Security keine Verschlüsselung durch. Zur Liste der Verschlüsselungsausnahmen gehören beispielsweise folgende Dateien und Ordner mit allen untergeordneten Ordnern:
  - %WINDIR%
  - %PROGRAMFILES%, %PROGRAMFILES(X86)%
  - Dateien der Systemregistrierung von Windows

  Die Liste mit Ausnahmen von der Verschlüsselung kann nicht angezeigt oder geändert werden. Dateien und Ordner aus der Liste mit Ausnahmen aus der Verschlüsselung können der Verschlüsselungsliste hinzugefügt werden; sie werden jedoch bei der Ausführung der Aufgabe zur Dateiverschlüsselung nicht verschlüsselt.

- Als Wechseldatenträger werden folgende Gerätetypen unterstützt:
  - Datenträger, die über eine USB-Schnittstelle verbunden werden
  - Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden
  - SSD-Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden

Dateiverschlüsselung auf lokalen Festplatten des Computers

Die Verschlüsselung von Dateien auf lokalen Laufwerken ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows Workstation installiert ist. Die Verschlüsselung von Dateien auf lokalen Laufwerken ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Dateiserver installiert ist.

Dieser Abschnitt enthält Informationen zur Verschlüsselung von Dateien auf lokalen Laufwerken. Außerdem wird hier erklärt, wie die Verschlüsselung von Dateien auf lokalen Laufwerken mithilfe von Kaspersky Endpoint Security und des Verwaltungs-Plug-ins für Kaspersky Endpoint Security angepasst und ausgeführt wird.

Dateiverschlüsselung auf lokalen Festplatten des Computers starten

Gehen Sie wie folgt vor, um Dateien auf lokalen Festplatten des Computers zu verschlüsseln:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Dateiverschlüsselung auf lokalen Laufwerken anpassen möchten.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Wählen Sie die gewünschte Richtlinie aus.

5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:

   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Dateien verschlüsseln**.

7. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Verschlüsselung**.

8. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Gemäß den Regeln**.

9. Klicken Sie auf der Registerkarte **Verschlüsselung** auf **Hinzufügen** und wählen Sie in der Dropdown-Liste eines der folgenden Elemente:

   a. Wählen Sie das Element **Standardordner**, um die von Kaspersky Lab empfohlenen Dateien aus den Ordnern der lokalen Benutzerprofile zur Verschlüsselungsregel hinzuzufügen.

      Das Fenster **Standardordner auswählen** wird geöffnet.

   b. Wählen Sie das Element **Ordnerpfad**, um einen Ordner, dessen Pfad manuell angegeben wird, zur Verschlüsselungsregel hinzuzufügen.

      Das Fenster **Ordner manuell hinzufügen** wird geöffnet.

   c. Wählen Sie das Element **Dateien nach Erweiterung**, um Dateierweiterungen zur Verschlüsselungsregel hinzuzufügen. Kaspersky Endpoint Security verschlüsselt die Dateien mit den angegebenen Erweiterungen auf allen lokalen Festplatten des Computers.

      Das Fenster **Liste für Dateierweiterungen hinzufügen / ändern** wird geöffnet.

   d. Wählen Sie das Element **Dateien nach Gruppe(n) für Erweiterungen**, um Gruppen von Dateierweiterungen zur Verschlüsselungsregel hinzuzufügen. Kaspersky Endpoint Security verschlüsselt die Dateien mit den Erweiterungen, die in den Erweiterungsgruppen aufgezählt sind, auf allen lokalen Festplatten des Computers.

      Das Fenster **Gruppen für Dateierweiterungen wählen** wird geöffnet.

10. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf die Schaltfläche **OK**, um die vorgenommenen Änderungen zu speichern.

11. Wenden Sie die Richtlinie an.

    Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Sofort nachdem die Richtlinie übernommen wurde, verschlüsselt Kaspersky Endpoint Security jene Dateien, die in der Verschlüsselungsregel angegeben sind und nicht in der Entschlüsselungsregel angegeben sind.

Wurde eine Datei sowohl zur Verschlüsselungsregel als auch zur Entschlüsselungsregel hinzugefügt, so geht Kaspersky Endpoint Security wie folgt vor: Wenn die Datei nicht verschlüsselt ist, wird sie nicht verschlüsselt, und wenn die Datei verschlüsselt ist, wird sie entschlüsselt.

Kaspersky Endpoint Security verschlüsselt unverschlüsselte Dateien, wenn deren Eigenschaften (Dateipfad, Dateiname, Dateierweiterung) nach der Änderung weiterhin die Kriterien der Verschlüsselungsregel erfüllen.

Kaspersky Endpoint Security wartet mit der Verschlüsselung geöffneter Dateien, bis sie geschlossen werden.

Erstellt der Benutzer eine neue Datei, deren Eigenschaften die Kriterien der Verschlüsselungsregel erfüllen, so verschlüsselt Kaspersky Endpoint Security die Datei sofort, wenn die Datei geöffnet wird.

Wenn Sie eine verschlüsselte Datei in einen anderen Ordner des lokalen Laufwerks verschieben, bleibt die Datei verschlüsselt, unabhängig davon, ob dieser Ordner zur Verschlüsselungsregel gehört.

Programmzugriffsrechte für verschlüsselte Dateien formulieren

Gehen Sie wie folgt vor, um Programmzugriffsrechte für verschlüsselte Dateien zu formulieren:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der entsprechenden Administrationsgruppe, für die Sie Regeln für den Zugriff von Programmen auf verschlüsselte Dateien erstellen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Dateien verschlüsseln**.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Gemäß den Regeln**.

   Zugriffsregeln gelten nur im Modus **Gemäß den Regeln**. Wenn Sie nach dem Übernehmen von Zugriffsregeln im Modus **Gemäß den Regeln** in den Modus **Nicht verändern** wechseln, so ignoriert Kaspersky Endpoint Security alle Zugriffsregeln. Alle Programme besitzen Zugriff auf alle verschlüsselten Dateien.

8. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Regeln für Programme**.

9. Wenn Sie ausschließlich Programme aus der Liste von Kaspersky Security Center wählen möchten, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme aus der Kaspersky Security Center Liste**.

   Das Fenster **Programme aus der Liste für Kaspersky Security Center hinzufügen** wird geöffnet.

   Gehen Sie wie folgt vor:

   a. Geben Sie Filter für die Anzeige der Programmliste in der Tabelle an. Geben Sie dazu Werte für die Einstellungen **Programm**, **Hersteller**, **Hinzugefügt** sowie für die Kontrollkästchen aus dem Block **Gruppe** an.

   b. Klicken Sie auf **Aktualisieren**.

      In der Tabelle wird eine Programmliste angezeigt, die den angegebenen Filtern entspricht.

   c. Aktivieren Sie in der Spalte **Programme** die Kontrollkästchen der Programme, für die Sie Zugriffsregeln für verschlüsselte Dateien erstellen möchten.

   d. Wählen Sie in der Dropdown-Liste **Regel für Programm(e)** eine Regel, die den Zugriff von Programmen auf verschlüsselte Dateien festlegt.

   e. Wählen Sie in der Dropdown-Liste **Aktion für bereits ausgewählte Programme** die Aktion, welche Kaspersky Endpoint Security mit den Zugriffsregeln für verschlüsselte Dateien ausführen soll, die bereits für die oben angegebenen Programme vorhanden sind.

   f. Klicken Sie auf **OK**.

   Die Informationen zur Programmzugriffsregel für verschlüsselte Dateien werden in der Tabelle in der Registerkarte **Regeln für Programme** angezeigt.

10. Um ein Programm manuell zu wählen, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme manuell**.

    Das Fenster **Namen von ausführbaren Programmdateien hinzufügen / ändern** wird geöffnet.

    Gehen Sie wie folgt vor:

    a. Geben Sie im Eingabefeld einen Namen oder eine Liste mit Namen von ausführbaren Programmdateien und deren Erweiterungen ein.

       Sie können die Namen von ausführbaren Programmdateien auch aus der Liste für Kaspersky Security Center hinzufügen. Klicken Sie dazu auf **Aus der Liste für Kaspersky Security Center hinzufügen**.

    b. Geben Sie erforderlichenfalls im Feld **Beschreibung** eine Beschreibung der Programmliste ein.

    c. Wählen Sie in der Dropdown-Liste **Regel für Programm(e)** eine Regel, die den Zugriff von Programmen auf verschlüsselte Dateien festlegt.

    d. Klicken Sie auf **OK**.

    Die Informationen zur Programmzugriffsregel für verschlüsselte Dateien werden in der Tabelle in der Registerkarte **Regeln für Programme** angezeigt.

11. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Verschlüsselung von Dateien, die von bestimmten Programmen erstellt und geändert werden

Sie können eine Regel erstellen, nach der Kaspersky Endpoint Security alle Dateien verschlüsseln soll, welche von in der Regel angegebenen Programmen erstellt oder geändert werden.

> Dateien, die von den angegebenen Programmen erstellt oder geändert worden sind, bevor die Verschlüsselungsregel übernommen wurde, werden nicht verschlüsselt.

Um die Verschlüsselung von Dateien anzupassen, die von bestimmten Programmen erstellt und geändert werden, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der entsprechenden Administrationsgruppe, für welche Sie die Verschlüsselung von Dateien anpassen möchten, die von bestimmten Programmen erstellt werden.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Dateien verschlüsseln**.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Gemäß den Regeln**.

   > Verschlüsselungsregeln gelten nur im Modus **Gemäß den Regeln**. Wenn Sie nach dem Übernehmen von Verschlüsselungsregeln im Modus **Gemäß den Regeln** in den Modus **Nicht verändern** wechseln, so ignoriert Kaspersky Endpoint Security alle Verschlüsselungsregeln. Dateien, die zuvor verschlüsselt worden sind, bleiben weiterhin verschlüsselt.

8. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Regeln für Programme**.
9. Wenn Sie ausschließlich Programme aus der Liste von Kaspersky Security Center wählen möchten, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme aus der Kaspersky Security Center Liste**.

   Das Fenster **Programme aus der Liste für Kaspersky Security Center hinzufügen** wird geöffnet.

Gehen Sie wie folgt vor:

a. Geben Sie Filter für die Anzeige der Programmliste in der Tabelle an. Geben Sie dazu Werte für die Einstellungen **Programm**, **Hersteller**, **Hinzugefügt** sowie für die Kontrollkästchen aus dem Block **Gruppe** an.

b. Klicken Sie auf **Aktualisieren**.

In der Tabelle wird eine Programmliste angezeigt, die den angegebenen Filtern entspricht.

c. Aktivieren Sie in der Spalte **Programme** die Kontrollkästchen jener Programme, deren erstellte Dateien verschlüsselt werden sollen.

d. Wählen Sie in der Liste **Regel für Programm(e)** das Element **Alle neu erstellten Dateien verschlüsseln**.

e. Wählen Sie in der Dropdown-Liste **Aktion für bereits ausgewählte Programme** die Aktion, welche Kaspersky Endpoint Security mit den Verschlüsselungsregeln für Dateien ausführen soll, die bereits für die oben angegebenen Programme erstellt worden sind.

f. Klicken Sie auf **OK**.

Informationen über die Verschlüsselungsregel für Dateien, die von den ausgewählten Programmen erstellt und geändert wurden, werden in einer Tabelle auf der Registerkarte **Regeln für Programme** angezeigt.

10. Um ein Programm manuell zu wählen, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme manuell**.

Das Fenster **Namen von ausführbaren Programmdateien hinzufügen / ändern** wird geöffnet.

Gehen Sie wie folgt vor:

a. Geben Sie im Eingabefeld einen Namen oder eine Liste mit Namen von ausführbaren Programmdateien und deren Erweiterungen ein.

Sie können die Namen von ausführbaren Programmdateien auch aus der Liste für Kaspersky Security Center hinzufügen. Klicken Sie dazu auf **Aus der Liste für Kaspersky Security Center hinzufügen**.

b. Geben Sie erforderlichenfalls im Feld **Beschreibung** eine Beschreibung der Programmliste ein.

c. Wählen Sie in der Liste **Regel für Programm(e)** das Element **Alle neu erstellten Dateien verschlüsseln**.

d. Klicken Sie auf **OK**.

Informationen über die Verschlüsselungsregel für Dateien, die von den ausgewählten Programmen erstellt und geändert wurden, werden in einer Tabelle auf der Registerkarte **Regeln für Programme** angezeigt.

11. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Entschlüsselungsregel erstellen

Um eine Entschlüsselungsregel zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen jener Administrationsgruppe, für welche Sie eine Liste mit zu entschlüsselnden Dateien erstellen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Dateien verschlüsseln**.
7. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Entschlüsselung**.
8. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Gemäß den Regeln**.
9. Klicken Sie auf der Registerkarte **Entschlüsselung** auf **Hinzufügen** und wählen Sie in der Dropdown-Liste eines der folgenden Elemente:
   a. Wählen Sie das Element **Standardordner**, um die von Kaspersky Lab empfohlenen Dateien aus den Ordnern der lokalen Benutzerprofile zur Entschlüsselungsregel hinzuzufügen.

      Das Fenster **Standardordner auswählen** wird geöffnet.

   b. Wählen Sie das Element **Ordnerpfad**, um den Ordner, dessen Pfad manuell angegeben wird, zur Entschlüsselungsregel hinzuzufügen.

      Das Fenster **Ordner manuell hinzufügen** wird geöffnet.

   c. Wählen Sie das Element **Dateien nach Erweiterung**, um Dateierweiterungen zur Entschlüsselungsregel hinzuzufügen. Dateien mit den angegebenen Erweiterungen werden auf allen lokalen Festplatten des Computers nicht von Kaspersky Endpoint Security verschlüsselt.

      Das Fenster **Liste für Dateierweiterungen hinzufügen / ändern** wird geöffnet.

   d. Wählen Sie das Element **Dateien nach Gruppe(n) für Erweiterungen**, um Gruppen von Dateierweiterungen zur Entschlüsselungsregel hinzuzufügen. Dateien mit den Erweiterungen, die in den Erweiterungsgruppen aufgezählt sind, werden auf allen lokalen Festplatten des Computers nicht von Kaspersky Endpoint Security verschlüsselt.

      Das Fenster **Gruppen für Dateierweiterungen wählen** wird geöffnet.
10. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf die Schaltfläche **OK**, um die vorgenommenen Änderungen zu speichern.
11. Wenden Sie die Richtlinie an.

Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Wurde eine Datei sowohl zur Verschlüsselungsregel als auch zur Entschlüsselungsregel hinzugefügt, so geht Kaspersky Endpoint Security wie folgt vor: Wenn die Datei nicht verschlüsselt ist, wird sie nicht verschlüsselt, und wenn die Datei verschlüsselt ist, wird sie entschlüsselt.

Dateientschlüsselung auf lokalen Festplatten des Computers

Gehen Sie wie folgt vor, um Dateien auf lokalen Datenträgern des Computers zu entschlüsseln:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Entschlüsselung von Dateien auf lokalen Laufwerken anpassen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die entsprechende Richtlinie.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Dateien verschlüsseln**.
7. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Verschlüsselung**.
8. Schließen Sie aus der Verschlüsselungsliste alle Dateien und Ordner aus, die Sie entschlüsseln möchten. Wählen Sie dazu in der Liste diese Dateien aus und wählen Sie im Kontextmenü der Schaltfläche **Löschen** den Punkt **Regel löschen und Dateien entschlüsseln**.

   Sie können mehrere Elemente gleichzeitig aus der Verschlüsselungsliste löschen. Halten Sie dazu die Taste **STRG** gedrückt, während Sie mit der linken Maustaste die entsprechenden Elemente auswählen. Wählen Sie dann im Kontextmenü der Schaltfläche **Löschen** den Punkt **Regel löschen und Dateien entschlüsseln** aus.

   Die aus der Verschlüsselungsliste gelöschten Dateien und Ordner werden automatisch zur Entschlüsselungsliste hinzugefügt.
9. Erstellen Sie eine Dateiliste für Entschlüsselung
10. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf die Schaltfläche **OK**, um die vorgenommenen Änderungen zu speichern.
11. Wenden Sie die Richtlinie an.

Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Unmittelbar nach der Übernahme der Richtlinie entschlüsselt Kaspersky Endpoint Security die verschlüsselten Dateien, die der Entschlüsselungsliste hinzugefügt wurden.

Kaspersky Endpoint Security entschlüsselt verschlüsselte Dateien, wenn ihre Parameter (Dateipfad / Dateiname / Dateierweiterung) geändert wurden und nach der Änderung den Parametern der Objekte entsprechen, die in die Entschlüsselungsliste aufgenommen sind.

Kaspersky Endpoint Security wartet mit der Entschlüsselung geöffneter Dateien, bis sie geschlossen werden.

Verschlüsselte Archive erstellen

Während der Erstellung eines verschlüsselten Archivs nimmt Kaspersky Endpoint Security keine Dateikomprimierung vor.

Gehen Sie folgendermaßen vor, um ein verschlüsseltes Archiv zu erstellen:

1. Verwenden Sie auf einem Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist und auf dem die Funktionalität zur Dateiverschlüsselung verfügbar ist, einen beliebigen Dateimanager, um jene Dateien und/oder Ordner zu markieren, die Sie zu einem verschlüsselten Archiv hinzufügen möchten. Öffnen Sie durch Rechtsklick das Kontextmenü.

2. Wählen Sie den Punkt **Verschlüsseltes Archiv erstellen** im Kontextmenü.

   Das Windows-Standardfenster **Pfad zum Speichern des verschlüsselten Archivs festlegen** wird geöffnet.

3. Wählen Sie im Microsoft-Windows-Standardfenster **Pfad zum Speichern des verschlüsselten Archivs festlegen**, wo das verschlüsselte Archiv auf dem Wechseldatenträger gespeichert werden soll. Klicken Sie auf **Speichern**.

   Das Fenster **Verschlüsseltes Archiv erstellen** wird geöffnet.

4. Geben Sie im Fenster **Verschlüsseltes Archiv erstellen** ein Kennwort ein und wiederholen Sie dieses.

5. Klicken Sie auf die Schaltfläche **Erstellen**.

   Der Vorgang zur Erstellung eines verschlüsselten Archivs wird gestartet. Nach Abschluss des Vorgangs wird am angegebenen Speicherort auf dem Wechseldatenträger ein verschlüsseltes kennwortgeschütztes selbstentpackendes Archiv erstellt.

Wenn Sie die Erstellung eines verschlüsselten Archivs abbrechen, führt Kaspersky Endpoint Security folgende Aktionen durch:

1. Das Programm stoppt die Kopiervorgänge der Dateien ins Archiv und beendet alle etwaigen Vorgänge der Archivverschlüsselung.

2. Es löscht alle temporären Dateien, die während der Archiverstellung und -verschlüsselung erstellt wurden, sowie die Datei des verschlüsselten Archivs.

3. Es informiert über die zwangsläufige Beendigung des Prozesses zur Erstellung eines verschlüsselten Archivs.

Verschlüsselte Archive entpacken

Gehen Sie folgendermaßen vor, um ein verschlüsseltes Archiv zu entpacken:

1. Markieren Sie in einem beliebigen Dateimanager das verschlüsselte Archiv und starten Sie mit der linken Maustaste den Extraktionsassistenten für verschlüsselte Archive.

   Es öffnet sich das Fenster **Kennworteingabe**.

2. Geben Sie das Kennwort ein, mit dem das verschlüsselte Archiv geschützt ist.

3. Klicken Sie im Fenster **Kennworteingabe** auf **OK**.

   Ist das Kennwort korrekt, öffnet sich das Standardfenster von Microsoft Windows **Ordner durchsuchen**.

4. Wählen Sie im Standardfenster von Microsoft Windows **Ordner durchsuchen** einen Ordner zum Entpacken des verschlüsselten Archivs und klicken Sie auf die Schaltfläche **OK**.

   Der Vorgang zum Entpacken des verschlüsselten Archivs in den angegebenen Ordner wird gestartet.

> Wenn das verschlüsselte Archiv bereits in den angegebenen Ordner entpackt wurde, werden die Dateien des verschlüsselten Archivs beim zweiten Entpackungsvorgang überschrieben.

Wenn Sie das Entpacken eines verschlüsselten Archivs abbrechen, führt Kaspersky Endpoint Security folgende Aktionen durch:

1. Der Entschlüsselungsvorgang des Archivs wird angehalten und alle etwaigen Kopiervorgänge der Dateien aus dem verschlüsselten Archiv werden unterbrochen.

2. Alle temporären Dateien, die während der Entschlüsselung und Entpackung des verschlüsselten Archivs erstellt wurden, sowie alle Dateien, die bereits aus dem verschlüsselten Archiv in den angegebenen Ordner kopiert wurden, werden gelöscht.

3. Der Benutzer wird über den zwangsläufigen Abbruch des Prozesses zur Entpackung eines verschlüsselten Archivs informiert.

Wechseldatenträger verschlüsseln

> Die Verschlüsselung von Wechseldatenträgern ist verfügbar, wenn Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows Workstation installiert ist. Die Verschlüsselung von Wechseldatenträgern ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Dateiserver installiert ist.

Dieser Abschnitt informiert über die Verschlüsselung von Wechseldatenträgern. Außerdem wird hier erklärt, wie die Verschlüsselung von Wechseldatenträgern mithilfe von Kaspersky Endpoint Security und des

Verwaltungs-Plug-ins für Kaspersky Endpoint Security angepasst und ausgeführt werden.

Verschlüsselung von Wechseldatenträgern starten

Um Wechseldatenträger zu verschlüsseln, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Verschlüsselung von Wechseldatenträgern anpassen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Wechseldatenträger verschlüsseln**.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** eine Aktion, die Kaspersky Endpoint Security standardmäßig mit allen Wechseldatenträgern ausführen soll, die mit Computern der gewählten Administrationsgruppe verbunden werden:
   - **Gesamten Wechseldatenträger verschlüsseln**. Bei Auswahl dieses Elements geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie für Kaspersky Security Center mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Der Inhalt von Wechseldatenträgern wird sektorbasiert verschlüsselt. Dabei werden nicht nur die Dateien verschlüsselt, die auf Wechseldatenträgern gespeichert sind, sondern auch die Dateisysteme der Wechseldatenträger sowie Dateinamen und Ordnerstrukturen auf Wechseldatenträgern. Bereits verschlüsselte Wechseldatenträger werden von Kaspersky Endpoint Security nicht erneut verschlüsselt.

     Diese Verschlüsselungsvariante bietet die Funktionalität der vollständigen Festplattenverschlüsselung durch das Programm Kaspersky Endpoint Security.

   - **Alle Dateien verschlüsseln**. Bei Auswahl dieses Elements geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie für Kaspersky Security Center mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Alle Dateien, die auf Wechseldatenträgern gespeichert sind, werden verschlüsselt. Bereits verschlüsselte Dateien werden von Kaspersky Endpoint Security nicht erneut verschlüsselt. Die Dateisysteme von Wechseldatenträgern sowie die Namen verschlüsselter Dateien und die Ordnerstruktur werden nicht verschlüsselt.

- **Nur neue Dateien verschlüsseln**. Bei Auswahl dieses Elements geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie für Kaspersky Security Center mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Es werden nur jene Dateien verschlüsselt, die auf Wechseldatenträgern gespeichert wurden oder die auf Wechseldatenträgern gespeichert waren und geändert wurden, nachdem die Richtlinie für Kaspersky Security Center zum letzten Mal übernommen wurde.

- **Gesamten Wechseldatenträger entschlüsseln**. Bei Auswahl dieses Elements geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie für Kaspersky Security Center mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Alle verschlüsselten Dateien, die auf Wechseldatenträgern gespeichert sind, sowie ihre Dateisysteme, falls diese verschlüsselt sind, werden entschlüsselt.

  Diese Verschlüsselungsvariante gewährleistet nicht nur die Verschlüsselungsfunktion für Dateien, sondern auch die Funktion zur vollständigen Festplattenverschlüsselung von Kaspersky Endpoint Security.

- **Nicht verändern**. Bei Auswahl dieses Elements geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie für Kaspersky Security Center mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Dateien auf Wechseldatenträgern werden nicht verschlüsselt und nicht entschlüsselt.

Kaspersky Endpoint Security unterstützt die Verschlüsselung von FAT- und NTFS-Dateisystemen. Wenn die Variante **Alle Dateien verschlüsseln** oder **Nur neue Dateien verschlüsseln** ausgewählt ist und mit dem Computer ein Wechseldatenträger mit einem nicht unterstützten Dateisystem verbunden ist, wird die Verschlüsselungsaufgabe dieses Wechseldatenträgers mit einem Fehler abgeschlossen und Kaspersky Endpoint Security legt für diesen Wechseldatenträger den Zugriffsstatus "Nur Lesen" fest.

8. Erstellen Sie Regeln für die Dateiverschlüsselung auf Wechseldatenträgern, deren Inhalt Sie verschlüsseln möchten.

9. Wenden Sie die Richtlinie an.

Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Wenn der Benutzer einen Wechseldatenträger verbindet oder dieser bereits verbunden ist, informiert Kaspersky Endpoint Security den Benutzer sofort nach dem Übernehmen der Richtlinie darüber, dass für den Wechseldatenträger eine Verschlüsselungsregel übernommen wird, nach welcher die Daten des Wechseldatenträgers verschlüsselt werden.

Wenn für die Datenverschlüsselung auf dem Wechseldatenträger die Regel *Nicht verändern* festgelegt ist, wird der Benutzer nicht informiert.

Das Programm warnt den Benutzer, dass die Verschlüsselung einige Zeit in Anspruch nehmen kann.

Das Programm bittet den Benutzer um eine Bestätigung der Durchführung des Verschlüsselungsvorgangs und führt folgende Aktionen durch:

- Es verschlüsselt Daten gemäß den Richtlinieneinstellungen, wenn der Benutzer die Anfrage zur Verschlüsselung bestätigt.
- Es belässt die Daten unverschlüsselt, wenn der Benutzer die Verschlüsselungsanfrage ablehnt, und es beschränkt den Zugriff auf die Dateien des Wechseldatenträgers auf das Lesen.
- Es belässt die Daten unverschlüsselt, wenn der Benutzer die Verschlüsselungsanfrage nicht beantwortet, beschränkt den Zugriff auf die Dateien des Wechseldatenträgers auf das Lesen, und fragt erneut nach einer Bestätigung für die Datenverschlüsselung, wenn die Richtlinie für Kaspersky Security Center zum nächsten Mal übernommen wird oder wenn der Wechseldatenträger zum nächsten Mal verbunden wird.

Die Richtlinie für Kaspersky Security Center mit den angegebenen Verschlüsselungseinstellungen für die Daten von Wechseldatenträgern wird für eine bestimmte Gruppe verwalteter Computer erstellt. Deshalb hängt das Ergebnis der Datenverschlüsselung von Wechseldatenträgern davon ab, mit welchem Computer der Wechseldatenträger verbunden ist.

Initiiert der Benutzer während der Datenverschlüsselung das sichere Entfernen des Wechseldatenträgers, so bricht Kaspersky Endpoint Security die Datenverschlüsselung ab und ermöglicht so, den Wechseldatenträger vor dem Abschluss des Verschlüsselungsvorgangs sicher zu entfernen.

Verschlüsselungsregel für Wechseldatenträger hinzufügen

Um eine Verschlüsselungsregel für Wechseldatenträger hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie Verschlüsselungsregeln für Wechseldatenträger hinzufügen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Wechseldatenträger verschlüsseln**.
7. Klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste eines der folgenden Elemente aus:
   - Um Verschlüsselungsregeln für Wechseldatenträger hinzuzufügen, die auf der Liste der vertrauenswürdigen Geräte für die Komponente Gerätekontrolle stehen, wählen Sie das Element **Aus der Liste für vertrauenswürdige Geräte dieser Richtlinie**.

Das Fenster **Geräte aus der Liste der vertrauenswürdigen Geräte hinzufügen** wird geöffnet.

- Um Verschlüsselungsregeln für Wechseldatenträger hinzuzufügen, die auf der Liste für Kaspersky Security Center stehen, wählen Sie das Element **Aus der Liste für Kaspersky Security Center**.

  Das Fenster **Geräte aus der Liste für Kaspersky Security Center hinzufügen** wird geöffnet.

8. Wenn Sie beim vorherigen Schritt das Element **Aus der Liste für Kaspersky Security Center** gewählt haben, legen Sie Anzeigefilter für die Geräte in der Tabelle fest. Gehen Sie dazu folgendermaßen vor:

   a. Geben Sie Werte für die folgenden Einstellungen an: **In der Tabelle die Geräte anzeigen, für die festgelegt ist**, **Name**, **Computer**, **Kaspersky-Festplattenverschlüsselung**.

   b. Klicken Sie auf **Aktualisieren**.

9. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus für die ausgewählten Geräte** die Aktion aus, die Kaspersky Endpoint Security mit auf Wechseldatenträgern gespeicherten Dateien ausführen soll.

10. Aktivieren Sie das Kontrollkästchen **Portabler Modus**, wenn Kaspersky Endpoint Security die Wechseldatenträger vor der Verschlüsselung so vorbereiten soll, dass die darauf verschlüsselten Dateien im portablen Modus verfügbar sind.

    Im portablen Modus können verschlüsselte Dateien auf Wechseldatenträgern auch dann verwendet werden, wenn der Wechseldatenträger mit einem Computer verbunden ist, auf dem die Verschlüsselungsfunktion nicht verfügbar ist.

11. Aktivieren Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln**, damit Kaspersky Endpoint Security nur jene Laufwerkssektoren verschlüsselt, die mit Dateien belegt sind.

    Verwenden Sie die Verschlüsselung auf einem Datenträger, der bereits benutzt wurde, so sollte der gesamte Datenträger verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, aus denen noch Informationen entnommen werden können. Die Funktion **Nur belegten Speicherplatz verschlüsseln** wird für neue Datenträger empfohlen, die bisher noch nicht benutzt wurden.

    Wenn ein Gerät zuvor mit der Funktion **Nur belegten Speicherplatz verschlüsseln** verschlüsselt wurde, so werden Sektoren, die nicht mit Dateien belegt sind, auch dann weiterhin nicht verschlüsselt, nachdem eine Richtlinie im Modus **Gesamten Wechseldatenträger verschlüsseln** übernommen wurde.

12. Wählen Sie in der Dropdown-Liste **Aktion für bereits ausgewählte Geräte** die Aktion aus, die Kaspersky Endpoint Security mit Verschlüsselungsregeln ausführen soll, die bereits für Wechseldatenträger festgelegt wurden.

    - Wenn Sie eine zuvor erstellte Verschlüsselungsregel für einen Wechseldatenträger nicht ändern möchten, wählen Sie das Element **Überspringen**.

    - Wenn Sie eine zuvor erstellte Verschlüsselungsregel für einen Wechseldatenträger durch eine neue Regel ersetzen möchten, wählen Sie das Element **Aktualisieren**.

13. Klicken Sie auf **OK**.

    Zeilen mit den Einstellungen der erstellten Verschlüsselungsregeln werden in der Tabelle **Manuell festgelegte Regeln** angezeigt.

14. Klicken Sie auf **OK**, um die Änderungen zu speichern.

    Die hinzugefügten Verschlüsselungsregeln für Wechseldatenträger werden für alle Wechseldatenträger übernommen, die mit Computern verbunden sind, welche der geänderten Richtlinie für Kaspersky Security Center unterliegen.

Verschlüsselungsregel für Wechseldatenträger ändern

Um die Verschlüsselungsregel für einen Wechseldatenträger zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Verschlüsselungsregel für den Wechseldatenträger ändern möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Wechseldatenträger verschlüsseln**.
7. Wählen Sie in der Liste der Wechseldatenträger, für die Verschlüsselungsregeln vorliegen, den Eintrag des entsprechenden Wechseldatenträgers.
8. Klicken Sie auf **Regel angeben**, um die Verschlüsselungsregel für diesen Wechseldatenträger zu ändern.

   Das Kontextmenü der Schaltfläche **Regel angeben** wird geöffnet.
9. Wählen Sie im Kontextmenü der Schaltfläche **Regel angeben** die Aktion, die Kaspersky Endpoint Security mit Dateien auf dem gewählten Wechseldatenträger ausführen soll.
10. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Die geänderten Verschlüsselungsregeln für Wechseldatenträger werden für alle Wechseldatenträger übernommen, die mit Computern verbunden sind, welche der geänderten Richtlinie für Kaspersky Security Center unterliegen.

Den portablen Modus für die Verwendung verschlüsselter Dateien auf Wechseldatenträgern aktivieren

Um den portablen Modus zu aktivieren, in dem verschlüsselte Dateien auf Wechseldatenträgern verwendet werden können, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie den portablen Modus für die Verwendung verschlüsselter Dateien auf Wechseldatenträgern aktivieren möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Wechseldatenträger verschlüsseln**.
7. Aktivieren Sie das Kontrollkästchen **Portabler Modus**.

   Der Portable Modus ist nur verfügbar, wenn in der Dropdown-Liste **Verschlüsselungsmodus für die ausgewählten Geräte** das Element **Alle Dateien verschlüsseln** oder **Nur neue Dateien verschlüsseln** ausgewählt ist.

8. Klicken Sie auf **OK**.
9. Wenden Sie die Richtlinie an.

   Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

10. Verbinden Sie den Wechseldatenträger mit einem Computer, an welchen die Richtlinie für Kaspersky Security Center verteilt wurde.
11. Bestätigen Sie den Vorgang zur Verschlüsselung des Wechseldatenträgers.

    Ein Fenster zum Erstellen eines Kennworts für den portablen Dateimanager wird geöffnet.

12. Legen Sie ein Kennwort fest, das den Anforderungen entspricht, und bestätigen Sie das Kennwort.
13. Klicken Sie auf **OK**.

    Kaspersky Endpoint Security verschlüsselt die Dateien auf dem Wechseldatenträger gemäß den Verschlüsselungsregeln, die in der Richtlinie für Kaspersky Security Center festgelegt sind. Der portable Dateimanager für die Verwendung verschlüsselter Dateien ist auch auf dem Wechseldatenträger gespeichert.

Ist der portable Modus aktiviert, so können verschlüsselte Dateien auf Wechseldatenträgern auch dann verwendet werden, wenn der Wechseldatenträger mit einem Computer verbunden ist, auf dem die Verschlüsselungsfunktion nicht verfügbar ist.

Wechseldatenträger entschlüsseln

Um Wechseldatenträger zu entschlüsseln, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Entschlüsselung von Wechseldatenträgern anpassen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Wechseldatenträger verschlüsseln**.
7. Um alle verschlüsselten Dateien zu entschlüsseln, die auf Wechseldatenträgern gespeichert sind, wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Aktion **Gesamten Wechseldatenträger entschlüsseln**.
8. Um die Daten zu entschlüsseln, die auf bestimmten Wechseldatenträgern gespeichert sind, ändern Sie die Verschlüsselungsregeln für die entsprechenden Wechseldatenträger. Gehen Sie dazu folgendermaßen vor:
   a. Wählen Sie in der Liste der Wechseldatenträger, für die Verschlüsselungsregeln vorliegen, den Eintrag des entsprechenden Wechseldatenträgers.
   b. Klicken Sie auf **Regel angeben**, um die Verschlüsselungsregel für diesen Wechseldatenträger zu ändern.

      Das Kontextmenü der Schaltfläche **Regel angeben** wird geöffnet.
   c. Wählen Sie im Kontextmenü der Schaltfläche **Regel angeben** den Punkt **Alle Dateien entschlüsseln** aus.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern.
10. Wenden Sie die Richtlinie an.

Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Wenn der Benutzer einen Wechseldatenträger verbindet oder dieser bereits verbunden ist, informiert Kaspersky Endpoint Security den Benutzer sofort nach dem Übernehmen der Richtlinie darüber, dass für den Wechseldatenträger eine Verschlüsselungsregel übernommen wird, mit welcher die verschlüsselten

Dateien, die auf dem Wechseldatenträger gespeichert sind, sowie gegebenenfalls das verschlüsselte Dateisystem des Wechseldatenträgers entschlüsselt werden. Das Programm warnt den Benutzer, dass die Entschlüsselung einige Zeit in Anspruch nehmen kann.

Die Richtlinie für Kaspersky Security Center mit den angegebenen Verschlüsselungseinstellungen für Daten auf Wechseldatenträgern wird für eine bestimmte Gruppe verwalteter Computer erstellt. Deshalb hängt das Ergebnis der Datenentschlüsselung auf Wechseldatenträgern davon ab, mit welchem Computer der Wechseldatenträger verbunden ist.

Initiiert der Benutzer während der Datenentschlüsselung das sichere Entfernen des Wechseldatenträgers, so bricht Kaspersky Endpoint Security die Datenentschlüsselung ab und ermöglicht so, den Wechseldatenträger vor dem Abschluss des Entschlüsselungsvorgangs sicher zu entfernen.

Vollständige Festplattenverschlüsselung

Ist das Programm Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Workstation installiert, so sind für die Verschlüsselung die Technologien BitLocker-Laufwerkverschlüsselung und Kaspersky-Festplattenverschlüsselung verfügbar. Ist das Programm Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows für Dateiserver installiert, so ist nur die Technologie BitLocker-Laufwerkverschlüsselung verfügbar.

Dieser Abschnitt enthält Informationen zur vollständigen Festplattenverschlüsselung und erklärt, wie die vollständige Festplattenverschlüsselung mithilfe von Kaspersky Endpoint Security und des Verwaltungs-Plug-ins von Kaspersky Endpoint Security eingerichtet und ausgeführt wird.

Über die vollständige Festplattenverschlüsselung

Bevor die vollständige Festplattenverschlüsselung gestartet wird, überprüft das Programm, ob die Verschlüsselung auf dem Gerät möglich ist. Dabei wird u. a. überprüft, ob die Systemfestplatte mit dem Authentifizierungsagenten oder mit der BitLocker-Verschlüsselungskomponente kompatibel ist. Für die Kompatibilitätsprüfung ist ein Neustart des Computers erforderlich. Nach dem Neustart des Computers nimmt das Programm automatisch alle notwendigen Prüfungen vor. Wenn die Kompatibilitätsprüfung erfolgreich verläuft, startet die vollständige Festplattenverschlüsselung, nachdem das System hochgefahren und das Programm gestartet wurde. Wenn die Überprüfung ergibt, dass die Systemfestplatte nicht mit dem Authentifizierungsagenten oder mit der BitLocker-Verschlüsselungskomponente kompatibel ist, muss der Computer mit dem Reset-Knopf am Computergehäuse neu gestartet werden. Kaspersky Endpoint Security protokolliert Informationen über die Inkompatibilität. Aufgrund dieser Informationen wird die vollständige Festplattenverschlüsselung nach dem Hochfahren des Betriebssystems nicht gestartet. Die Berichte von Kaspersky Security Center enthalten Informationen über dieses Ereignis.

Wenn die Hardware-Konfiguration des Computers verändert wurde und anschließend die Systemfestplatte auf Kompatibilität mit dem Authentifizierungsagenten und mit der BitLocker-Verschlüsselungskomponente überprüft werden soll, müssen zuerst die Inkompatibilitätsinformationen gelöscht werden, die das Programm bei der vorherigen Überprüfung ermittelt hat. Geben Sie dazu vor der vollständigen Festplattenverschlüsselung in der Befehlszeile folgenden Befehl ein: `avp pbatestreset`. Wenn sich das Betriebssystem nicht mehr hochfahren lässt, nachdem die Kompatibilität der Systemfestplatte mit dem Authentifizierungsagenten überprüft wurde, müssen mithilfe des Reparatur-Tools die Objekte und Daten gelöscht werden, die nach dem Testlauf des Authentifizierungsagenten verblieben sind. Starten Sie danach Kaspersky Endpoint Security und führen Sie erneut den Befehl `avp pbatestreset` aus.

Nach dem Start der vollständigen Festplattenverschlüsselung verschlüsselt Kaspersky Endpoint Security alle Daten, die auf Festplatten geschrieben werden.

Wenn der Benutzer den Computer während der vollständigen Festplattenverschlüsselung ausschaltet oder neu startet, wird der Authentifizierungsagent vor dem nächsten Start des Betriebssystems geladen. Nach der Anmeldung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung fort.

Wechselt das Betriebssystem während der vollständigen Festplattenverschlüsselung in den Ruhezustand (hibernation mode), so wird der Authentifizierungsagent beim Beenden des Ruhezustandes geladen. Nach der Anmeldung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung fort.

Wechselt das Betriebssystem während der vollständigen Festplattenverschlüsselung in den Energiesparmodus (sleep mode), so setzt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung nach dem Beenden des Energiesparmodus fort, ohne den Authentifizierungsagenten zu laden.

Es gibt zwei Methoden, mit denen sich der Benutzer im Authentifizierungsagenten authentifizieren kann:

- Durch Eingabe von Name und Kennwort eines Benutzerkontos für den Authentifizierungsagenten, wenn das Benutzerkonto vom Administrator des lokalen Unternehmensnetzwerks mit Mitteln von Kaspersky Security Center erstellt wurde.
- Durch Eingabe des Kennworts für einen Token oder eine Smartcard, die mit dem Computer verbunden sind.

  Ein Token oder eine Smartcard kann nur verwendet werden, wenn die Festplatten des Computers mithilfe des AES256-Verschlüsselungsalgorithmus verschlüsselt sind. Sind die Festplatten des Computers mithilfe des AES56-Verschlüsselungsalgorithmus verschlüsselt, so kann dem Befehl keine elektronische Zertifikatdatei hinzugefügt werden.

Der Authentifizierungsagent unterstützt Tastaturlayouts für die folgenden Sprachen:

- Englisch (Großbritannien)
- Englisch (USA)
- Arabisch (Algerien, Marokko, Tunesien, AZERTY-Layout)
- Spanisch (Lateinamerika)
- Italienisch
- Deutsch (Deutschland und Österreich)
- Deutsch (Schweiz)
- Portugiesisch (Brasilien, ABNT2-Layout)
- Russisch (für IBM-/Windows-Tastatur mit 105 Tasten und JCUKEN-Tastaturlayout)

- Türkisch (QWERTY-Layout)
- Französisch (Frankreich)
- Französisch (Schweiz)
- Französisch (Belgien, AZERTY-Tastaturlayout)
- Japanisch (für Tastatur mit 106 Tasten und QWERTY-Tastaturlayout)

Ein Tastaturlayout steht im Authentifizierungsagenten zur Verfügung, wenn es in den Einstellungen des Betriebssystems unter Region und Sprache hinzugefügt wurde und auf dem Windows-Begrüßungsbildschirm verfügbar ist.

Wenn der Name des Benutzerkontos für den Authentifizierungsagenten Zeichen enthält, die nicht mithilfe der im Authentifizierungsagenten verfügbaren Tastaturlayouts eingegeben werden können, so ist der Zugriff auf verschlüsselte Festplatten erst möglich, nachdem die Festplatten mithilfe des Reparatur-Tools wiederhergestellt wurden oder nachdem Name und Kennwort des Benutzerkontos für den Authentifizierungsagenten wiederhergestellt wurden.

Kaspersky Endpoint Security unterstützt folgende Tokens, Smartcard-Lesegeräte und Smartcards:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Smart Card)
- SafeNet eToken 4100 72K Java (Smart Card)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB)
- Rutoken EZP (USB)
- Rutoken EZP (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Smart Card)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Reader)

- Gemalto IDPrime .NET 511

Vollständige Festplattenverschlüsselung mithilfe der Technologie Kaspersky-Festplattenverschlüsselung

Es wird empfohlen, vor dem Start der vollständigen Festplattenverschlüsselung sicherzustellen, dass der Computer nicht infiziert ist. Dazu muss eine vollständige Untersuchung oder eine Untersuchung der wichtigen Computerbereiche gestartet werden. Die vollständige Festplattenverschlüsselung auf einem Computer, der von einem Rootkit infiziert ist, kann zur Funktionsuntüchtigkeit des Computers führen.

Um eine vollständige Festplattenverschlüsselung mithilfe der Technologie Kaspersky-Festplattenverschlüsselung auszuführen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die vollständige Festplattenverschlüsselung anpassen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Vollständige Festplattenverschlüsselung**.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Variante **Kaspersky-Festplattenverschlüsselung**.

   Das Verfahren "Kaspersky-Festplattenverschlüsselung" kann nicht verwendet werden, wenn auf dem Computer Festplatten vorhanden sind, die mithilfe von BitLocker verschlüsselt sind.

8. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Aktion **Alle Festplatten verschlüsseln**.

   Wenn auf einem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung aller Festplatten nur noch jenes Betriebssystem ausführen, in dem das Programm installiert ist.

Wenn bestimmte Festplatten von der Verschlüsselung ausgenommen werden sollen, müssen Sie diese in einer Liste angeben.

9. Wählen Sie eine der folgenden Verschlüsselungsmethoden:

   - Damit nur die Festplattensektoren verschlüsselt werden, die mit Dateien belegt sind, aktivieren Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln**.

     Verwenden Sie die Verschlüsselung auf einem Datenträger, der bereits benutzt wurde, so sollte der gesamte Datenträger verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, aus denen noch Informationen entnommen werden können. Die Funktion **Nur belegten Speicherplatz verschlüsseln** wird für neue Datenträger empfohlen, die bisher noch nicht benutzt wurden.

   - Damit die gesamte Festplatte verschlüsselt wird, deaktivieren Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln**.

     Diese Funktion kann nur für unverschlüsselte Geräte verwendet werden. Wenn ein Gerät zuvor mit der Funktion **Nur belegten Speicherplatz verschlüsseln** verschlüsselt wurde, so werden Sektoren, die nicht mit Dateien belegt sind, auch dann weiterhin nicht verschlüsselt, nachdem eine Richtlinie im Modus **Alle Festplatten verschlüsseln** übernommen wurde.

10. Wenn bei der Verschlüsselung des Computers ein Kompatibilitätsproblem mit der Hardware auftritt, können Sie das Kontrollkästchen **Legacy USB Support verwenden** aktivieren, um die Unterstützung von USB-Geräten zu Beginn des Startvorgangs des Computers im BIOS einzuschalten.

    Nach dem Start des Betriebssystems beeinflusst der Status der Funktion Legacy USB Support (aktiviert/deaktiviert) die Unterstützung von USB-Geräten nicht mehr.

    Ist die Funktion Legacy USB Support aktiviert, so unterstützt der Authentifizierungsagent die Arbeit mit USB-Tokens nicht, wenn der Computer im BIOS-Modus läuft. Die Funktion sollte nur beim Auftreten von Hardware-Kompatibilitätsproblemen verwendet werden und ausschließlich für jene Computer aktiviert werden, auf welchen das Problem aufgetreten ist.

11. Klicken Sie auf **OK**, um die Änderungen zu speichern.

12. Wenden Sie die Richtlinie an.

    Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Vollständige Festplattenverschlüsselung mithilfe der Technologie BitLocker-Laufwerkverschlüsselung

Es wird empfohlen, vor dem Start der vollständigen Festplattenverschlüsselung des Computers sicherzustellen, dass der Computer nicht infiziert ist. Dazu muss eine vollständige Untersuchung oder eine Untersuchung der wichtigen Computerbereiche gestartet werden. Die vollständige Festplattenverschlüsselung auf einem Computer, der von einem Rootkit infiziert ist, kann zur Funktionsuntüchtigkeit des Computers führen.

Damit die BitLocker-Laufwerkverschlüsselung auf Computern mit einem Server-Betriebssystem einwandfrei funktioniert, kann es erforderlich sein, die Komponente **BitLocker-Laufwerkverschlüsselung** mithilfe des Assistenten zum Hinzufügen von Rollen zu installieren.

Um eine vollständige Festplattenverschlüsselung mithilfe der Technologie BitLocker-Laufwerkverschlüsselung auszuführen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die vollständige Festplattenverschlüsselung anpassen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Vollständige Festplattenverschlüsselung**.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Variante **BitLocker-Laufwerkverschlüsselung**.
8. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** den Punkt **Alle Festplatten verschlüsseln**.

   Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem die Verschlüsselung ausgeführt wurde.

9. Wenn Sie für die Informationseingabe in der Preboot-Umgebung eine Bildschirmtastatur verwenden möchten, aktivieren Sie das Kontrollkästchen **Verwendung der Authentifizierung erlauben, die Preboot-Tastatureingaben auf Tablets erfordert**.

Es wird empfohlen, diese Einstellung nur für Geräte zu verwenden, die während des Startvorgangs auch alternative Mittel für die Dateneingabe bieten, wie beispielsweise eine USB-Tastatur.

10. Wählen Sie einen der folgenden Verschlüsselungstypen:

    - Wenn Sie die Hardwareverschlüsselung verwenden möchten, aktivieren Sie das Kontrollkästchen **Hardwareverschlüsselung verwenden**.
    - Wenn Sie die softwarebasierte Verschlüsselung verwenden möchten, deaktivieren Sie das Kontrollkästchen **Hardwareverschlüsselung verwenden**.

11. Wählen Sie eine der folgenden Verschlüsselungsmethoden:

    - Damit nur die Festplattensektoren verschlüsselt werden, die mit Dateien belegt sind, aktivieren Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln**.
    - Damit die gesamte Festplatte verschlüsselt wird, deaktivieren Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln**.

      Diese Funktion kann nur für unverschlüsselte Geräte verwendet werden. Wenn ein Gerät zuvor mit der Funktion **Nur belegten Speicherplatz verschlüsseln** verschlüsselt wurde, so werden Sektoren, die nicht mit Dateien belegt sind, auch dann weiterhin nicht verschlüsselt, nachdem eine Richtlinie im Modus **Alle Festplatten verschlüsseln** übernommen wurde.

12. Wählen Sie eine Methode für die Freigabe von Festplatten, die mithilfe von BitLocker verschlüsselt sind:

    - Wenn Sie zur Speicherung von Chiffrierschlüsseln ein Trusted Platform Module (TPM) verwenden möchten, wählen Sie die Variante **Trusted Platform Module (TPM) verwenden**.
    - Wenn Sie das Trusted Platform Module (TPM) nicht für die vollständige Festplattenverschlüsselung verwenden, wählen Sie die Variante **Kennwort verwenden** und geben Sie im Feld **Mindestlänge des Kennworts** an, wie viele Zeichen das Kennwort mindestens enthalten muss.

    Für die Betriebssysteme Windows 7 und Windows 2008 R2 sowie für ältere Versionen ist das Vorhandensein eines Trusted Platform Module (TPM) obligatorisch.

13. Wenn Sie beim vorherigen Schritt die Variante **Trusted Platform Module (TPM) verwenden** gewählt haben, gehen Sie wie folgt vor:

    - Wenn Sie einen PIN-Code festlegen möchten, nach dem der Benutzer gefragt wird, wenn er versucht, auf einen Chiffrierschlüssel zuzugreifen, aktivieren Sie das Kontrollkästchen **PIN-Code verwenden** und geben Sie im Feld **Mindestlänge des PIN-Codes** an, wie viele Ziffern der PIN-Code mindestens enthalten muss.

- Wenn Sie möchten, dass der Zugriff auf verschlüsselte Festplatten mithilfe eines Kennworts möglich ist, falls auf dem Computer kein Trusted Platform Module vorhanden ist, so aktivieren Sie das Kontrollkästchen **Kennwort verwenden, wenn Trusted Platform Module (TPM) nicht verfügbar ist** und geben Sie im Feld **Mindestlänge des Kennworts** an, wie viele Zeichen das Kennwort mindestens enthalten muss.

  In dieser Situation erfolgt der Zugriff auf Chiffrierschlüssel mithilfe des festgelegten Kennworts auf die gleiche Weise, wie wenn das Kontrollkästchen **Kennwort verwenden** aktiviert ist.

  Wenn das Kontrollkästchen **Kennwort verwenden, wenn Trusted Platform Module (TPM) nicht verfügbar ist** deaktiviert ist und Trusted Platform Module nicht verfügbar ist, wird die vollständige Festplattenverschlüsselung nicht gestartet.

14. Klicken Sie auf **OK**, um die Änderungen zu speichern.

15. Wenden Sie die Richtlinie an.

    Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Nachdem die Richtlinie auf einem Client-Computer übernommen wurde, auf dem das Programm Kaspersky Endpoint Security installiert ist, erscheinen folgende Abfragen:

- Ist in der Richtlinie für Kaspersky Security Center die Verschlüsselung der Systemfestplatte vorgesehen, so bestehen zwei Möglichkeiten: Es erscheint entweder ein Abfragefenster für den PIN-Code, falls Trusted Platform Module verwendet wird, oder es erscheint ein Abfragefenster für die Preboot-Authentifizierung, falls TPM nicht vorhanden ist.

- Ist im Betriebssystem der FIPS-Kompatibilitätsmodus (Federal Information Processing Standard) aktiviert, so erscheint in den Betriebssystemen Windows 8 und in älteren Versionen ein Abfragefenster zur Verbindung eines USB-Gerätes für die Speicherung der Wiederherstellungsschlüsseldatei.

Besteht kein Zugriff auf die Chiffrierschlüssel, so kann der Benutzer beim Administrator des lokalen Unternehmensnetzwerks einen Wiederherstellungsschlüssel anfordern (falls der Wiederherstellungsschlüssel zuvor nicht auf einem USB-Gerät gespeichert wurde oder falls der Schlüssel verloren gegangen ist).

Liste mit Festplatten erstellen, die aus der Verschlüsselung ausgeschlossen werden sollen

Eine Ausnahmeliste für die Verschlüsselung kann nur für das Verfahren "Kaspersky-Festplattenverschlüsselung" erstellt werden.

Gehen Sie wie folgt vor, um eine Liste mit Festplatten zu erstellen, die aus der Verschlüsselung ausgeschlossen werden sollen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen jener Administrationsgruppe, für welche Sie eine Liste mit Festplatten erstellen möchten, die von der Verschlüsselung ausgeschlossen werden sollen.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Wählen Sie die gewünschte Richtlinie aus.

5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:

   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Vollständige Festplattenverschlüsselung**.

7. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Variante **Kaspersky-Festplattenverschlüsselung**.

   In der Tabelle **Folgende Festplatten nicht verschlüsseln** werden Einträge mit Festplatten angezeigt, die nicht vom Programm verschlüsselt werden. Wenn Sie noch keine Liste mit Festplatten für die Ausnahme aus der Verschlüsselung erstellt haben, ist diese Tabelle leer.

8. Gehen Sie wie folgt vor, um der Liste mit Festplatten neue Festplatten hinzuzufügen, die nicht vom Programm verschlüsselt werden sollen:

   a. Klicken Sie auf **Hinzufügen**.

      Das Fenster **Geräte aus der Liste für Kaspersky Security Center hinzufügen** wird geöffnet.

   b. Geben Sie im Fenster **Geräte aus der Liste für Kaspersky Security Center hinzufügen** Werte für die Einstellungen **Name**, **Computer**, **Datenträgertyp**, **Kaspersky-Festplattenverschlüsselung** an.

   c. Klicken Sie auf **Aktualisieren**.

   d. Aktivieren Sie in der Spalte **Name** die Kontrollkästchen in den Tabellenzeilen für jene Festplatten, die zur Liste der nicht zu verschlüsselnden Festplatten hinzugefügt werden sollen.

   e. Klicken Sie auf **OK**.

   Die ausgewählten Festplatten werden in der Tabelle **Folgende Festplatten nicht verschlüsseln** angezeigt.

9. Um Festplatten aus der Ausnahmetabelle zu löschen, wählen Sie in der Tabelle **Folgende Festplatten nicht verschlüsseln** eine oder mehrere Zeilen und klicken Sie auf **Löschen**.

   Um in der Tabelle mehrere Zeilen zu wählen, halten Sie die Taste **STRG** gedrückt.

10. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Entschlüsselung von Festplatten

Sie können Festplatten auch dann entschlüsseln, wenn keine aktuelle Lizenz vorliegt, welche die Datenverschlüsselung zulässt.

Gehen Sie folgendermaßen vor, um Festplatten zu entschlüsseln:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Entschlüsselung von Festplatten anpassen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Vollständige Festplattenverschlüsselung**.
7. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** das Verfahren, mit dem die Festplatten verschlüsselt wurden.
8. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Alle Festplatten entschlüsseln**, wenn Sie alle verschlüsselten Festplatten entschlüsseln möchten.
   - Fügen Sie in der Tabelle **Folgende Festplatten nicht verschlüsseln** alle verschlüsselten Festplatten hinzu, die Sie entschlüsseln möchten.

     Diese Variante ist nur für das Verschlüsselungsverfahren "Kaspersky-Festplattenverschlüsselung" verfügbar.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern.
10. Wenden Sie die Richtlinie an.

    Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Wenn der Benutzer während der Entschlüsselung von Festplatten, die mit dem Verfahren Kaspersky-Festplattenverschlüsselung verschlüsselt wurden, den Computer ausschaltet oder neu startet, wird der Authentifizierungsagent vor dem nächsten Start des Betriebssystems geladen. Nach der Authentifizierung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die Entschlüsselung der Festplatten fort.

Wechselt das Betriebssystem während der Entschlüsselung von Festplatten, die mit dem Verfahren Kaspersky-Festplattenverschlüsselung verschlüsselt wurden, in den Ruhezustand (hibernation mode), so wird der Authentifizierungsagent beim Beenden des Ruhezustandes geladen. Nach der Authentifizierung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die Entschlüsselung der Festplatten fort. Nach der Entschlüsselung der Festplatten ist der Ruhezustand erst wieder verfügbar, nachdem das Betriebssystem neu gestartet wurde.

Wechselt das Betriebssystem während der Festplattenentschlüsselung in den Energiesparmodus (sleep mode), so setzt Kaspersky Endpoint Security beim Beenden des Energiesparmodus die Festplattenentschlüsselung fort, ohne den Authentifizierungsagenten zu laden.

Verwendung des Authentifizierungsagenten

Sind die Systemfestplatten verschlüsselt, so wird vor dem Laden des Betriebssystems der Authentifizierungsagent geladen. Authentifizieren Sie sich mithilfe des Authentifizierungsagenten, damit die verschlüsselten Systemfestplatten freigegeben werden und das Betriebssystem hochgefahren wird.

Nach erfolgreicher Authentifizierung wird das Betriebssystem hochgefahren. Bei jedem nachfolgenden Neustart des Betriebssystems ist eine erneute Authentifizierung erforderlich.

In manchen Fällen kann der Benutzer den Authentifizierungsvorgang nicht abschließen. Eine Authentifizierung ist beispielsweise nicht möglich, wenn der Benutzer die Anmeldedaten des Authentifizierungsagenten-Benutzerkontos für den Token oder die Smartcard vergessen hat oder den Token oder die Smartcard verloren hat.

Hat der Benutzer die Anmeldedaten für den Authentifizierungsagenten oder das Kennwort des Tokens oder der Smartcard vergessen, so muss er sich für die Wiederherstellung an den Administrator des lokalen Unternehmensnetzwerks wenden.

Hat der Benutzer den Token oder die Smartcard verloren, so muss der Administrator die elektronische Zertifikatdatei des neuen Tokens oder der neuen Smartcard zum Befehl für das Erstellen des Authentifizierungsagenten-Benutzerkontos hinzufügen. Anschließend muss der Benutzer den Vorgang zur Freigabe von verschlüsselten Geräten oder zur Datenwiederherstellung auf verschlüsselten Geräten durchführen.

Verwendung eines Tokens oder einer Smartcard bei der Arbeit mit dem Authentifizierungsagenten

Bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten kann ein Token oder eine Smartcard verwendet werden. Dazu muss die Datei des elektronischen Zertifikats für den Token oder die Smartcard zu dem Befehl hinzugefügt werden, mit dem das Authentifizierungsagenten-Benutzerkonto erstellt wird.

Ein Token oder eine Smartcard kann nur verwendet werden, wenn die Festplatten des Computers mithilfe des AES256-Verschlüsselungsalgorithmus verschlüsselt sind. Sind die Festplatten des Computers mithilfe des AES56-Verschlüsselungsalgorithmus verschlüsselt, so kann dem Befehl keine elektronische Zertifikatdatei hinzugefügt werden.

Um die Datei des elektronischen Zertifikats für einen Token oder eine Smartcard zu dem Befehl hinzuzufügen, mit dem das Authentifizierungsagenten-Benutzerkonto erstellt wird, muss die Datei zuerst mithilfe des Zertifikatsverwaltungsprogramms eines Drittanbieters gespeichert werden.

Das Zertifikat für den Token oder die Smartcard muss folgende Eigenschaften besitzen:

- Das Zertifikat entspricht dem Standard X.509 und die Zertifikatsdatei besitzt die Codierung DER.

  Wenn das elektronische Zertifikat des Tokens oder der Smartcard diese Voraussetzung nicht erfüllt, lädt das Verwaltungs-Plug-in die Datei dieses Zertifikats nicht in den Befehl, mit dem das Authentifizierungsagenten-Benutzerkonto erstellt wird, und zeigt einen Fehler an.

- Der Parameter `KeyUsage`, der den Zweck des Zertifikats angibt, muss den Wert `keyEncipherment` oder `dataEncipherment` besitzen.

  Wenn das elektronische Zertifikat des Tokens oder der Smartcard diese Voraussetzung nicht erfüllt, lädt das Verwaltungs-Plug-in die Datei dieses Zertifikats in den Befehl, mit dem das Authentifizierungsagenten-Benutzerkonto erstellt wird, und zeigt eine Warnung an.

- Das Zertifikat enthält einen RSA-Schlüssel mit einer Mindestlänge von 1024 Bit.

  Wenn das elektronische Zertifikat des Tokens oder der Smartcard diese Voraussetzung nicht erfüllt, lädt das Verwaltungs-Plug-in die Datei dieses Zertifikats nicht in den Befehl, mit dem das Authentifizierungsagenten-Benutzerkonto erstellt wird, und zeigt einen Fehler an.

Hilfetexte für den Authentifizierungsagenten ändern

Bevor Sie die Hilfetexte für den Authentifizierungsagenten ändern, beachten Sie die Liste der Zeichen, die in der Preboot-Umgebung unterstützt werden.

Um die Hilfetexte für den Authentifizierungsagenten zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Hilfetexte für den Authentifizierungsagenten ändern möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Allgemeine Verschlüsselungseinstellungen**.

7. Klicken Sie im Block **Vorlagen** auf **Hilfe**.

   Das Fenster **Hilfetexte für den Authentifizierungsagenten** wird geöffnet.

8. Gehen Sie wie folgt vor:

   - Öffnen Sie die Registerkarte **Authentifizierung**, um den Hilfetext zu ändern, welcher im Fenster des Authentifizierungsagenten bei dem Schritt angezeigt wird, bei dem die Anmeldedaten eingegeben werden.
   - Öffnen Sie die Registerkarte **Kennwort ändern**, um den Hilfetext zu ändern, der im Fenster des Authentifizierungsagenten bei dem Schritt angezeigt wird, bei dem das Kennwort für ein Benutzerkonto für den Authentifizierungsagenten geändert wird.
   - Öffnen Sie die Registerkarte **Kennwort wiederherstellen**, um den Hilfetext zu ändern, der im Fenster des Authentifizierungsagenten bei dem Schritt angezeigt wird, bei dem das Kennwort für ein Benutzerkonto für den Authentifizierungsagenten wiederhergestellt wird.

9. Ändern Sie die Hilfetexte.

   Um den ursprünglichen Text wiederherzustellen, klicken Sie auf **Standard**.

   > Der Hilfetext kann maximal 16 Zeilen umfassen. Die maximale Zeilenlänge beträgt 64 Zeichen.

10. Klicken Sie auf **OK**.

11. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf die Schaltfläche **OK**, um die vorgenommenen Änderungen zu speichern.

Beschränkungen für die Zeichenunterstützung in Hilfetexten für den Authentifizierungsagenten

In der Preboot-Umgebung werden folgende Unicode-Zeichen unterstützt:

- Basis-Lateinisch (0000 - 007F)
- Lateinisch-1, Ergänzung (0080 - 00FF)
- Lateinisch, erweitert-A (0100 - 017F)
- Lateinisch, erweitert-B (0180 - 024F)
- Spacing Modifier Letters (02B0 - 02FF)
- Kombinierende diakritische Zeichen (0300 - 036F)
- Griechisch und Koptisch (0370 - 03FF)
- Kyrillisch (0400 - 04FF)
- Hebräisch (0590 - 05FF)

- Arabisch (0600 - 06FF)
- Lateinisch, weiterer Zusatz (1E00 - 1EFF)
- Allgemeine Interpunktion (2000 - 206F)
- Währungszeichen (20A0 - 20CF)
- Buchstabenähnliche Symbole (2100 - 214F)
- Geometrische Formen (25A0 - 25FF)
- Arabische Präsentationsformen-B (FE70 - FEFF)

Zeichen, die nicht in dieser Liste angegeben sind, werden in der Preboot-Umgebung nicht unterstützt. Es wird davon abgeraten, solche Zeichen in den Hilfetexten des Authentifizierungsagenten zu verwenden.

Protokollierungsstufe für den Authentifizierungsagenten wählen

Das Programm zeichnet folgende Informationen in einer Protokolldatei auf: Dienstinformationen über die Verwendung des Authentifizierungsagenten und Informationen über die Benutzeraktionen im Authentifizierungsagenten.

Um die Protokollierungsstufe für den Authentifizierungsagenten festzulegen, gehen Sie wie folgt vor:

1. Drücken Sie sofort nach dem Start des Computers, dessen Festplatten verschlüsselt sind, die Taste **F3**, um das Fenster mit den Einstellungen des Authentifizierungsagenten zu öffnen.
2. Wählen Sie im Konfigurationsfenster des Authentifizierungsagenten eine Protokollierungsstufe aus:
   - **Disable debug logging (default)**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei keine Informationen über die Ereignisse des Authentifizierungsagenten.
   - **Enable debug logging**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten.
   - **Enable verbose logging**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei detaillierte Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten.

     Für diese Stufe gilt ein höherer Genauigkeitsgrad als bei Auswahl der Stufe **Enable debug logging**. Durch die hohe Aufzeichnungsgenauigkeit kann das Laden des Authentifizierungsagenten und des Betriebssystems verlangsamt werden.

   - **Enable debug logging and select serial port**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei Informationen über die Verwendung des Authentifizierungsagenten und über

die Benutzeraktionen im Authentifizierungsagenten. Außerdem werden die Informationen über den COM-Port übertragen.

Ist der Computer, dessen Festplatten verschlüsselt sind, über den COM-Port mit einem anderen Computer verbunden, so können die Ereignisse des Authentifizierungsagenten mithilfe des anderen Computers verfolgt werden.

- **Enable verbose debug logging and select serial port**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei detaillierte Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten. Außerdem werden die Informationen über den COM-Port übertragen.

  > Für diese Stufe gilt ein höherer Genauigkeitsgrad als bei Auswahl der Stufe **Enable debug logging and select serial port**. Durch die hohe Aufzeichnungsgenauigkeit kann das Laden des Authentifizierungsagenten und des Betriebssystems verlangsamt werden.

Eine Protokolldatei des Authentifizierungsagenten wird dann aufgezeichnet, wenn auf dem Computer verschlüsselte Festplatten vorhanden sind oder wenn die vollständige Festplattenverschlüsselung ausgeführt wird.

Die Protokolldatei des Authentifizierungsagenten wird im Gegensatz zu anderen Protokolldateien für das Programm nicht an Kaspersky Lab übertragen. Falls erforderlich, können Sie die Protokolldatei des Authentifizierungsagenten selbst zur Analyse an Kaspersky Lab schicken.

Authentifizierungsagenten-Konten verwalten

Zur Verwaltung von Benutzerkonten des Authentifizierungsagenten können Sie die folgenden Tools von Kaspersky Security Center nutzen:

- Gruppenaufgabe zur Verwaltung von Benutzerkonten des Authentifizierungsagenten. Mithilfe dieser Aufgabe können Sie die Authentifizierungsagenten-Benutzerkonten für eine Gruppe von Client-Computern verwalten.
- Lokale Aufgabe **Verschlüsselung (Verwaltung von Konten)**. Mithilfe dieser Aufgabe können Sie die Authentifizierungsagenten-Benutzerkonten für einzelne Client-Computer verwalten.

Um die Einstellungen der Aufgabe zur Verwaltung von Authentifizierungsagenten-Benutzerkonten anzupassen, gehen Sie wie folgt vor:

1. Erstellen Sie (Lokale Aufgabe erstellen, Gruppenaufgabe erstellen) eine Aufgabe für die Verwaltung von Authentifizierungsagenten-Benutzerkonten.
2. Öffnen Sie den Abschnitt **Einstellungen** des Fensters **Eigenschaften: <Name der Aufgabe zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten>**.
3. Fügen Sie einen Befehl für das Erstellen von Benutzerkonten des Authentifizierungsagenten hinzu.
4. Fügen Sie einen Befehl für das Ändern von Benutzerkonten des Authentifizierungsagenten hinzu.
5. Fügen Sie einen Befehl zum Löschen von Benutzerkonten des Authentifizierungsagenten hinzu.

6. Ändern Sie erforderlichenfalls die hinzugefügten Befehle zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten. Wählen Sie dazu in der Tabelle **Steuerungsbefehle für die Benutzerkonten des Authentifizierungsagenten** einen Befehl aus und klicken Sie auf **Ändern**.

7. Löschen Sie erforderlichenfalls die hinzugefügten Befehle zur Verwaltung von Authentifizierungsagenten-Benutzerkonten. Wählen Sie dazu in der Tabelle **Steuerungsbefehle für die Benutzerkonten des Authentifizierungsagenten** einen oder mehrere Befehle aus und klicken Sie auf **Löschen**.

   Um in der Tabelle mehrere Zeilen zu wählen, halten Sie die Taste **STRG** gedrückt.

8. Klicken Sie im Eigenschaftenfenster der Aufgabe auf **OK**, um die vorgenommenen Änderungen zu speichern.

9. Starten Sie die Aufgabe.

Die Befehle zur Verwaltung von Authentifizierungsagenten-Benutzerkonten, die zur Aufgabe hinzugefügt wurden, werden ausgeführt.

Befehl zum Erstellen eines Benutzerkontos für den Authentifizierungsagenten hinzufügen

Um einen Befehl zum Erstellen eines Benutzerkontos für den Authentifizierungsagenten hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie den Abschnitt **Einstellungen** des Fensters **Eigenschaften: <Name der Aufgabe zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten>**.

2. Klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Befehl zum Hinzufügen eines Benutzerkontos**.

   Das Fenster **Benutzerkonto hinzufügen** wird geöffnet.

3. Geben Sie im Fenster **Benutzerkonto hinzufügen** im Feld **Windows-Benutzerkonto** den Namen des Microsoft-Windows-Benutzerkontos an, auf dessen Basis das Benutzerkonto für den Authentifizierungsagenten erstellt werden soll.

   Geben Sie dazu den Namen des Benutzerkontos manuell ein oder klicken Sie auf die Schaltfläche **Auswählen**.

4. Wenn Sie den Namen des Microsoft-Windows-Benutzerkontos manuell eingegeben haben, klicken Sie auf **Erlauben**, um die Sicherheits-ID (SID, Security Identifier) des Benutzerkontos zu ermitteln.

   Wenn Sie die Sicherheits-ID nicht mithilfe der Schaltfläche **Erlauben** ermitteln, wird sie ermittelt, wenn die Aufgabe auf dem Computer ausgeführt wird.

   Es ist sinnvoll, die Sicherheits-ID des Microsoft-Windows-Benutzerkontos dann zu ermitteln, wenn der Befehl zum Erstellen eines Authentifizierungsagenten-Benutzerkontos hinzugefügt wird. So kann überprüft werden, ob der manuell eingegebene Name des Microsoft-Windows-Benutzerkontos korrekt ist. Wenn das eingegebene Microsoft-Windows-Benutzerkonto nicht auf

dem Computer oder in einer vertrauenswürdigen Domäne vorhanden ist, für welche die lokale Aufgabe **Verschlüsselung (Benutzerkonten verwalten)** geändert wird, so wird die Aufgabe zur Verwaltung von Benutzerkonten des Authentifizierungsagenten mit einem Fehler abgeschlossen.

5. Aktivieren Sie das Kontrollkästchen **Vorhandenes Benutzerkonto ersetzen**, wenn Sie möchten, dass ein bereits für den Authentifizierungsagenten erstelltes Benutzerkonto mit demselben Namen durch das neu hinzugefügte Benutzerkonto ersetzt wird.

   Dieser Schritt ist verfügbar, wenn Sie den Befehl zum Erstellen eines Benutzerkontos für den Authentifizierungsagenten in den Eigenschaften einer Gruppenaufgabe zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten hinzufügen. Dieser Schritt ist nicht verfügbar, wenn Sie den Befehl zur Erstellung eines Kontos des Authentifizierungsagenten in den Eigenschaften der lokalen Aufgabe **Verschlüsselung (Verwaltung von Konten)** hinzufügen.

6. Geben Sie im Feld **Benutzername** den Namen des Benutzerkontos für den Authentifizierungsagenten ein, der zur Authentifizierung für den Zugriff auf verschlüsselte Festplatten dient.

7. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Kennwort erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten das Kennwort des Benutzerkontos für den Authentifizierungsagenten abfragt.

8. Wenn Sie beim vorherigen Schritt das Kontrollkästchen **Anmeldung mit Kennwort erlauben** aktiviert haben, gehen Sie wie folgt vor:

   a. Geben Sie im Feld **Kennwort** das Kennwort des Benutzerkontos für den Authentifizierungsagenten ein, das zur Authentifizierung für den Zugriff auf verschlüsselte Festplatten dient.

   b. Wiederholen Sie im Feld **Kennwort bestätigen** das Kennwort des Benutzerkontos für den Authentifizierungsagenten, das Sie beim vorherigen Schritt eingegeben haben.

   c. Führen Sie eine der folgenden Aktionen aus:

      - Wählen Sie die Variante **Kennwort bei der ersten Authentifizierung ändern** aus, wenn Sie möchten, dass das Programm einen Benutzer, der sich zum ersten Mal am in dem Befehl angegebenen Benutzerkonto anmeldet, zur Änderung des Kennworts auffordert.

      - Wählen Sie andernfalls die Variante **Keine Kennwortänderung verlangen**.

9. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Zertifikat erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten dazu auffordert, einen Token oder eine Smartcard mit dem Computer zu verbinden.

10. Wenn Sie beim vorherigen Schritt das Kontrollkästchen **Anmeldung mit Zertifikat erlauben** aktiviert haben, klicken Sie auf **Durchsuchen** und geben Sie im Fenster **Zertifikatdatei auswählen** das elektronische Zertifikat des Tokens oder der Smartcard an.

11. Geben Sie erforderlichenfalls im Feld **Beschreibung des Befehls** die Informationen des Benutzerkontos für den Authentifizierungsagenten ein, welche Sie für die Verwendung des Befehls benötigen.

12. Führen Sie eine der folgenden Aktionen aus:

    - Wählen Sie die Variante **Authentifizierung zulassen** aus, damit das Programm einem Benutzer, welcher bei dem im Befehl angegebenen Benutzerkonto angemeldet ist, den Zugriff auf die Anmeldung im Authentifizierungsagenten erlaubt.

    - Wählen Sie die Variante **Authentifizierung verbieten** aus, damit das Programm einem Benutzer, welcher bei dem im Befehl angegebenen Benutzerkonto angemeldet ist, den Zugriff auf die Anmeldung im Authentifizierungsagenten verbietet.

13. Klicken Sie im Fenster **Benutzerkonto hinzufügen** auf **OK**.

Befehl zum Ändern eines Benutzerkontos für den Authentifizierungsagenten hinzufügen

Um einen Befehl zum Ändern eines Benutzerkontos für den Authentifizierungsagenten hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Abschnitt **Einstellungen** des Fensters **Eigenschaften: <Name der Aufgabe zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten>** im Kontextmenü der Schaltfläche **Hinzufügen** den Punkt **Befehl zum Ändern eines Benutzerkontos** aus.

   Das Fenster **Benutzerkonto ändern** wird geöffnet.

2. Geben Sie im Fenster **Benutzerkonto ändern** im Feld **Windows-Benutzerkonto** den Namen des Microsoft-Windows-Benutzerkontos an, auf dessen Basis das zu ändernde Benutzerkonto für den Authentifizierungsagenten erstellt wurde. Geben Sie dazu den Namen des Benutzerkontos manuell ein oder klicken Sie auf die Schaltfläche **Auswählen**.

3. Wenn Sie den Namen des Microsoft-Windows-Benutzerkontos manuell eingegeben haben, klicken Sie auf **Erlauben**, um die Sicherheits-ID (SID, Security Identifier) des Benutzerkontos zu ermitteln.

   Wenn Sie die Sicherheits-ID nicht mithilfe der Schaltfläche **Erlauben** ermitteln, wird sie ermittelt, wenn die Aufgabe auf dem Computer ausgeführt wird.

   > Es ist sinnvoll, die Sicherheits-ID des Microsoft-Windows-Benutzerkontos dann zu ermitteln, wenn der Befehl zum Ändern eines Authentifizierungsagenten-Benutzerkontos hinzugefügt wird. So kann überprüft werden, ob der manuell eingegebene Name des Microsoft-Windows-Benutzerkontos korrekt ist. Wenn das eingegebene Microsoft-Windows-Benutzerkonto nicht existiert oder sich in einer nicht vertrauenswürdigen Domäne befindet, wird die Gruppenaufgabe zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten mit einem Fehler abgeschlossen.

4. Aktivieren Sie das Kontrollkästchen **Benutzername ändern** und geben Sie einen neuen Namen für das Benutzerkonto des Authentifizierungsagenten ein, damit Kaspersky Endpoint Security den Benutzernamen in den Namen aus dem darunter angebrachten Feld ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Microsoft-Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

5. Aktivieren Sie das Kontrollkästchen **Einstellungen für die Anmeldung mit Kennwort ändern**, um Zugriff auf die Einstellungen für die Anmeldung mit einem Kennwort zu erhalten.

6. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Kennwort erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten das Kennwort des Benutzerkontos für den Authentifizierungsagenten abfragt.

7. Wenn Sie beim vorherigen Schritt das Kontrollkästchen **Anmeldung mit Kennwort erlauben** aktiviert haben, gehen Sie wie folgt vor:

   a. Geben Sie im Feld **Kennwort** das neue Kennwort des Benutzerkontos für den Authentifizierungsagenten ein.

   b. Wiederholen Sie im Feld **Kennwort bestätigen** das Kennwort, das Sie beim vorherigen Schritt eingegeben haben.

8. Aktivieren Sie das Kontrollkästchen **Regel für die Kennwortänderung bei der Anmeldung im Authentifizierungsagenten ändern**, damit Kaspersky Endpoint Security den Wert für die Kennwortänderung in den darunter angegebenen Wert ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Microsoft-Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

9. Legen Sie einen Wert für die Kennwortänderung bei der Anmeldung über den Authentifizierungsagenten fest.

10. Aktivieren Sie das Kontrollkästchen **Einstellungen für die Anmeldung mit Zertifikat ändern**, um Zugriff auf die Einstellungen für die Anmeldung mit einem elektronischen Token- oder Smartcard-Zertifikat zu erhalten.

11. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Zertifikat erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten das Kennwort für einen angeschlossenen Token oder eine Smartcard abfragt.

12. Wenn Sie beim vorherigen Schritt das Kontrollkästchen **Anmeldung mit Zertifikat erlauben** aktiviert haben, klicken Sie auf **Durchsuchen** und geben Sie im Fenster **Zertifikatdatei auswählen** das elektronische Zertifikat des Tokens oder der Smartcard an.

13. Aktivieren Sie das Kontrollkästchen **Beschreibung des Befehls ändern** und ändern Sie die Beschreibung des Befehls, damit Kaspersky Endpoint Security die Beschreibung ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Microsoft-Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

14. Aktivieren Sie das Kontrollkästchen **Regel für den Zugriff auf die Anmeldung im Authentifizierungsagenten ändern**, damit Kaspersky Endpoint Security die Zugriffsregel für die Anmeldung über den Authentifizierungsagenten in die darunter angegebene Regel ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

15. Legen Sie eine Regel für den Zugriff auf die Authentifizierung im Authentifizierungsagenten fest.

16. Klicken Sie im Fenster **Benutzerkonto ändern** auf **OK**.

Befehl zum Löschen eines Benutzerkontos für den Authentifizierungsagenten hinzufügen

Um einen Befehl zum Löschen eines Authentifizierungsagenten-Benutzerkontos hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Abschnitt **Einstellungen** des Fensters **Eigenschaften: <Name der Aufgabe zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten>** im Kontextmenü der Schaltfläche **Hinzufügen** den Punkt **Befehl zum Löschen eines Benutzerkontos** aus.

   Das Fenster **Benutzerkonto löschen** wird geöffnet.

2. Geben Sie im Fenster **Benutzerkonto löschen** im Feld **Windows-Benutzerkonto** den Namen des Microsoft-Windows-Benutzerkontos an, auf dessen Basis das zu löschende Authentifizierungsagenten-Benutzerkonto erstellt wurde. Geben Sie dazu den Namen des Benutzerkontos manuell ein oder klicken Sie auf die Schaltfläche **Auswählen**.

3. Wenn Sie den Namen des Microsoft-Windows-Benutzerkontos manuell eingegeben haben, klicken Sie auf **Erlauben**, um die Sicherheits-ID (SID, Security Identifier) des Benutzerkontos zu ermitteln.

   Wenn Sie die Sicherheits-ID nicht mithilfe der Schaltfläche **Erlauben** ermitteln, wird sie ermittelt, wenn die Aufgabe auf dem Computer ausgeführt wird.

   > Es ist sinnvoll, die Sicherheits-ID des Microsoft-Windows-Benutzerkontos dann zu ermitteln, wenn der Befehl zum Löschen eines Authentifizierungsagenten-Benutzerkontos hinzugefügt wird. So kann überprüft werden, ob der manuell eingegebene Name des Microsoft-Windows-Benutzerkontos korrekt ist. Wenn das eingegebene Microsoft-Windows-Benutzerkonto nicht existiert oder sich in einer nicht vertrauenswürdigen Domäne befindet, wird die Gruppenaufgabe zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten mit einem Fehler abgeschlossen.

4. Klicken Sie im Fenster **Benutzerkonto löschen** auf **OK**.

Anmeldedaten des Authentifizierungsagenten wiederherstellen

> Diese Anleitung richtet sich an Benutzer von Client-Computern, auf denen das Programm Kaspersky Endpoint Security installiert ist.

Um den Benutzernamen und das Kennwort eines Authentifizierungsagenten-Benutzerkontos wiederherzustellen, gehen Sie wie folgt vor:

1. Auf einem Computer mit verschlüsselten Festplatten wird zuerst der Authentifizierungsagent geladen und danach das Betriebssystem. Klicken Sie auf der Benutzeroberfläche des Authentifizierungsagenten auf die Schaltfläche **Forgot your password**, um die Wiederherstellung des Namens und des Kennworts für das Authentifizierungsagenten-Benutzerkonto zu starten.

2. Folgen Sie den Anweisungen des Authentifizierungsagenten, um die Blöcke der Wiederherstellungsanfrage für den Namen und das Kennwort des Authentifizierungsagenten-Benutzerkontos anzufordern.

3. Diktieren Sie dem Administrator des lokalen Unternehmensnetzwerks den Inhalt der Anfrageblöcke und den Computernamen.

4. Geben Sie die Blöcke aus der Antwort auf die Wiederherstellungsanfrage für den Namen und das Kennwort des Authentifizierungsagenten-Benutzerkontos ein. Die Antwort wurde vom Administrator des lokalen Unternehmensnetzwerks erstellt und an Sie geschickt.

5. Geben Sie ein neues Kennwort für das Benutzerkonto des Authentifizierungsagenten ein und bestätigen Sie das Kennwort.

   Der Name des Authentifizierungsagenten-Benutzerkontos wird anhand der Blöcke aus der Antwort auf die Wiederherstellungsanfrage für den Benutzernamen und das Kennwort des Authentifizierungsagenten-Benutzerkontos ermittelt.

Nachdem das neue Kennwort für das Authentifizierungsagenten-Benutzerkonto eingegeben und bestätigt wurde, wird das Kennwort gespeichert und die verschlüsselten Festplatten werden freigegeben.

Antwort auf die Benutzeranfrage zur Wiederherstellung von Anmeldedaten für den Authentifizierungsagenten

Um eine Antwortblöcke für die Anfrage zur Wiederherstellung des Benutzernamens und des Kennworts für ein Authentifizierungsagenten-Benutzerkontos zu erstellen und an den Benutzer zu übermitteln, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der Computer des Benutzers gehört, der die Wiederherstellung des Benutzernamens und des Kennworts für das Authentifizierungsagenten-Benutzerkonto angefordert hat.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.

4. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, welcher die Wiederherstellung des Benutzernamens und des Kennworts für das Authentifizierungsagenten-Benutzerkonto angefordert hat, und öffnen Sie mit Rechtsklick das Kontextmenü.

5. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus** aus.

   Das Fenster **Freigabe im Offline-Modus** wird geöffnet.

6. Wählen Sie im Fenster **Freigabe im Offline-Modus** die Registerkarte **Authentifizierungsagent** aus.

7. Wählen Sie im Abschnitt **Verwendeter Verschlüsselungsalgorithmus** einen Typ für den Verschlüsselungsalgorithmus.

8. Wählen Sie in der Liste **Benutzerkonto** den Namen des Authentifizierungsagenten-Benutzerkontos, das für jenen Benutzer erstellt wurde, der die Wiederherstellung des Benutzernamens und Kennworts für das Authentifizierungsagenten-Benutzerkonto beantragt hat.

9. Wählen Sie in der Dropdown-Liste **Festplatte** die verschlüsselte Festplatte, auf welche der Zugriff wiederhergestellt werden soll.

10. Geben Sie im Abschnitt **Benutzeranfrage** die Anfrageblöcke ein, die der Benutzer diktiert hat.

Der Inhalt der Blöcke für die Antwort auf die Benutzeranfrage zur Wiederherstellung des Benutzernamens und des Kennworts für das Authentifizierungsagenten-Benutzerkonto wird im Feld **Zugriffsschlüssel** angezeigt.

11. Lesen Sie dem Benutzer den Inhalt der Antwortblöcke vor.

Informationen zur Datenverschlüsselung anzeigen

Dieser Abschnitt erklärt, wie Informationen über die Datenverschlüsselung angezeigt werden können.

Über die Varianten für den Verschlüsselungsstatus

Während der Verschlüsselung und Entschlüsselung von Daten erhält Kaspersky Security Center von Kaspersky Endpoint Security Informationen zum Status der Übernahme von Verschlüsselungseinstellungen auf den Client-Computern.

Für die Verschlüsselung sind folgende Statusvarianten möglich:

- *Es wurde keine Verschlüsselungsrichtlinie festgelegt*. Für den Computer wurde keine Verschlüsselungsrichtlinie für Kaspersky Security Center festgelegt.
- *Bei der Übernahme der Richtlinie*. Auf dem Computer wird die Verschlüsselung und/oder Entschlüsselung von Daten ausgeführt.
- *Fehler*. Bei der Verschlüsselung und/oder Entschlüsselung von Daten ist auf dem Computer ein Fehler aufgetreten.
- *Ein Neustart ist erforderlich*. Ein Neustart des Computers ist erforderlich, um die Verschlüsselung oder Entschlüsselung von Daten auf dem Computer zu initialisieren oder abzuschließen.
- *Entspricht der Richtlinie*. Die Datenverschlüsselung wurde auf dem Computer mit den Verschlüsselungseinstellungen ausgeführt, die der für diesen Computer übernommenen Richtlinie für Kaspersky Security Center entsprechen.
- *Vom Benutzer abgebrochen*. Der Benutzer hat den Vorgang für die Dateiverschlüsselung auf dem Wechseldatenträger nicht bestätigt.

Verschlüsselungsstatus anzeigen

Gehen Sie wie folgt vor, um die Verschlüsselungsstatus für die Daten des Computers anzuzeigen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Computer gehört.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.

   Auf der Registerkarte **Geräte** im Arbeitsbereich werden die Eigenschaften der Computer der gewählten Administrationsgruppe angezeigt.

4. Verschieben Sie auf der Registerkarte **Geräte** im Arbeitsbereich das Bildlauffeld ganz nach rechts.

5. Falls die Spalte **Verschlüsselungsstatus** nicht angezeigt wird, gehen Sie wie folgt vor:

    1. Öffnen Sie durch Rechtsklick das Kontextmenü für den Tabellenkopf.

    2. Wählen Sie im Kontextmenü in der Dropdown-Liste **Ansicht** den Punkt **Spalten hinzufügen oder löschen** aus.

       Das Fenster **Spalten hinzufügen oder löschen** wird geöffnet.

    3. Aktivieren Sie im Fenster **Spalten hinzufügen oder löschen** das Kontrollkästchen **Verschlüsselungsstatus**.

    4. Klicken Sie auf **OK**.

    In der Spalte **Verschlüsselungsstatus** werden die Statusvarianten für die Datenverschlüsselung auf den Computern der ausgewählten Administrationsgruppe angezeigt. Dieser Status beruht auf Informationen über die Verschlüsselung von Dateien auf den lokalen Computerlaufwerken und über die vollständige Festplattenverschlüsselung.

Verschlüsselungsstatistik in den Informationsbereichen von Kaspersky Security Center anzeigen

Gehen Sie wie folgt vor, um die Statusmeldungen zur Dateiverschlüsselung in den Informationsbereichen von Kaspersky Security Center anzuzeigen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver – <Name des Computers>**.

3. Wählen Sie im Arbeitsbereich, der sich rechts von der Verwaltungskonsole befindet, die Registerkarte **Statistik**.

4. Erstellen Sie eine neue Seite mit Informationsbereichen mit einer Statistik für die Datenverschlüsselung. Gehen Sie dazu folgendermaßen vor:

    a. Klicken Sie auf der Registerkarte **Statistik** auf **Ansicht einstellen**.

       Das Fenster **Eigenschaften: Statistik** wird geöffnet.

    b. Klicken Sie im Fenster **Eigenschaften: Statistik** auf **Hinzufügen**.

       Das Fenster **Eigenschaften: Neue Seite** wird geöffnet.

    c. Geben Sie im Abschnitt **Allgemein** des Fensters **Eigenschaften: Neue Seite** den Namen der Seite ein.

    d. Klicken Sie im Abschnitt **Informationsbereiche** auf **Hinzufügen**.

       Das Fenster **Neuer Informationsbereich** wird geöffnet.

    e. Wählen Sie im Fenster **Neuer Informationsbereich** in der Gruppe **Schutzstatus** das Element **Geräte verschlüsseln**.

f. Klicken Sie auf **OK**.

Das Fenster **Eigenschaften: Geräte verschlüsseln** wird geöffnet.

g. Ändern Sie bei Bedarf die Einstellungen des Informationsbereichs. Nutzen Sie dazu die Abschnitte **Ansicht** und **Geräte** im Fenster **Eigenschaften: Geräte verschlüsseln**.

h. Klicken Sie auf **OK**.

i. Wiederholen Sie die Punkte d – h dieser Anleitung. Wählen Sie dabei im Fenster **Neuer Informationsbereich** in der Gruppe **Schutzstatus** das Element **Wechseldatenträger verschlüsseln** aus.

Die hinzugefügten Informationsbereiche werden in der Liste **Informationsbereiche** im Fenster **Eigenschaften: Neue Seite** angezeigt.

j. Klicken Sie im Fenster **Eigenschaften: Neue Seite** auf **OK**.

Der Name der Seite mit Informationsbereichen, die während der vorhergehenden Schritte erstellt wurde, erscheint in der Liste **Seiten** im Fenster **Eigenschaften: Statistik**.

k. Klicken Sie im Fenster **Eigenschaften: Statistik** auf **Schließen**.

5. Öffnen Sie auf der Registerkarte **Statistik** die Seite, die bei den vorhergehenden Schritten der Anleitung erstellt wurde.

Es werden Informationsbereiche angezeigt, in denen Sie den Verschlüsselungsstatus von Computern und Wechseldatenträgern einsehen können.

Fehler anzeigen, die bei der Dateiverschlüsselung auf lokalen Computerlaufwerken auftreten

Um Fehler anzuzeigen, die bei der Dateiverschlüsselung auf lokalen Computerlaufwerken auftreten, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, in welcher sich der Computer befindet, für den Sie eine Fehlerliste für die Dateiverschlüsselung anzeigen möchten.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.

4. Markieren Sie den Computer auf der Registerkarte **Geräte** in der Liste und öffnen Sie durch Rechtsklick das Kontextmenü.

5. Führen Sie eine der folgenden Aktionen aus:

- Wählen Sie im Kontextmenü des Computers den Punkt **Schutz** aus.
- Wählen Sie im Kontextmenü des Computers den Punkt **Eigenschaften** aus. Wählen Sie im folgenden Fenster **Eigenschaften: <Computername>** den Abschnitt **Schutz** aus.

6. Öffnen Sie im Abschnitt **Schutz** im Fenster **Eigenschaften: <Name des Computers>** mit dem Link **Datenverschlüsselungsfehler anzeigen** das Fenster **Datenverschlüsselungsfehler**.

   In diesem Fenster werden Informationen über Fehler bei der Dateiverschlüsselung auf lokalen Laufwerken angezeigt. Wenn ein Fehler korrigiert wurde, löscht Kaspersky Security Center im Fenster **Fehler bei der Dateiverschlüsselung** die Informationen dazu.

Bericht über die Datenverschlüsselung anzeigen

Gehen Sie folgendermaßen vor, um einen Bericht über die Datenverschlüsselung anzuzeigen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte**.

3. Klicken Sie auf **Berichtsvorlage erstellen**.

   Der Assistent für das Erstellen einer Berichtsvorlage wird gestartet.

4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie im Fenster **Typ der Berichtsvorlage wählen** im Abschnitt **Andere** einen der folgenden Punkte:

   - **Bericht über den Verschlüsselungsstatus der verwalteten Geräte**
   - **Bericht über den Verschlüsselungsstatus von Massenspeichergeräten**
   - **Bericht über Fehler bei Dateiverschlüsselung**
   - **Bericht über das Blockieren des Zugriffs auf verschlüsselte Dateien**.

   Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.

5. Wählen Sie die Berichtsvorlage, die Sie bei den vorherigen Schritten der Anleitung erstellt haben.

6. Wählen Sie im Kontextmenü der Vorlage den Punkt **Bericht anzeigen** aus.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Mit verschlüsselten Dateien arbeiten, wenn die Dateiverschlüsselungsfunktion eingeschränkt ist

Wenn die Richtlinie für Kaspersky Security Center übernommen wird und anschließend eine Dateiverschlüsselung erfolgt, erhält Kaspersky Endpoint Security einen Chiffrierschlüssel, welcher für den direkten Zugriff auf die verschlüsselten Dateien erforderlich ist. Mithilfe eines Chiffrierschlüssels kann ein Benutzer direkten Zugriff auf verschlüsselte Dateien erhalten. Voraussetzung dafür ist, dass der Benutzer bei einem beliebigen Windows-Benutzerkonto angemeldet ist, das zum Zeitpunkt der Dateiverschlüsselung aktiv war. Damit Benutzer, die bei Windows-Benutzerkonten angemeldet sind, welche zum Zeitpunkt der Dateiverschlüsselung inaktiv waren, auf verschlüsselte Dateien zugreifen können, ist eine Verbindung mit Kaspersky Security Center erforderlich.

Verschlüsselte Dateien können in folgenden Fällen nicht verfügbar sein:

- Auf dem Benutzercomputer sind Chiffrierschlüssel vorhanden, es besteht aber keine Verbindung zu Kaspersky Security Center. Diese Verbindung ist für die Arbeit mit Chiffrierschlüsseln erforderlich. In diesem Fall muss der Benutzer den Zugriff auf die verschlüsselten Dateien beim Administrator des lokalen Unternehmensnetzwerks anfordern.

  Wenn keine Verbindung zu Kaspersky Security Center besteht, ist es erforderlich:

  - für den Zugriff auf verschlüsselte Dateien, die auf Computerfestplatten gespeichert sind, einen Zugriffsschlüssel anzufordern
  - für den Zugriff auf verschlüsselte Dateien, die auf Wechseldatenträgern gespeichert sind, für jeden Wechseldatenträger einen separaten Zugriffsschlüssel für die verschlüsselten Dateien anzufordern

- Die Verschlüsselungskomponenten wurden vom Benutzercomputer entfernt. In diesem Fall kann der Benutzer verschlüsselte Dateien auf lokalen Datenträgern und auf Wechseldatenträgern zwar öffnen, der Inhalt der Dateien wird aber in verschlüsselter Form angezeigt.

  Der Benutzer kann unter folgenden Bedingungen mit verschlüsselten Dateien arbeiten:

  - Die Dateien befinden sich in verschlüsselten Archiven, die auf einem Computer erstellt wurden, auf dem das Programm Kaspersky Endpoint Security installiert ist.
  - Die Dateien sind auf Wechseldatenträgern gespeichert, für welche die Arbeit im portablen Modus zugelassen ist.

Zugriff auf verschlüsselte Dateien bei fehlender Verbindung mit Kaspersky Security Center anfordern

Diese Anleitung richtet sich an Benutzer von Client-Computern, auf denen das Programm Kaspersky Endpoint Security installiert ist.

Um trotz fehlender Verbindung mit Kaspersky Security Center Zugriff auf verschlüsselte Dateien zu erhalten, gehen Sie wie folgt vor:

1. Rufen Sie die verschlüsselte Datei auf, auf die Sie Zugriff erhalten möchten.

   Besteht zum Zeitpunkt des Dateiaufrufs keine Verbindung zu Kaspersky Security Center, so erstellt Kaspersky Endpoint Security eine Zugriffsanfrage-Datei für alle verschlüsselten Dateien, die auf lokalen Laufwerken des Computers gespeichert sind. Voraussetzung ist, dass sich die von Ihnen aufgerufene Datei auf einem lokalen Laufwerk befindet. Kaspersky Endpoint Security erstellt eine Zugriffsanfrage-Datei für alle verschlüsselten Dateien, die auf einem Wechseldatenträger gespeichert sind. Voraussetzung ist, dass sich die von Ihnen aufgerufene Datei auf einem Wechseldatenträger befindet. Das Fenster **Dateizugriff wurde verweigert** wird geöffnet.

2. Senden Sie die Zugriffsanfrage-Datei für verschlüsselte Dateien an den Administrator des lokalen Unternehmensnetzwerks. Führen Sie dazu eine der folgenden Aktionen aus:

   - Klicken Sie auf **Per E-Mail senden**, um die erstellte Zugriffsanfrage-Datei für verschlüsselte Dateien per E-Mail an den Administrator des lokalen Unternehmensnetzwerks zu senden.

- Klicken Sie auf **Speichern**, um Zugriffsanfrage-Datei für verschlüsselte Dateien zu speichern und auf eine andere Weise an den Administrator des lokalen Unternehmensnetzwerks zu übermitteln.

3. Sie erhalten nun die Schlüsseldatei für den Zugriff auf verschlüsselte Dateien, die vom Administrator des lokalen Unternehmensnetzwerks erstellt und an Sie übergeben wurde.

4. Aktivieren Sie den Zugriffsschlüssel für verschlüsselte Dateien auf eine der folgenden Arten:

   - Markieren Sie in einem beliebigen Dateimanager die Zugriffsschlüsseldatei für verschlüsselte Dateien und öffnen Sie die Datei durch Doppelklick.

   - Gehen Sie wie folgt vor:

     a. Öffnen Sie das Hauptfenster von Kaspersky Endpoint Security.

     b. Klicken Sie auf die Schaltfläche .

     Das Fenster **Ereignisse** wird geöffnet.

     c. Wählen Sie die Registerkarte **Status des Zugriffs auf Dateien und Geräte**.

     Auf der Registerkarte sind alle Anfragen für den Zugriff auf verschlüsselte Dateien aufgelistet.

     d. Wählen Sie die Anfrage, für welche Sie eine Zugriffsschlüsseldatei für verschlüsselte Dateien erhalten haben.

     e. Klicken Sie auf die Schaltfläche **Durchsuchen**, um den erhaltenen Zugriffsschlüssel für verschlüsselte Dateien zu laden.

     Das standardmäßige Microsoft Windows-Fenster **Datei des Zugriffsschlüssels auswählen** wird geöffnet.

     f. Wählen Sie im Microsoft-Windows-Standardfenster **Zugriffsanfrage-Datei auswählen** die vom Administrator des lokalen Unternehmensnetzwerks stammende Datei mit der Erweiterung kesdr, deren Name mit dem Namen der ausgewählten Zugriffsanfrage-Datei für verschlüsselte Dateien übereinstimmt.

     g. Klicken Sie auf **Öffnen**.

     h. Klicken Sie im Fenster **Ereignisse** auf **OK**.

Kaspersky Endpoint Security gewährt nun Zugriff auf alle verschlüsselten Dateien, die auf den lokalen Computerlaufwerken gespeichert sind. Als Voraussetzung gilt, dass die Zugriffsanfrage-Datei für die verschlüsselten Dateien beim Aufruf einer Datei erstellt wurde, die sich auf einem lokalen Laufwerk befindet. Kaspersky Endpoint Security gewährt Zugriff auf alle verschlüsselten Dateien, die auf dem Wechseldatenträger gespeichert sind, wenn die Zugriffsanfrage-Datei für verschlüsselte Dateien beim Aufruf einer Datei erstellt wurde, die sich auf einem Wechseldatenträger befindet. Um Zugriff auf verschlüsselte Dateien zu erhalten, die sich auf anderen Wechseldatenträgern befinden, müssen separate Zugriffsschlüssel für diese Wechseldatenträger angefordert werden.

Freigabe von verschlüsselten Dateien bei fehlender Verbindung zu Kaspersky Security Center

Um einem Benutzer trotz fehlender Verbindung mit Kaspersky Security Center Zugriff auf verschlüsselte Dateien zu gewähren, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der Computer des Benutzers gehört, der die Zugriffsanfrage für verschlüsselte Dateien gestellt hat.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, von dem die Zugriffsanfrage für verschlüsselte Dateien stammt, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
5. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus** aus.

   Das Fenster **Freigabe im Offline-Modus** wird geöffnet.
6. Wählen Sie im Fenster **Freigabe im Offline-Modus** die Registerkarte **Verschlüsselung** aus.
7. Klicken Sie auf der Registerkarte **Verschlüsselung** auf **Durchsuchen**.

   Das standardmäßige Microsoft Windows-Fenster **Zugriffsanfrage-Datei auswählen** wird geöffnet.
8. Geben Sie im Fenster **Zugriffsanfrage-Datei auswählen** den Pfad der Zugriffsanfrage-Datei an, die Sie vom Benutzer erhalten haben, und klicken Sie auf die Schaltfläche **Öffnen**.

   Kaspersky Security Center erstellt eine Zugriffsschlüsseldatei für die verschlüsselten Dateien. Auf der Registerkarte **Verschlüsselung** werden Informationen zur Anfrage des Benutzers angezeigt.
9. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf die Schaltfläche **Per E-Mail senden**, um die erstellte Schlüsseldatei für den Zugriff auf verschlüsselte Dateien per E-Mail an den Benutzer zu senden.
   - Klicken Sie auf **Speichern**, um die Zugriffsschlüsseldatei für verschlüsselte Dateien zu speichern und sie auf eine andere Weise an den Benutzer zu übermitteln.

Meldungsvorlagen für den Zugriff auf verschlüsselte Dateien anpassen

Gehen Sie wie folgt vor, um Meldungsvorlagen für den Zugriff auf verschlüsselte Dateien anzupassen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Nachrichtenvorlagen für die Freigabe von verschlüsselten Dateien ändern möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die entsprechende Richtlinie.

5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:

   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

6. Wählen Sie im Abschnitt **Datenverschlüsselung** den Unterabschnitt **Allgemeine Verschlüsselungseinstellungen**.

7. Klicken Sie im Abschnitt **Vorlagen** auf **Vorlagen**.

   Das Fenster **Vorlagen** wird geöffnet.

8. Gehen Sie wie folgt vor:

   - Um die Vorlage für eine vom Benutzer gesendete Nachricht zu ändern, wählen Sie die Registerkarte **Nachricht vom Benutzer**. Wenn der Benutzer auf die verschlüsselte Datei zugreift, während sich auf dem Computer kein Zugriffsschlüssel für die verschlüsselten Dateien befindet, wird das Fenster **Zugriff auf die Datei verboten** geöffnet. Bei Klick auf **Per E-Mail senden** im Fenster **Dateizugriff wurde verweigert** wird automatisch eine vom Benutzer stammende Nachricht erstellt. Diese Nachricht wird zusammen mit der Anforderungsdatei für den Zugriff auf verschlüsselte Dateien an den Administrator des lokalen Unternehmensnetzwerks gesendet.
   - Um die Vorlage für eine vom Administrator gesendete Nachricht zu ändern, wählen Sie die Registerkarte **Nachricht vom Administrator**. Diese Nachricht wird durch Klick auf **Per E-Mail senden** im Fenster **Freigabe von verschlüsselten Dateien** automatisch erstellt und an den Benutzer zugestellt, nachdem ihm der Zugriff auf verschlüsselte Dateien gewährt wurde.

9. Ändern Sie die Meldungsvorlagen.

   Sie können die Schaltfläche **Standard** und die Dropdown-Liste **Variable** verwenden.

10. Klicken Sie auf **OK**.

11. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf die Schaltfläche **OK**, um die vorgenommenen Änderungen zu speichern.

Mit verschlüsselten Geräten arbeiten, wenn kein Zugriff besteht

Freigabe von verschlüsselten Geräten

In folgenden Fällen kann es erforderlich sein, dass der Benutzer den Zugriff auf verschlüsselte Geräte anfordert:

- Die Festplatte wurde auf einem anderen Computer verschlüsselt.
- Auf dem Computer ist kein Chiffrierschlüssel für das Gerät vorhanden (z. B. beim ersten Zugriff auf einen verschlüsselten Wechseldatenträger auf diesem Computer) und es besteht keine Verbindung zu Kaspersky Security Center.

  Nachdem der Benutzer den Zugriffsschlüssel für ein verschlüsseltes Gerät übernommen hat, speichert Kaspersky Endpoint Security den Chiffrierschlüssel auf diesem Benutzercomputer und gibt künftig den Zugriff auf dieses Gerät frei, auch wenn keine Verbindung zu Kaspersky Security Center besteht.

Die Freigabe von verschlüsselten Geräten kann wie folgt erfolgen:

1. Der Benutzer erstellt über die Benutzeroberfläche von Kaspersky Endpoint Security eine Zugriffsanfrage-Datei mit der Erweiterung kesdc und übermittelt die Datei an den Administrator des lokalen Unternehmensnetzwerks.

2. Der Administrator erstellt in der Verwaltungskonsole für Kaspersky Security Center eine Zugriffsschlüsseldatei mit der Erweiterung kesdr und übermittelt die Datei an den Benutzer.

3. Der Benutzer übernimmt den Zugriffsschlüssel.

Daten auf verschlüsselten Geräten wiederherstellen

Für die Arbeit mit verschlüsselten Geräten kann der Benutzer das Reparatur-Tool für verschlüsselte Geräte (im Folgenden "Reparatur-Tool") verwenden. Dies kann in folgenden Fällen erforderlich sein:

- Der Freigabevorgang mithilfe eines Zugriffsschlüssels ist fehlgeschlagen.

- Auf dem Computer mit dem verschlüsselten Gerät sind die Verschlüsselungskomponenten nicht installiert.

Die Daten, die erforderlich sind, um den Zugriff auf verschlüsselte Geräte mithilfe des Reparatur-Tools wiederherzustellen, befinden sich für einen bestimmten Zeitraum in unverschlüsselter Form im Arbeitsspeicher des Benutzercomputers. Um das Risiko eines unbefugten Zugriffs auf diese Daten zu reduzieren, wird empfohlen, den Wiederherstellungsvorgang nur auf vertrauenswürdigen Computern auszuführen.

Die Datenwiederherstellung auf verschlüsselten Geräten wird wie folgt ausgeführt:

1. Der Benutzer erstellt mithilfe des Reparatur-Tools eine Zugriffsanfrage-Datei mit der Erweiterung fdertc und übermittelt die Datei an den Administrator des lokalen Unternehmensnetzwerks.

2. Der Administrator erstellt in der Verwaltungskonsole für Kaspersky Security Center eine Zugriffsschlüsseldatei mit der Erweiterung fdertr und übermittelt die Datei an den Benutzer.

3. Der Benutzer übernimmt den Zugriffsschlüssel.

Für die Wiederherstellung von Daten auf verschlüsselten Systemfestplatten kann der Benutzer im Reparatur-Tool auch die Anmeldedaten für den Authentifizierungsagenten angeben. Sind die Metadaten des Authentifizierungsagenten-Benutzerkontos beschädigt, so muss der Benutzer die Wiederherstellung mithilfe einer Zugriffsanfrage-Datei ausführen.

Bevor Daten auf verschlüsselten Geräten wiederhergestellt werden, sollte entweder der betreffende Computer aus der Verschlüsselungsrichtlinie für Kaspersky Security Center entnommen werden oder die Verschlüsselung in den Einstellungen der Richtlinie für Kaspersky Security Center deaktiviert werden. Dadurch wird verhindert, dass das Gerät erneut verschlüsselt wird.

Freigabe von verschlüsselten Geräten über die Programmoberfläche

Diese Anleitung richtet sich an Benutzer von Client-Computern, auf denen das Programm Kaspersky Endpoint Security installiert ist.

Um über die Benutzeroberfläche Zugriff auf verschlüsselte Geräte zu erhalten, gehen Sie wie folgt vor:

1. Rufen Sie das verschlüsselte Gerät auf, auf das Sie Zugriff erhalten möchten.

   Das Fenster **Der Datenzugriff wurde verweigert** wird geöffnet.

2. Senden Sie die Zugriffsanfrage-Datei mit der Erweiterung kesdc für den Zugriff auf das verschlüsselte Gerät an den Administrator des lokalen Unternehmensnetzwerks. Führen Sie dazu eine der folgenden Aktionen aus:

   - Klicken Sie auf **Per E-Mail senden**, um die erstellte Zugriffsanfrage-Datei für das verschlüsselte Gerät per E-Mail an den Administrator des lokalen Unternehmensnetzwerks zu senden.
   - Klicken Sie auf **Speichern**, um die Zugriffsanfrage-Datei für das verschlüsselte Gerät zu speichern und auf eine andere Weise an den Administrator des lokalen Unternehmensnetzwerks zu übermitteln.

   Wenn Sie das Fenster **Der Datenzugriff wurde verweigert** schließen, ohne die Zugriffsanfrage-Datei gespeichert oder an den Administrator des lokalen Unternehmensnetzwerks gesendet zu haben, können Sie dies jederzeit im Fenster **Ereignisse** auf der Registerkarte **Status des Zugriffs auf Dateien und Geräte** tun. Um dieses Fenster zu öffnen, klicken Sie im Programmhauptfenster auf die Schaltfläche .

3. Fordern Sie eine Zugriffsschlüsseldatei für das verschlüsselte Gerät an und speichern Sie die Datei. Die Datei wird vom Administrator des lokalen Unternehmensnetzwerks erstellt und an Sie gesendet.

4. Übernehmen Sie den Zugriffsschlüssel für das verschlüsselte Gerät auf eine der folgenden Arten:

   - Suchen Sie in einem beliebigen Dateimanager die Zugriffsschlüsseldatei für das verschlüsselte Gerät und öffnen Sie die Datei durch Doppelklick.
   - Gehen Sie wie folgt vor:

     a. Öffnen Sie das Hauptfenster von Kaspersky Endpoint Security.

     b. Klicken Sie auf die Schaltfläche , um das Fenster **Ereignisse** zu öffnen.

     c. Wählen Sie die Registerkarte **Status des Zugriffs auf Dateien und Geräte**.

     Auf der Registerkarte wird eine Liste mit allen Anfragen für den Zugriff auf verschlüsselte Dateien und Geräte angezeigt.

d. Wählen Sie die Anfrage, für welche Sie eine Zugriffsschlüsseldatei für das verschlüsselte Gerät erhalten haben.

e. Klicken Sie auf die Schaltfläche **Durchsuchen**, um den erhaltenen Zugriffsschlüssel für das verschlüsselte Gerät zu laden.

Das standardmäßige Microsoft Windows-Fenster **Datei des Zugriffsschlüssels auswählen** wird geöffnet.

f. Wählen Sie im Microsoft-Windows-Standardfenster **Datei des Zugriffsschlüssels auswählen** die vom Administrator des lokalen Unternehmensnetzwerks stammende Datei mit der Erweiterung kesdr, deren Name mit dem Namen der entsprechenden Zugriffsanfrage-Datei für das verschlüsselte Gerät übereinstimmt.

g. Klicken Sie auf **Öffnen**.

h. Klicken Sie im Fenster **Status des Zugriffs auf Dateien und Geräte** auf **OK**.

Kaspersky Endpoint Security gibt das verschlüsselte Gerät frei.

Verschlüsselte Geräte für einen Benutzer freigeben

Um ein verschlüsseltes Gerät für einen Benutzer freizugeben, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der Computer des Benutzers gehört, der die Zugriffsanfrage für das verschlüsselte Gerät gestellt hat.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, von dem die Zugriffsanfrage für das verschlüsselte Gerät stammt, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
5. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus** aus.

   Das Fenster **Freigabe im Offline-Modus** wird geöffnet.
6. Wählen Sie im Fenster **Freigabe im Offline-Modus** die Registerkarte **Verschlüsselung** aus.
7. Klicken Sie auf der Registerkarte **Verschlüsselung** auf **Durchsuchen**.

   Das standardmäßige Microsoft Windows-Fenster **Zugriffsanfrage-Datei auswählen** wird geöffnet.
8. Geben Sie im Fenster **Zugriffsanfrage-Datei auswählen** den Pfad der Zugriffsanfrage-Datei mit der Erweiterung kesdc an, die Sie vom Benutzer erhalten haben.
9. Klicken Sie auf **Öffnen**.

   Kaspersky Security Center erstellt eine Schlüsseldatei für den Zugriff auf das verschlüsselte Gerät. Die Datei besitzt die Erweiterung kesdr. Auf der Registerkarte **Verschlüsselung** werden Informationen zur Anfrage des Benutzers angezeigt.

10. Führen Sie eine der folgenden Aktionen aus:

    - Klicken Sie auf die Schaltfläche **Per E-Mail senden**, um die erstellte Schlüsseldatei für den Zugriff auf das verschlüsselte Gerät per E-Mail an den Benutzer zu senden.
    - Klicken Sie auf **Speichern**, um die Zugriffsschlüsseldatei für das verschlüsselte Gerät zu speichern und sie auf eine andere Weise an den Benutzer zu übermitteln.

Wiederherstellungsschlüssel für Festplatten, die mithilfe von BitLocker verschlüsselt sind, an einen Benutzer übermitteln

Um den Wiederherstellungsschlüssel für eine Systemfestplatte, die mit BitLocker verschlüsselt ist, an den Benutzer zu übermitteln, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der Computer des Benutzers gehört, von dem die Zugriffsanfrage für den verschlüsselten Datenträger stammt.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Wählen Sie auf der Registerkarte **Geräte** den Computer des Benutzers, von dem die Zugriffsanfrage für den verschlüsselten Datenträger stammt.
5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Freigabe im Offline-Modus** aus.

   Das Fenster **Freigabe im Offline-Modus** wird geöffnet.
6. Wählen Sie im Fenster **Freigabe im Offline-Modus** die Registerkarte **Zugriff auf ein Systemlaufwerk mit BitLocker-Schutz** aus.
7. Fordern Sie beim Benutzer die ID des Wiederherstellungsschlüssels an, die im Eingabefenster für das BitLocker-Kennwort angegeben ist, und vergleichen Sie diese ID mit der ID im Feld **ID des Wiederherstellungsschlüssels**.

   > Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf das angegebene Systemlaufwerk wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.
8. Übermitteln Sie den Schlüssel, der im Feld **Wiederherstellungsschlüssel** angegeben ist, an den Benutzer.

Um den Wiederherstellungsschlüssel für eine Nicht-Systemfestplatte, die mit BitLocker verschlüsselt ist, an den Benutzer zu übermitteln, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Verschlüsselung und Datenschutz → Verschlüsselte Geräte**.

   Im Arbeitsbereich wird eine Liste mit verschlüsselten Geräten angezeigt.

3. Wählen Sie im Arbeitsbereich das verschlüsselte Gerät, auf welches der Zugriff wiederhergestellt werden soll.

4. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Zugriffsschlüssel für das angegebene verschlüsselte Gerät abrufen**.

   Das Fenster **Zugriffswiederherstellung für ein mithilfe von BitLocker verschlüsseltes Laufwerk** wird geöffnet.

5. Fordern Sie beim Benutzer die ID des Wiederherstellungsschlüssels an, die im Eingabefenster für das BitLocker-Kennwort angegeben ist, und vergleichen Sie diese ID mit der ID im Feld **ID des Wiederherstellungsschlüssels**.

   > Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf den angegebenen Datenträger wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.

6. Übermitteln Sie den Schlüssel, der im Feld **Wiederherstellungsschlüssel** angegeben ist, an den Benutzer.

Ausführbare Datei des Reparatur-Tools erstellen

> Diese Anleitung richtet sich an Benutzer von Client-Computern, auf denen das Programm Kaspersky Endpoint Security installiert ist.

Gehen Sie folgendermaßen vor, um eine ausführbare Datei des Wiederherstellungstools zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie auf die Schaltfläche **Support**, die sich links unten im Programmhauptfenster befindet, um das Fenster **Support** zu öffnen.

3. Klicken Sie im Fenster **Support** auf die Schaltfläche **Verschlüsseltes Gerät wiederherstellen**.

   Das Reparatur-Tool für verschlüsselte Geräte wird gestartet.

4. Klicken Sie im Fenster des Wiederherstellungstools auf **Autonomes Reparatur-Tool erstellen**.

   Das Fenster **Autonomes Reparatur-Tool erstellen** wird geöffnet.

5. Tippen Sie entweder im Feld **Speichern unter** den Pfad des Ordners ein, in dem die ausführbare Datei für das Reparatur-Tool gespeichert werden soll, oder verwenden Sie die Schaltfläche **Durchsuchen**.

6. Klicken Sie im Fenster **Autonomes Reparatur-Tool erstellen** auf **OK**.

Die ausführbare Datei des Wiederherstellungstools fdert.exe wird im angegebenen Ordner gespeichert.

Daten auf verschlüsselten Geräten mithilfe des Reparatur-Tools wiederherstellen

Diese Anleitung richtet sich an Benutzer von Client-Computern, auf denen das Programm Kaspersky Endpoint Security installiert ist.

Um den Zugriff auf ein verschlüsseltes Gerät mithilfe des Reparatur-Tools wiederherzustellen, gehen Sie wie folgt vor:

1. Starten Sie das Wiederherstellungstool auf eine der folgenden Weisen:

   - Klicken Sie im Programmhauptfenster von Kaspersky Endpoint Security auf die Schaltfläche **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf **Verschlüsseltes Gerät wiederherstellen**.

   - Starten Sie die ausführbare Datei des Wiederherstellungstools fdert.exe, die mit dem Programm Kaspersky Endpoint Security erstellt wurde.

2. Wählen Sie im Fenster des Wiederherstellungstools in der Dropdown-Liste **Gerät auswählen** das verschlüsselte Gerät, zu dem Sie den Zugriff wiederherstellen möchten.

3. Klicken Sie auf die Schaltfläche **Diagnose**, damit das Tool feststellen kann, welche Aktion mit dem verschlüsselten Gerät ausgeführt werden soll: entsperren oder entschlüsseln.

   Ist die Verschlüsselungsfunktionalität von Kaspersky Endpoint Security auf dem Computer verfügbar, so bietet das Reparatur-Tool an, das Gerät zu entsperren. Beim Entsperren wird das Gerät nicht entschlüsselt, es wird aber der direkte Zugriff freigegeben. Ist die Verschlüsselungsfunktionalität von Kaspersky Endpoint Security auf dem Computer nicht verfügbar, so bietet das Reparatur-Tool an, das Gerät zu entschlüsseln.

4. Klicken Sie auf **MBR reparieren**, wenn bei der Diagnose einer verschlüsselten Systemfestplatte Probleme gemeldet wurden, die mit dem Master Boot Record (MBR) des Geräts zusammenhängen.

   Eine Reparatur des Master Boot Records des Geräts kann den Empfang von Informationen beschleunigen, die für das Entsperren und die Entschlüsselung des Geräts benötigt werden.

5. Klicken Sie abhängig von den Ergebnissen der Diagnose auf **Entsperren** oder **Entschlüsseln**.

   Das Fenster **Einstellungen der Geräteentsperrung** oder **Entschlüsselungseinstellungen für das Gerät** wird geöffnet.

6. Um Daten mithilfe des Authentifizierungsagenten-Benutzerkontos wiederherzustellen, gehen Sie wie folgt vor:

   a. Wählen Sie die Variante **Einstellungen des Benutzerkontos für den Authentifizierungsagenten verwenden**.

b. Geben Sie in den Feldern **Name** und **Kennwort** die Anmeldedaten für den Authentifizierungsagenten an.

Diese Methode ist nur bei der Wiederherstellung von Daten auf einer Systemfestplatte möglich. Wurde die Systemfestplatte beschädigt und die Daten über das Authentifizierungsagenten-Benutzerkonto sind verloren gegangen, so muss für die Wiederherstellung von Daten auf einem verschlüsselten Gerät beim Administrator des lokalen Unternehmensnetzwerks ein Zugriffsschlüssel angefordert werden.

7. Um die Daten mithilfe eines Zugriffsschlüssels wiederherzustellen, gehen Sie wie folgt vor:

   a. Wählen Sie die Variante **Zugriffsschlüssel für das Gerät manuell angeben**.

   b. Klicken Sie auf die Schaltfläche **Zugriffsschlüssel anfordern**.

   c. Das Fenster **Zugriffsschlüssel für das Gerät anfordern** wird geöffnet.

   d. Klicken Sie auf **Speichern** und wählen Sie einen Ordner, um die Zugriffsanfrage-Datei mit der Erweiterung fdertc zu speichern.

   e. Senden Sie die Zugriffsanfrage-Datei an den Administrator des lokalen Unternehmensnetzwerks.

   Schließen Sie das Fenster **Zugriffsschlüssel für das Gerät anfordern** nicht, bevor Sie einen Zugriffsschlüssel erhalten haben. Wenn dieses Fenster erneut geöffnet wird, kann der zuvor vom Administrator erstellte Zugriffsschlüssel nicht mehr verwendet werden.

   f. Fordern Sie eine Zugriffsschlüsseldatei an und speichern Sie die Datei. Die Datei wird vom Administrator des lokalen Unternehmensnetzwerks erstellt und an Sie gesendet.

   g. Klicken Sie auf **Laden** und wählen Sie im folgenden Fenster eine Zugriffsschlüsseldatei mit der Erweiterung fdertr.

8. Wenn Sie die Entschlüsselung eines Geräts ausführen, müssen Sie im Fenster **Entschlüsselungseinstellungen für das Gerät** auch die übrigen Entschlüsselungseinstellungen angeben. Gehen Sie dazu folgendermaßen vor:

   - Geben Sie einen Bereich für die Entschlüsselung an:
     - Wenn Sie das gesamte Gerät entschlüsseln möchten, wählen Sie die Variante **Ganzes Gerät entschlüsseln**.
     - Wenn Sie einen Teil der Daten auf dem Gerät entschlüsseln möchten, wählen Sie die Variante **Bestimmte Bereiche des Geräts entschlüsseln** und geben Sie mithilfe der Felder **Start** und **Ende** den Bereich für die Entschlüsselung an.
   - Legen Sie fest, wo die entschlüsselten Daten gespeichert werden sollen:
     - Damit die Daten auf dem ursprünglichen Gerät durch die entschlüsselten Daten überschrieben werden, deaktivieren Sie das Kontrollkästchen **Daten nach der Entschlüsselung in Datei speichern**.
     - Damit die entschlüsselten Daten getrennt von den verschlüsselten Quelldaten gespeichert werden, aktivieren Sie das Kontrollkästchen **Daten nach der Entschlüsselung in Datei**

speichern und geben Sie mithilfe der Schaltfläche **Durchsuchen** einen Zielpfad für die Daten an.

9. Klicken Sie auf **OK**.

Der Vorgang zum Entsperren und zur Entschlüsselung des Geräts wird gestartet.

Antwort auf die Benutzeranfrage zur Wiederherstellung von Daten auf verschlüsselten Geräten

Um eine Zugriffsschlüsseldatei für ein verschlüsseltes Gerät zu erstellen und an einen Benutzer zu übermitteln, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Verschlüsselung und Datenschutz → Verschlüsselte Geräte**.

3. Wählen Sie im Arbeitsbereich das verschlüsselte Gerät, für das Sie eine Zugriffsschlüsseldatei erstellen möchten, und wählen Sie im Kontextmenü des Geräts den Punkt **Zugriffsschlüssel für das angegebene verschlüsselte Gerät abrufen**.

   Wenn Sie nicht sicher sind, für welchen Computer die Zugriffsanfrage-Datei erstellt wurde, wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Verschlüsselung und Datenschutz** und klicken Sie im Arbeitsbereich auf den Link **Chiffrierschlüssel für das Gerät abrufen**.

   Das Fenster **Freigabe eines Geräts** wird geöffnet.

4. Wählen Sie den entsprechenden Verschlüsselungsalgorithmus. Wählen Sie dazu eine der folgenden Varianten:

   - **AES256**, wenn auf dem Computer, auf welchem das Gerät verschlüsselt wurde, das Programm Kaspersky Endpoint Security aus dem Programmpaket installiert wurde, das sich im Ordner aes256 befindet.

   - **AES56**, wenn auf dem Computer, auf welchem das Gerät verschlüsselt wurde, das Programm Kaspersky Endpoint Security aus dem Programmpaket installiert wurde, das sich im Ordner aes56 befindet.

5. Klicken Sie auf **Durchsuchen**.

   Das standardmäßige Microsoft Windows-Fenster **Zugriffsanfrage-Datei auswählen** wird geöffnet.

6. Geben Sie im Fenster **Zugriffsanfrage-Datei auswählen** den Pfad der Zugriffsanfrage-Datei mit der Erweiterung fdertc an, die Sie vom Benutzer erhalten haben.

7. Klicken Sie auf **Öffnen**.

Kaspersky Security Center erstellt eine Schlüsseldatei für den Zugriff auf das verschlüsselte Gerät. Die Datei besitzt die Erweiterung fdertr.

8. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf die Schaltfläche **Per E-Mail senden**, um die erstellte Schlüsseldatei für den Zugriff auf das verschlüsselte Gerät per E-Mail an den Benutzer zu senden.

   - Klicken Sie auf **Speichern**, um die Zugriffsschlüsseldatei für das verschlüsselte Gerät zu speichern und sie auf eine andere Weise an den Benutzer zu übermitteln.

Zugriff auf verschlüsselte Daten beim Ausfall des Betriebssystems wiederherstellen

Um bei einem Ausfall des Betriebssystems den Zugriff auf verschlüsselte Dateien und Wechseldatenträger wiederherzustellen, gehen Sie wie folgt vor:

1. Installieren Sie das Betriebssystem neu, ohne die Festplatte zu formatieren.

2. Installieren Sie Kaspersky Endpoint Security.

3. Stellen Sie eine Verbindung zwischen dem Computer und dem Administrationsserver für Kaspersky Security Center her, von welchem der Computer zum Zeitpunkt der Datenverschlüsselung verwaltet wurde (s. *Administratorhandbuch zu Kaspersky Security Center*).

Der Zugriff auf verschlüsselte Daten wird zu den gleichen Bedingungen gewährt wie vor dem Ausfall des Betriebssystems.

Notfall-CD erstellen

Die Notfall-CD kann eingesetzt werden, wenn ein Zugriff auf die verschlüsselte Systemfestplatte nicht möglich ist und sich das Betriebssystem nicht hochfahren lässt.

Sie können mithilfe der Notfall-CD ein Abbild des Windows-Betriebssystems laden und mithilfe des im Abbild enthaltenen Wiederherstellungstools den Zugriff auf die verschlüsselte Systemfestplatte wiederherstellen.

Gehen Sie folgendermaßen vor, um eine Notfall-CD zu erstellen:

1. Erstellen Sie eine ausführbare Datei für das Reparatur-Tool für verschlüsselte Geräte.

2. Erstellen Sie ein benutzerdefiniertes Windows PE-Abbild. Wenn Sie das benutzerdefinierte Windows PE-Abbild erstellen, fügen Sie dem Abbild die Datei des Reparatur-Tools für verschlüsselte Geräte hinzu.

3. Speichern Sie das benutzerdefinierte Windows PE-Abbild auf einem bootfähigen Medium, beispielsweise auf einer CD oder einem Wechseldatenträger.

   Eine Anleitung zum Erstellen eines benutzerdefinierten Windows PE-Abbilds finden Sie in der Microsoft-Hilfe (beispielsweise bei Microsoft TechNet).

Endpoint Sensor

Die Einstellungen der Komponente Endpoint Sensor sind nur in der Verwaltungskonsole für Kaspersky Security Center verfügbar. Um die Komponente verwenden zu können, muss das Verwaltungs-Plug-in installiert werden.

Dieser Abschnitt informiert über Endpoint Sensor und erklärt, wie die Komponente aktiviert oder deaktiviert wird.

Über Endpoint Sensor

Endpoint Sensor ist eine Komponente von Kaspersky Anti Targeted Attack Platform. Diese Lösung dient der rechtzeitigen Erkennung von Bedrohungen wie beispielsweise gezielten Angriffen.

Die Komponente wird auf Client-Computern installiert. Die Komponente überwacht auf diesen Computern kontinuierlich Prozesse, offene Netzwerkverbindungen und Dateiänderungen, und leitet diese Informationen an Kaspersky Anti Targeted Attack Platform weiter.

Die Funktionalität der Komponente ist für die folgenden Betriebssysteme verfügbar:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition
- Microsoft Windows Server 2016

Weitere Informationen zu Kaspersky Anti Targeted Attack Platform, welche nicht in dieser Hilfe enthalten sind, finden Sie in der Hilfe zu Kaspersky Anti Targeted Attack Platform.

Auf den Computern, auf denen die Komponente Endpoint Sensor installiert ist, muss eine direkte eingehende Verbindung ohne Proxyserver mit dem Server für Kaspersky Anti Targeted Attack Platform erlaubt sein.

Komponente Endpoint Sensor aktivieren und deaktivieren

Um die Komponente Endpoint Sensor zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Richtlinieneinstellungen ändern möchten.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.
6. Wählen Sie den Abschnitt **Endpoint Sensor**.
7. Führen Sie eine der folgenden Aktionen aus:
   - Um Endpoint Sensor einzuschalten, aktivieren Sie das Kontrollkästchen **Endpoint Sensor**.
   - Um Endpoint Sensor auszuschalten, deaktivieren Sie das Kontrollkästchen **Endpoint Sensor**.
8. Wenn Sie beim vorherigen Schritt das Kontrollkästchen aktiviert haben, gehen Sie wie folgt vor:
   a. Geben Sie im Feld **Serveradresse** die Adresse des Servers für Kaspersky Anti Targeted Attack Platform an. Die Serveradresse besteht aus:
      1. Name des Protokolls
      2. IP-Adresse oder vollständiger Domänenname (FQDN) des Servers
      3. Pfad der Windows-Ereignissammlung auf dem Server
   b. Geben Sie im Feld **Port** die Nummer des Ports an, der für die Verbindung mit dem Server für Kaspersky Anti Targeted Attack Platform verwendet wird.
9. Klicken Sie auf **OK**.
10. Wenden Sie die Richtlinie an.

    Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Update der Datenbanken und Programm-Module

Dieser Abschnitt informiert über das Update der Datenbanken und Programm-Module (im Folgenden "Update") und erklärt die Einstellungen für das Update.

Über das Update der Datenbanken und Programm-Module

Das Update der Datenbanken und Programm-Module von Kaspersky Endpoint Security gewährleistet die Aktualität des Computerschutzes. Jeden Tag tauchen neue Viren und andere Schadprogramme auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken

von Kaspersky Endpoint Security enthalten. Damit neue Bedrohungen rechtzeitig erkannt werden können, müssen Sie die Datenbanken und Programm-Module regelmäßig aktualisieren.

Für ein regelmäßiges Update ist eine aktuelle Programmlizenz erforderlich. Ohne Lizenz können Sie das Programm nur ein Mal aktualisieren.

Als primäre Update-Quelle für Kaspersky Endpoint Security dienen die Update-Server von Kaspersky Lab.

Der Computer muss mit dem Internet verbunden sein, um das Update-Paket erfolgreich von den Kaspersky-Lab-Update-Servern herunterzuladen. Standardmäßig wird die Internetverbindung automatisch ermittelt. Wenn Sie einen Proxyserver verwenden, müssen die Proxyserver-Einstellungen angepasst werden.

Bei einer Aktualisierung werden folgende Objekte auf Ihren Computer heruntergeladen und darauf installiert:

- Datenbanken für Kaspersky Endpoint Security. Der Computerschutz basiert auf Datenbanken, die Signaturen für Viren und andere bedrohliche Programme, sowie Informationen über entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese Informationen bei der Suche nach und der Desinfektion von infizierten Dateien auf dem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird empfohlen, die Datenbanken regelmäßig zu aktualisieren.

  Gemeinsam mit den Datenbanken von Kaspersky Endpoint Security werden auch die Netzwerktreiber aktualisiert, die gewährleisten, dass die Schutzkomponenten den Netzwerkverkehr abfangen können.

- Programm-Module. Neben den Datenbanken von Kaspersky Endpoint Security können auch die Programm-Module aktualisiert werden. Updates für Programm-Module beheben Schwachstellen von Kaspersky Endpoint Security, fügen neue Funktionen hinzu und optimieren vorhandene Funktionen.

Bei der Aktualisierung werden die auf Ihrem Computer installierten Programm-Module und Datenbanken mit der aktuellen Version verglichen, die in der Update-Quelle vorliegt. Sind die Datenbanken und Programm-Module nicht aktuell, werden fehlende Teile der Updates auf dem Computer installiert.

Beim Update der Programm-Module kann auch die Kontexthilfe für das Programm aktualisiert werden.

Sind die Datenbanken stark veraltet, kann das Update-Paket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehreren Dutzend Megabyte).

Informationen über den aktuellen Status der Datenbanken für Kaspersky Endpoint Security werden im Block **Update** im Fenster **Aufgaben** angezeigt.

Informationen über die Aktualisierungsergebnisse und über alle Ereignisse, die bei der Ausführung einer Update-Aufgabe auftreten, werden im Bericht von Kaspersky Endpoint Security protokolliert.

Über Update-Quellen

Eine *Update-Quelle* ist eine Ressource, die Updates der Datenbanken und der Programm-Module für Kaspersky Endpoint Security enthält.

Als Update-Quelle kann ein FTP- oder HTTP-Server (z. B. Kaspersky Security Center, Kaspersky-Lab-Update-Server), ein Netzwerkordner oder ein lokaler Ordner dienen.

Wenn Sie keinen Zugang zu den Kaspersky-Lab-Update-Servern besitzen (z. B. bei eingeschränktem Internetzugang), können Sie bei der Zentrale von Kaspersky Lab die Adressen der Kaspersky-Lab-Partner erfahren. Die Partner von Kaspersky Lab stellen Ihnen die Updates auf einem Wechseldatenträger zur Verfügung.

Wenn Sie Updates auf einem Wechseldatenträger bestellen, geben Sie bitte an, ob Sie auch Updates für die Programm-Module benötigen.

Update-Einstellungen konfigurieren

Zur Konfiguration des Updates stehen Ihnen die folgenden Aktionen zur Verfügung:

- Hinzufügen neuer Update-Quellen

  Standardmäßig enthält die Liste für Update-Quellen den Server von Kaspersky Security Center und die Kaspersky-Lab-Update-Server. Sie können der Liste weitere Update-Quellen hinzufügen. Als Update-Quellen können HTTP- oder FTP-Server oder gemeinsame Ordner angegeben werden.

  Wurden mehrere Ressourcen als Update-Quellen gewählt, greift Kaspersky Endpoint Security bei einer Aktualisierung streng der Reihe nach darauf zu. Bei der Update-Aufgabe wird das Update-Paket aus der ersten verfügbaren Update-Quelle verwendet.

  Wurde als Update-Quelle eine Ressource gewählt, die sich außerhalb des lokalen Firmennetzwerks befindet, ist für die Aktualisierung eine Internetverbindung erforderlich.

- Auswahl der Region des Kaspersky-Lab-Update-Servers

  Wenn Sie die Kaspersky-Lab-Server als Update-Quelle verwenden, können Sie einen Standort des Kaspersky-Lab-Update-Servers für den Update-Download wählen. Kaspersky Lab verfügt in mehreren Ländern der Erde über Update-Server. Durch die Nutzung des geografisch am nächsten gelegenen Kaspersky-Lab-Update-Servers kann der Download des Update-Pakets beschleunigt werden.

  Standardmäßig werden in den Update-Einstellungen die Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet.

- Anpassen des Updates für Kaspersky Endpoint Security aus einem gemeinsamen Ordner

  Um Internet-Datenverkehr einzusparen, können Sie festlegen, dass das Update von Kaspersky Endpoint Security auf den Computern des lokalen Netzwerks aus einem gemeinsamen Ordner erfolgen soll. Dazu lädt ein Computer des lokalen Firmennetzwerks das aktuelle Update-Paket vom Server für Kaspersky Security Center oder von den Kaspersky-Lab-Update-Servern herunter und kopiert das heruntergeladene Update-Paket in einen gemeinsamen Ordner. Anschließend können die übrigen Computer des lokalen Netzwerks das Update-Paket aus dem gemeinsamen Ordner herunterladen.

- Auswahl des Startmodus für die Update-Aufgabe

Ist der Start der Update-Aufgabe nicht möglich (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet ist), können Sie festlegen, dass der Start einer übersprungenen Update-Aufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt.

Sie können festlegen, dass der Start der Update-Aufgabe nach dem Start des Programms aufgeschoben wird. Dies ist möglich, wenn Sie für die Update-Aufgabe den Startmodus **Nach Zeitplan** gewählt haben und der Startzeitpunkt von Kaspersky Endpoint Security mit dem Startzeitplan der Update-Aufgabe übereinstimmt. Die Update-Aufgabe wird erst dann gestartet, wenn der vorgegebene Zeitraum nach dem Start von Kaspersky Endpoint Security verstrichen ist.

- Anpassen der Starts der Update-Aufgabe mit den Rechten eines anderen Benutzers

Update-Quelle hinzufügen

Gehen Sie folgendermaßen vor, um eine Update-Quelle hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Update**.

   Im rechten Fensterbereich werden die Einstellungen für das Update der Datenbanken und Programm-Module angezeigt.
3. Klicken Sie unter **Startmodus und Update-Quelle** auf **Update-Quelle**.

   Die Registerkarte **Quelle** des Fensters **Update** wird geöffnet.
4. Klicken Sie auf der Registerkarte **Quelle** auf **Hinzufügen**.

   Das Fenster **Update-Quelle wählen** wird geöffnet.
5. Wählen Sie im Fenster **Update-Quelle wählen** einen Ordner, der das Update-Paket enthält, oder geben Sie im Feld **Quelle** den vollständigen Pfad an.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Fenster **Update** auf **OK**.
8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Region des Update-Servers wählen

Um die Region des Update-Servers auswählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Update**.

   Im rechten Fensterbereich werden die Einstellungen für das Update der Datenbanken und Programm-Module angezeigt.
3. Klicken Sie unter **Startmodus und Update-Quelle** auf **Update-Quelle**.

Die Registerkarte **Quelle** des Fensters **Update** wird geöffnet.

4. Wählen Sie auf der Registerkarte **Quelle** unter **Regionale Einstellungen** die Option **Aus der Liste wählen**.
5. Wählen Sie in der Dropdown-Liste das Land, das am nächsten bei Ihrem Standort liegt.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Update aus dem gemeinsamen Ordner anpassen

Das Anpassen des Updates für Kaspersky Endpoint Security aus einem gemeinsamen Ordner umfasst folgende Etappen:

1. Kopieren des Update-Pakets in einen gemeinsamen Ordner auf einem Computer des lokalen Firmennetzwerks aktivieren
2. Update für Kaspersky Endpoint Security aus dem gemeinsamen Ordner auf den übrigen Computern des lokalen Firmennetzwerks anpassen

Gehen Sie folgendermaßen vor, um den Modus zur Verteilung des Update-Pakets aus einem gemeinsamen Ordner zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Update**.

   Im rechten Fensterbereich werden die Einstellungen für das Update der Datenbanken und Programm-Module angezeigt.
3. Aktivieren Sie im Abschnitt **Erweitert** das Kontrollkästchen **Updates in folgenden Ordner kopieren**.
4. Geben Sie den Pfad zum gemeinsamen Ordner an, in den das heruntergeladene Update-Paket kopiert werden soll. Dazu stehen folgende Methoden zur Verfügung:
   - Geben Sie den Pfad zum gemeinsamen Ordner im Feld an, das sich unter dem Kontrollkästchen **Updates in folgenden Ordner kopieren** befindet.
   - Klicken Sie auf **Durchsuchen**. Wählen Sie dann im folgenden Fenster **Ordner wählen** den entsprechenden Ordner und klicken Sie auf **OK**.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Um das Update für Kaspersky Endpoint Security aus einem gemeinsamen Ordner anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Update**.

Im rechten Fensterbereich werden die Einstellungen für das Update der Datenbanken und Programm-Module angezeigt.

3. Klicken Sie unter **Startmodus und Update-Quelle** auf **Update-Quelle**.

   Die Registerkarte **Quelle** des Fensters **Update** wird geöffnet.

4. Klicken Sie auf der Registerkarte **Quelle** auf **Hinzufügen**.

   Das Fenster **Update-Quelle wählen** wird geöffnet.

5. Wählen Sie im Fenster **Update-Quelle wählen** den gemeinsamen Ordner, in dem das Update-Paket gespeichert werden soll, oder geben Sie im Feld **Quelle** den vollständigen Pfad zum gemeinsamen Ordner an.

6. Klicken Sie auf **OK**.

7. Deaktivieren Sie auf der Registerkarte **Quelle** das Kontrollkästchen für die Update-Quellen, die nicht als gemeinsamer Ordner dienen sollen.

8. Klicken Sie auf **OK**.

9. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Startmodus für die Update-Aufgabe wählen

Um einen Startmodus für die Update-Aufgabe zu wählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Update**.

   Im rechten Fensterbereich werden die Einstellungen für das Update der Datenbanken und Programm-Module angezeigt.

3. Klicken Sie auf **Startmodus**.

   Die Registerkarte **Startmodus** des Fensters **Update** wird geöffnet.

4. Wählen Sie im Abschnitt **Startmodus** eine der folgenden Optionen für den Startmodus der Update-Aufgabe:

   - Wählen Sie die Option **Automatisch**, damit Kaspersky Endpoint Security beim Start der Update-Aufgabe berücksichtigt, ob an der Update-Quelle ein Update-Paket vorhanden ist. Die Häufigkeit, mit der Kaspersky Endpoint Security nach einem neuen Update-Paket sucht, kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken.

   - Wählen Sie die Option **Manuell**, wenn Sie die Update-Aufgabe manuell starten möchten.

   - Wählen Sie die Option **Nach Zeitplan**, um einen Startzeitplan für die Update-Aufgabe anzupassen.

5. Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie die Option **Automatisch** oder **Manuell** gewählt haben, gehen Sie weiter zu Punkt 6 dieser Anleitung.

- Wenn Sie die Option **Nach Zeitplan** gewählt haben, legen Sie einen Startzeitplan für die Update-Aufgabe fest. Gehen Sie dazu folgendermaßen vor:

  a. Legen Sie in der Dropdown-Liste **Frequenz** fest, wann die Update-Aufgabe gestartet werden soll. Wählen Sie eine der folgenden Varianten: **Minuten**, **Stunden**, **Tage**, **Jede Woche**, **Zum festgelegten Zeitpunkt**, **Jeden Monat**, **Nach dem Programmstart**.

  b. Passen Sie in Abhängigkeit von dem in der Dropdown-Liste **Frequenz** ausgewählten Element den genauen Zeitpunkt für den Start der Update-Aufgabe an.

  c. Geben Sie im Feld **Ausführung nach Programmstart aufschieben für** an, für welchen Zeitraum der Start der Update-Aufgabe nach dem Start von Kaspersky Endpoint Security aufgeschoben werden soll.

  > Wurde in der Dropdown-Liste **Frequenz** das Element **Nach dem Programmstart** gewählt, ist das Feld **Ausführung nach Programmstart aufschieben für** nicht verfügbar.

  d. Aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, damit Kaspersky Endpoint Security Update-Aufgaben, die nicht rechtzeitig gestartet werden konnten, so bald wie möglich ausführt.

  > Wurde in der Dropdown-Liste **Frequenz** das Element **Stunden**, **Minuten** oder **Nach dem Programmstart** gewählt, ist das Kontrollkästchen **Übersprungene Aufgaben starten** nicht verfügbar.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Update-Aufgabe mit den Rechten eines anderen Benutzers starten

Die Update-Aufgabe für Kaspersky Endpoint Security wird standardmäßig im Namen des Benutzers gestartet, mit dessen Rechten Sie sich im Betriebssystem angemeldet haben. Das Update für Kaspersky Endpoint Security kann aber auch aus einer Update-Quelle erfolgen, für welche der Benutzer keine Zugriffsrechte besitzt (z. B. aus einem gemeinsamen Ordner, welcher das Update-Paket enthält) oder für welche die Verwendung der Authentifizierung auf dem Proxyserver nicht angepasst ist. Sie können in den Einstellungen für Kaspersky Endpoint Security einen Benutzer angeben, der über die entsprechenden Rechte verfügt, und die Update-Aufgabe für Kaspersky Endpoint Security im Namen dieses Benutzers starten.

Gehen Sie folgendermaßen vor, um die Update-Aufgabe mit den Rechten eines anderen Benutzers zu starten:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Update**.

   Im rechten Fensterbereich werden die Einstellungen für das Update der Datenbanken und Programm-Module angezeigt.

3. Klicken Sie unter **Startmodus und Update-Quelle** auf **Startmodus**.

   Die Registerkarte **Startmodus** des Fensters **Update** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Startmodus** im Abschnitt **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des folgenden Benutzers**.

5. Tragen Sie im Feld **Name** den Benutzerkonto-Namen des Benutzers ein, dessen Rechte für den Zugriff auf die Update-Quelle verwendet werden sollen.

6. Tragen Sie im Feld **Kennwort** das Kennwort des Benutzers ein, dessen Rechte für den Zugriff auf die Update-Quelle verwendet werden sollen.

7. Klicken Sie auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Update für die Programm-Module anpassen

Um das Update für Programm-Module anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Update**.

   Im rechten Fensterbereich werden die Einstellungen für das Update der Datenbanken und Programm-Module angezeigt.

3. Führen Sie im Abschnitt **Erweitert** eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Updates für Programm-Module herunterladen**, wenn Sie möchten, dass das Programm die Updates für Programm-Module mit in Update-Pakete aufnimmt.

   - Andernfalls deaktivieren Sie das Kontrollkästchen **Updates für Programm-Module herunterladen**.

4. Wenn Sie beim vorherigen Schritt das Kontrollkästchen **Updates für Programm-Module herunterladen** aktiviert haben, geben Sie an, unter welchen Bedingungen das Programm die Updates für Programm-Module installieren soll.

   - Wählen Sie die Variante **Kritische und genehmigte Updates installieren**, wenn Sie möchten, dass das Programm kritische Updates für die Programm-Module automatisch und die restlichen Updates für die Programm-Module nach Genehmigung der Installation lokal über die Benutzeroberfläche des Programms oder mithilfe von Kaspersky Security Center installiert.

- Wählen Sie die Variante **Nur genehmigte Updates installieren**, wenn Sie möchten, dass das Programm Updates für die Programm-Module nur nach Genehmigung der Installation lokal über die Benutzeroberfläche des Programms oder mithilfe von Kaspersky Security Center installiert.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Update-Aufgabe starten und abbrechen

Eine Update-Aufgabe für Kaspersky Endpoint Security kann unabhängig vom gewählten Startmodus für die Update-Aufgabe jederzeit gestartet oder abgebrochen werden.

> Sie benötigen eine Internetverbindung, um ein Update-Paket von den Kaspersky-Lab-Update-Servern herunterzuladen.

Gehen Sie folgendermaßen vor, um die Update-Aufgabe zu starten oder zu beenden:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie auf die Schaltfläche **Aufgaben**, die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Aufgaben** wird geöffnet.

3. Wählen Sie mit der linken Maustaste den Block mit dem Namen der Update-Aufgabe.

   Der ausgewählte Block wird geöffnet.

4. Führen Sie eine der folgenden Aktionen aus:

   - Um die Update-Aufgabe zu starten, wählen Sie im Menü den Punkt **Start** aus.

     Der Status der Aufgabenausführung, der unter dem Namen der Update-Aufgabe angezeigt wird, ändert sich in *Wird ausgeführt*.

   - Um die Update-Aufgabe abzubrechen, wählen Sie im Menü den Punkt **Abbrechen** aus.

     Der Status der Aufgabenausführung, der unter dem Namen der Update-Aufgabe angezeigt wird, ändert sich in *Abgebrochen*.

Um von der einfachen Programmoberfläche aus eine Update-Aufgabe zu starten oder abzubrechen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.

2. Führen Sie im Kontextmenü in der Dropdown-Liste **Aufgaben** eine der folgenden Aktionen aus:

   - Wählen Sie eine nicht gestartete Update-Aufgabe aus, um sie zu starten.

   - Wählen Sie eine laufende Update-Aufgabe aus, um sie abzubrechen.

   - Wählen Sie eine angehaltene Update-Aufgabe aus, um sie erneut zu starten.

Rollback zum vorherigen Update

Nach dem ersten Update der Datenbanken und Programm-Module steht eine Rollback-Funktion zur Verfügung, mit der Sie zu den vorherigen Datenbanken und Programm-Modulen zurückkehren können.

Jedes Mal, wenn der Benutzer das Update startet, erstellt Kaspersky Endpoint Security zuerst eine Sicherungskopie der bisher verwendeten Datenbanken und Programm-Module und beginnt dann mit der Aktualisierung. Somit kann bei Bedarf zur Verwendung der vorherigen Datenbanken und Programm-Module zurückgekehrt werden. Die Rollback-Funktion für das letzte Update ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, die dazu führt, dass Kaspersky Endpoint Security ein harmloses Programm blockiert.

Gehen Sie folgendermaßen vor, um das letzte Update rückgängig zu machen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Aufgaben**, die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Aufgaben** wird geöffnet.
3. Wählen Sie mit der linken Maustaste den Block mit dem Namen der Aufgabe für das Update-Rollback.

   Der ausgewählte Block wird geöffnet.
4. Klicken Sie auf **Start**.

   Die Aufgabe für das Update-Rollback wird gestartet.

   Der Status der Aufgabenausführung, welcher unter dem Namen der Aufgabe für das Update-Rollback angezeigt wird, ändert sich in *Wird ausgeführt*.

Um von der einfachen Programmoberfläche aus eine Aufgabe zum Update-Rollback zu starten oder abzubrechen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Führen Sie im Kontextmenü in der Dropdown-Liste **Aufgaben** eine der folgenden Aktionen aus:
   - Wählen Sie eine nicht gestartete Aufgabe zum Update-Rollback aus, um sie zu starten.
   - Wählen Sie eine laufende Aufgabe zum Update-Rollback aus, um sie abzubrechen.
   - Wählen Sie eine angehaltene Aufgabe zum Update-Rollback aus, um sie erneut zu starten.

Verwendung des Proxyservers anpassen

Gehen Sie folgendermaßen vor, um die Proxyserver-Einstellungen anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Update**.

Im rechten Fensterbereich werden die Einstellungen für das Update der Datenbanken und Programm-Module angezeigt.

3. Klicken Sie unter **Proxyserver** auf **Einstellungen**.

   Das Fenster **Proxyserver-Einstellungen** wird geöffnet.

   > Sie können das Fenster **Proxyserver-Einstellungen** auch aus dem Unterabschnitt **Programmeinstellungen** des Abschnitts **Allgemeine Einstellungen** im Programmkonfigurationsfenster öffnen.

4. Aktivieren Sie im Fenster **Proxyserver-Einstellungen** das Kontrollkästchen **Proxyserver verwenden**.

5. Wählen Sie eine der folgenden Varianten aus, nach welcher die Adresse des Proxyservers ermittelt werden soll:

   - **Proxyserver-Einstellungen automatisch ermitteln**.

     Diese Variante gilt als Standard.

   - **Folgende Adresse und Port für den Proxyserver verwenden**.

6. Wenn Sie die Variante **Folgende Adresse und Port für den Proxyserver verwenden** ausgewählt haben, geben Sie in den Feldern **Adresse** und **Port** die entsprechenden Werte an.

7. Damit die Authentifizierung auf dem Proxyserver verwendet wird, aktivieren Sie das Kontrollkästchen **Benutzername und Kennwort für die Authentifizierung angeben** und geben Sie in folgenden Feldern die entsprechenden Werte an:

   - **Benutzername**.

     Eingabefeld für den Benutzernamen, der für die Authentifizierung auf dem Proxyserver dient.

   - **Kennwort**.

     Eingabefeld für das Benutzerkennwort, das für die Authentifizierung auf dem Proxyserver dient.

8. Damit der Proxyserver nicht verwendet wird, wenn Kaspersky Endpoint Security aus einem gemeinsamen Ordner aktualisiert wird, aktivieren Sie das Kontrollkästchen **Für lokale Adressen keinen Proxyserver verwenden**.

9. Klicken Sie auf **OK**.

10. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Untersuchung des Computers

Die Untersuchung auf Viren ist ein wichtiger Faktor für die Gewährleistung der Computersicherheit. Untersuchungen auf Viren sollten regelmäßig durchgeführt werden, um eine mögliche Ausbreitung von schädlichen Programmen auszuschließen, die von den Schutzkomponenten beispielsweise aufgrund einer zu niedrigen Schutzstufe nicht erkannt wurden.

Dieser Abschnitt informiert über die Besonderheiten und die Konfiguration von Untersuchungsaufgaben sowie über Sicherheitsstufen, Methoden und Technologien für die Untersuchung. Außerdem bietet er eine Anleitung für die Arbeit mit Dateien, die bei der Virenuntersuchung nicht von Kaspersky Endpoint Security verarbeitet worden sind.

Über die Untersuchungsaufgaben

Kaspersky Endpoint Security verfügt über folgende Aufgaben zur Suche nach Viren und anderen bedrohlichen Programmen, sowie zur Integritätsprüfung der Programm-Module:

- **Vollständige Untersuchung**. Ausführliche Untersuchung des Systems. Standardmäßig untersucht Kaspersky Endpoint Security folgende Objekte:
  - Arbeitsspeicher des Kerns
  - Objekte, die beim Hochfahren des Betriebssystems geladen werden
  - Bootsektoren
  - Backup des Betriebssystems
  - alle Festplatten und Wechseldatenträger
- **Untersuchung wichtiger Bereiche**. Kaspersky Endpoint Security untersucht standardmäßig den Kernel-Speicher, die laufenden Prozesse und die Bootsektoren.
- **Benutzerdefinierte Untersuchung**. Kaspersky Endpoint Security untersucht die vom Benutzer ausgewählten Objekte. Sie können ein beliebiges Objekt aus der folgenden Liste untersuchen:
  - Arbeitsspeicher des Kerns
  - Objekte, die beim Hochfahren des Betriebssystems geladen werden
  - Backup des Betriebssystems
  - E-Mail-Postfach von Outlook
  - alle Festplatten, Wechseldatenträger und Netzlaufwerke
  - eine beliebige ausgewählte Datei
- **Integritätsprüfung**. Kaspersky Endpoint Security überprüft, ob die Programm-Module Beschädigungen oder Änderungen aufweisen.

Die Aufgabe zur vollständigen Untersuchung und die Aufgabe zur Untersuchung wichtiger Bereiche sind spezifische Aufgaben. Der Untersuchungsbereich für diese Aufgaben sollte nicht geändert werden.

Nach dem Start von Untersuchungsaufgaben wird der Fortschritt der Untersuchung unter dem Namen der laufenden Untersuchungsaufgabe im Fenster **Aufgaben** angezeigt.

Informationen über die Untersuchungsergebnisse und über alle Ereignisse, die bei der Ausführung einer Untersuchungsaufgabe eintreten, werden im Bericht von Kaspersky Endpoint Security protokolliert.

Untersuchungsaufgabe starten und abbrechen

Unabhängig vom Startmodus kann eine Untersuchungsaufgabe jederzeit gestartet oder abgebrochen werden.

Gehen Sie folgendermaßen vor, um die Untersuchungsaufgabe zu starten oder zu beenden:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Aufgaben**, die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Aufgaben** wird geöffnet.
3. Wählen Sie mit der linken Maustaste den Block mit dem Namen der Untersuchungsaufgabe.

   Der ausgewählte Block wird geöffnet.
4. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Untersuchungsaufgabe starten möchten, klicken Sie auf **Start**.

     Der Status der Aufgabenausführung, der unter dem Namen der Untersuchungsaufgabe angezeigt wird, ändert sich in *Wird ausgeführt*.
   - Wenn Sie die Untersuchungsaufgabe abbrechen möchten, wählen Sie im Kontextmenü den Punkt **Abbrechen**.

     Der Status der Aufgabenausführung, der unter dem Namen der Untersuchungsaufgabe angezeigt wird, ändert sich in *Abgebrochen*.

Um von der einfachen Programmoberfläche aus eine Untersuchungsaufgabe zu starten oder abzubrechen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Führen Sie im Kontextmenü in der Dropdown-Liste **Aufgaben** eine der folgenden Aktionen aus:

   - Wählen Sie eine nicht gestartete Untersuchungsaufgabe aus, um sie zu starten.
   - Wählen Sie eine laufende Untersuchungsaufgabe aus, um sie abzubrechen.
   - Wählen Sie eine angehaltene Untersuchungsaufgabe aus, um sie erneut zu starten.

Untersuchungsaufgaben konfigurieren

Zur Konfiguration von Untersuchungsaufgaben stehen Ihnen folgende Aktionen zur Verfügung:

- Sicherheitsstufe ändern

Sie können eine der vordefinierten Sicherheitsstufen wählen oder die Einstellungen einer Sicherheitsstufe anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

- Ändern der Aktion, die Kaspersky Endpoint Security beim Fund einer infizierten Datei ausführen soll
- Festlegen des Untersuchungsbereichs

  Sie können den Untersuchungsbereich erweitern oder einschränken, indem Sie Untersuchungsobjekte hinzufügen oder entfernen, oder den Typ der zu untersuchenden Dateien ändern.

- Optimierung der Untersuchung

  Die Dateiuntersuchung lässt sich in folgender Hinsicht optimieren: Untersuchungsdauer verkürzen und Arbeitsgeschwindigkeit von Kaspersky Endpoint Security erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien. Außerdem können Sie die Untersuchungsdauer für eine einzelne Datei beschränken. Nach Ablauf des vorgegebenen Zeitraums schließt Kaspersky Endpoint Security eine Datei aus der laufenden Untersuchung aus (außer Archiven und Objekten, die aus mehreren Dateien bestehen).

  Außerdem können Sie die Verwendung der Technologien iChecker und iSwift aktivieren. Mit den Technologien iChecker und iSwift lässt sich die Dateiuntersuchung beschleunigen. Dabei werden Dateien von der Untersuchung ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

- Anpassen der Untersuchung von zusammengesetzten Dateien
- Untersuchungsmethoden anpassen

  Kaspersky Endpoint Security verwendet die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse. Bei der Signaturanalyse vergleicht Kaspersky Endpoint Security ein gefundenes Objekt mit den Einträgen in den Programm-Datenbanken. Aufgrund von Empfehlungen der Kaspersky-Lab-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.

  Sie können die heuristische Analyse verwenden, um den Schutz noch wirksamer zu gestalten. Bei der heuristischen Analyse analysiert Kaspersky Endpoint Security die Aktivität, die Objekte im Betriebssystem zeigen. Die heuristische Analyse kann neue schädliche Objekte erkennen, die noch nicht in den Datenbanken von Kaspersky Endpoint Security verzeichnet sind.

- Auswahl des Startmodus für Untersuchungsaufgaben

  Ist der Start der Untersuchungsaufgabe nicht möglich (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet ist), können Sie festlegen, dass der Start einer übersprungenen Untersuchungsaufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt.

  Sie können festlegen, dass der Start der Untersuchungsaufgabe nach dem Start des Programms aufgeschoben wird. Dies ist möglich, wenn Sie für die Untersuchungsaufgabe den Startmodus **Nach Zeitplan** gewählt haben und der Startzeitpunkt von Kaspersky Endpoint Security mit dem Startzeitplan der Untersuchungsaufgabe übereinstimmt. Die Untersuchungsaufgabe wird erst dann gestartet, wenn der vorgegebene Zeitraum nach dem Start von Kaspersky Endpoint Security verstrichen ist.

- Anpassen des Starts der Untersuchungsaufgabe mit den Rechten eines anderen Benutzers
- Anpassen der Untersuchung von Wechseldatenträgern beim Anschließen

Sicherheitsstufe ändern

Kaspersky Endpoint Security bietet unterschiedliche Einstellungsvarianten für die Ausführung von Untersuchungsaufgaben. Einstellungssätze, die im Programm gespeichert sind, heißen *Sicherheitsstufen*. Es gibt drei vordefinierte Sicherheitsstufen: **Hoch**, **Empfohlen**, **Niedrig**. Die Einstellungen der Sicherheitsstufe **Empfohlen** gelten als optimal. Sie werden von den Kaspersky-Lab-Experten angeraten.

Um die Sicherheitsstufe zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt der entsprechenden Untersuchungsaufgabe: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**.

   Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.

3. Führen Sie unter **Sicherheitsstufe** eine der folgenden Aktionen aus:

   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen (**Hoch**, **Empfohlen**, **Niedrig**), verwenden Sie den Schieberegler.

   - Wenn Sie die Sicherheitsstufe selbst anpassen möchten, klicken Sie auf **Einstellungen** und nehmen Sie im folgenden Fenster mit dem Namen der Untersuchungsaufgabe die entsprechenden Einstellungen vor.

     Nachdem Sie die Einstellungen einer Sicherheitsstufe geändert haben, ändert sich der Name der Sicherheitsstufe im Block **Sicherheitsstufe** in **Benutzerdefiniert**.

   - Wenn Sie die Sicherheitsstufe **Empfohlen** festlegen möchten, klicken Sie auf **Standard**.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktion für infizierte Dateien ändern

Beim Fund von infizierten Dateien versucht Kaspersky Endpoint Security standardmäßig, diese Dateien zu desinfizieren oder, falls eine Desinfektion nicht möglich ist, zu löschen.

Gehen Sie folgendermaßen vor, um die Aktion für infizierte Dateien zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt der entsprechenden Untersuchungsaufgabe aus: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche**, **Benutzerdefinierte Untersuchung** oder **Untersuchung aus dem Kontextmenü**.

   Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.

3. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** eine der folgenden Varianten aus:

   - Aktivieren Sie das Kontrollkästchen **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, damit Kaspersky Endpoint Security beim Fund von infizierten Dateien versucht, diese Dateien zu desinfizieren, oder diese Dateien löscht, falls eine Desinfektion nicht möglich ist.

- Aktivieren Sie das Kontrollkästchen **Desinfizieren. Informieren, wenn Desinfektion nicht möglich**, damit Kaspersky Endpoint Security beim Fund von infizierten Dateien versucht, diese Dateien zu desinfizieren, und Sie informiert, falls eine Desinfektion nicht möglich ist.

- Aktivieren Sie das Kontrollkästchen **Informieren**, damit Kaspersky Endpoint Security beim Fund von infizierten Dateien Sie darüber informiert.

Beim Fund von infizierten Dateien, die zu einer Anwendung aus dem Windows Store gehören, führt Kaspersky Endpoint Security die Aktion **Löschen** aus.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Liste der Untersuchungsobjekte erstellen

Um eine Liste mit Untersuchungsobjekten anzulegen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt der entsprechenden Untersuchungsaufgabe aus: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche**, **Benutzerdefinierte Untersuchung** oder **Untersuchung aus dem Kontextmenü**.

   Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.

3. Klicken Sie auf **Untersuchungsbereich**.

   Das Fenster **Untersuchungsbereich** wird geöffnet.

4. Um ein neues Objekt zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

   a. Klicken Sie auf **Hinzufügen**.

      Das Fenster **Untersuchungsbereich wählen** wird geöffnet.

   b. Wählen Sie ein Objekt und klicken Sie auf **Hinzufügen**.

      Alle Objekte, die im Fenster **Untersuchungsbereich wählen** markiert sind, werden in der Liste **Untersuchungsbereich** angezeigt.

   c. Klicken Sie auf **OK**.

5. Um den Pfad eines Objekts aus dem Untersuchungsbereich zu ändern, gehen Sie wie folgt vor:

   a. Wählen Sie das Objekt aus dem Untersuchungsbereich.

   b. Klicken Sie auf **Ändern**.

      Das Fenster **Untersuchungsbereich wählen** wird geöffnet.

   c. Geben Sie den neuen Pfad für das Objekt des Untersuchungsbereichs an.

d. Klicken Sie auf **OK**.

6. Um ein Objekt aus dem Untersuchungsbereich zu löschen, gehen Sie wie folgt vor:

   a. Wählen Sie das Objekt, das Sie aus dem Untersuchungsbereich löschen möchten.

      Um mehrere Objekte zu wählen, halten Sie die Taste **STRG** gedrückt.

   b. Klicken Sie auf **Löschen**.

      Ein Fenster zur Bestätigung des Löschvorgangs wird geöffnet.

   c. Bestätigen Sie das Löschen mit **Ja**.

   Objekte, die standardmäßig zum Untersuchungsbereich gehören, können nicht gelöscht oder geändert werden.

7. Um ein Objekt aus dem Untersuchungsbereich auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen im Fenster **Untersuchungsbereich**.

   Das Objekt verbleibt in der Liste der Objekte des Untersuchungsbereichs, wird aber bei der Untersuchungsaufgabe nicht gescannt.

8. Klicken Sie auf **OK**.

9. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Typ der zu untersuchenden Dateien wählen

Um einen Typ für die zu untersuchenden Dateien auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt der entsprechenden Untersuchungsaufgabe aus: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche**, **Benutzerdefinierte Untersuchung** oder **Untersuchung aus dem Kontextmenü**.

   Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.

3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster mit dem Namen der gewählten Untersuchungsaufgabe wird geöffnet.

4. Wählen Sie im Fenster mit dem Namen der gewählten Untersuchungsaufgabe die Registerkarte **Gültigkeitsbereich**.

5. Geben Sie unter **Dateitypen** den Typ der Dateien an, die von der gewählten Untersuchungsaufgabe untersucht werden sollen:

   - Wählen Sie **Alle Dateien**, wenn alle Dateien untersucht werden sollen.

- Wählen Sie **Dateien nach Format untersuchen**, wenn Dateien jener Formate untersucht werden sollen, die am häufigsten infiziert werden.

- Wählen Sie **Dateien nach Erweiterung untersuchen**, wenn Dateien mit solchen Erweiterungen untersucht werden sollen, die typisch für jene Dateien sind, die am häufigsten infiziert werden.

Bei der Auswahl des Typs für die zu untersuchenden Dateien sollte Folgendes beachtet werden:

- Für eine Reihe von Dateiformaten (z. B. TXT) ist das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung gering. Gleichzeitig gibt es Dateiformate, die ausführbaren Code enthalten (z. B. die Formate EXE und DLL) oder enthalten können (z. B. das Format DOC). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist hoch.

- Ein Angreifer kann einen Virus oder ein anderes bedrohliches Programm in einer ausführbaren Datei, deren Erweiterung in TXT geändert wurde, an Ihren Computer senden. Wenn Sie die Dateiuntersuchung nach Erweiterung festgelegt haben, überspringt das Programm eine solche Datei bei der Untersuchung. Wurde die Untersuchung von Dateien nach Format festgelegt, so analysiert die Komponente Schutz vor bedrohlichen Dateien die Kopfzeile der Datei unabhängig von deren Erweiterung. Falls sich ergibt, dass die Datei das Format EXE besitzt, so wird die Datei untersucht.

6. Klicken Sie im Fenster mit dem Namen der Untersuchungsaufgabe auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Dateiuntersuchung optimieren

Gehen Sie folgendermaßen vor, um die Untersuchung von Dateien zu optimieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt der entsprechenden Untersuchungsaufgabe aus: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche**, **Benutzerdefinierte Untersuchung** oder **Untersuchung aus dem Kontextmenü**.

   Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.

3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster mit dem Namen der gewählten Untersuchungsaufgabe wird geöffnet.

4. Wählen Sie im folgenden Fenster die Registerkarte **Gültigkeitsbereich**.

5. Führen Sie im Abschnitt **Untersuchung optimieren** folgende Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

   - Aktivieren Sie das Kontrollkästchen **Dateien überspringen, wenn Untersuchung länger dauert als** und geben Sie die Untersuchungsdauer für eine einzelne Datei an (in Sekunden).

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Untersuchung von zusammengesetzten Dateien

Eine häufig anzutreffende Methode zum Verstecken von Viren und anderen gefährlichen Programmen ist die Einbettung der Schädlinge in zusammengesetzte Dateien wie beispielsweise Archive oder Datenbanken. Eine zusammengesetzte Datei muss entpackt werden, um Viren und sonstige Schadprogramme aufzuspüren, die auf diese Weise versteckt wurden. Dadurch kann die Untersuchungsgeschwindigkeit sinken. Sie können die Typen der zusammengesetzten Dateien, die untersucht werden sollen, beschränken und dadurch die Untersuchungsgeschwindigkeit erhöhen.

Gehen Sie folgendermaßen vor, um die Untersuchung von zusammengesetzten Dateien anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt der entsprechenden Untersuchungsaufgabe: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**.

   Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.

3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster mit dem Namen der gewählten Untersuchungsaufgabe wird geöffnet.

4. Wählen Sie im folgenden Fenster die Registerkarte **Gültigkeitsbereich**.

5. Geben Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Installationspakete, Office-Format-Dateien, in Mail-Format-Dateien, kennwortgeschützte Archive.

6. Wenn im Abschnitt **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen** deaktiviert ist, klicken Sie auf den Link **alle / neue**, der sich neben dem Namen des Typs für die zusammengesetzten Datei befindet. Legen Sie dann fest, ob alle Dateien dieses Typs oder nur neue Dateien dieses Typs untersucht werden sollen.

   Der Link verändert seinen Wert, wenn er angeklickt wird.

   Ist das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen** aktiviert, werden nur neue Dateien untersucht.

7. Klicken Sie auf **Erweitert**.

   Das Fenster **Zusammengesetzte Dateien** wird geöffnet.

8. Führen Sie unter **Größenbeschränkung** eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und geben Sie im Feld **Maximale Dateigröße** einen entsprechenden Wert an, wenn umfangreiche zusammengesetzte Dateien nicht entpackt werden sollen.

   - Damit zusammengesetzte Dateien unabhängig von ihrer Größe entpackt werden, deaktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**.

Unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist, werden umfangreiche Dateien beim Extrahieren aus Archiven von Kaspersky Endpoint Security untersucht.

9. Klicken Sie auf **OK**.
10. Klicken Sie im Fenster mit dem Aufgabennamen auf **OK**.
11. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Untersuchungsmethoden verwenden

Gehen Sie folgendermaßen vor, um die Untersuchungsmethoden zu verwenden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt der entsprechenden Untersuchungsaufgabe aus: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche**, **Benutzerdefinierte Untersuchung** oder **Untersuchung aus dem Kontextmenü**.

   Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.
3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster mit dem Namen der gewählten Untersuchungsaufgabe wird geöffnet.
4. Wählen Sie im folgenden Fenster die Registerkarte **Erweitert**.
5. Aktivieren Sie im Abschnitt **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse**, damit das Programm während der Ausführung einer Untersuchungsaufgabe die heuristische Analyse einsetzt. Stellen Sie dann mit dem Schieberegler die Stufe der heuristischen Analyse ein: **oberflächlich**, **mittel** oder **tief**.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Untersuchungstechnologien verwenden

Gehen Sie folgendermaßen vor, um die Untersuchungstechnologien zu verwenden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt der entsprechenden Untersuchungsaufgabe aus: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche**, **Benutzerdefinierte Untersuchung** oder **Untersuchung aus dem Kontextmenü**.

Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.

3. Klicken Sie unter **Sicherheitsstufe** auf **Einstellungen**.

   Das Fenster mit dem Namen der gewählten Untersuchungsaufgabe wird geöffnet.

4. Wählen Sie im folgenden Fenster die Registerkarte **Erweitert**.

5. Aktivieren Sie im Abschnitt **Untersuchungstechnologien** die Kontrollkästchen für die Technologien, die bei der Untersuchung verwendet werden sollen.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Startmodus für eine Untersuchungsaufgabe wählen

Um einen Startmodus für die Untersuchungsaufgabe zu wählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt mit dem Namen der entsprechenden Aufgabe: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**.

   Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.

3. Klicken Sie auf **Startmodus**.

   Das Eigenschaftenfenster der gewählten Aufgabe wird auf der Registerkarte **Startmodus** geöffnet.

4. Wählen Sie im Abschnitt **Startmodus** einen Startmodus für die Aufgabe: **Manuell** oder **Nach Zeitplan**.

5. Wenn Sie die Variante **Nach Zeitplan** gewählt haben, geben Sie die Zeitplaneinstellungen an. Gehen Sie dazu folgendermaßen vor:

   a. Wählen Sie in der Dropdown-Liste **Frequenz** eine Frequenz für den Aufgabenstart (**Minuten**, **Stunden**, **Tage**, **Jede Woche**, **Zum festgelegten Zeitpunkt**, **Jeden Monat**, **Nach dem Programmstart**, **Nach jedem Update**).

   b. Passen Sie je nach gewählter Frequenz die erweiterten Einstellungen für den Startzeitplan der Aufgabe an.

   c. Aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, damit Kaspersky Endpoint Security Untersuchungsaufgaben, die nicht rechtzeitig gestartet werden konnten, so bald wie möglich ausführt.

      Ist in der Dropdown-Liste **Frequenz** das Element **Minuten**, **Stunden**, **Nach dem Programmstart** oder **Nach jedem Update** ausgewählt, so ist das Kontrollkästchen

Übersprungene Aufgaben starten nicht verfügbar.

a. Aktivieren Sie das Kontrollkästchen **Nur bei Computerleerlauf ausführen**, damit Kaspersky Endpoint Security die Aufgabe anhält, wenn die Computerressourcen ausgelastet sind.

Diese Zeitplanvariante erlaubt einen sparsamen Umgang mit der Rechnerleistung.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Start der Untersuchungsaufgabe mit den Rechten eines anderen Benutzers anpassen

Die Untersuchungsaufgabe wird standardmäßig mit den Rechten des Benutzerkontos gestartet, mit welchem der Benutzer im Betriebssystem angemeldet ist. Es kann aber erforderlich sein, eine Untersuchungsaufgabe mit den Rechten eines anderen Benutzers zu starten. Sie können in den Einstellungen der Untersuchungsaufgabe einen Benutzer angeben, der über die entsprechenden Rechte verfügt, und die Untersuchungsaufgabe im Namen dieses Benutzers starten.

Gehen Sie folgendermaßen vor, um den Start der Untersuchungsaufgabe mit den Rechten eines anderen Benutzers zu konfigurieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt mit dem Namen der entsprechenden Aufgabe: **Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**.

   Im rechten Fensterbereich werden die Einstellungen für die gewählte Untersuchungsaufgabe angezeigt.

3. Klicken Sie auf **Startmodus**.

   Das Eigenschaftenfenster der gewählten Aufgabe wird auf der Registerkarte **Startmodus** geöffnet.

4. Aktivieren Sie auf der Registerkarte **Startmodus** im Abschnitt **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des folgenden Benutzers**.

5. Tragen Sie im Feld **Name** den Namen des Benutzers ein, dessen Rechte für den Start der Untersuchungsaufgabe verwendet werden sollen.

6. Tragen Sie im Feld **Kennwort** das Kennwort des Benutzers ein, dessen Rechte für den Start der Untersuchungsaufgabe verwendet werden sollen.

7. Klicken Sie auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Wechseldatenträger beim Anschließen an den Computer untersuchen

Bestimmte schädliche Programme nutzen Schwachstellen des Betriebssystems aus, um sich über lokale Netzwerke und Wechseldatenträger auszubreiten. Kaspersky Endpoint Security bietet eine Funktion, mit der Wechseldatenträger auf Viren und andere Schadprogramme untersucht werden können, wenn sie an den Computer angeschlossen werden.

Um die Untersuchung von Wechseldatenträgern anzupassen, wenn diese mit dem Computer verbunden werden, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Untersuchung von Wechseldatenträgern**.

   Im rechten Fensterbereich werden die Einstellungen für die Untersuchung von Wechseldatenträgern angezeigt.

3. Wählen Sie in der Dropdown-Liste **Aktion beim Anschließen eines Wechseldatenträgers** die entsprechende Aktion aus:

   - **Nicht untersuchen**
   - **Genaue Untersuchung**.

     In diesem Modus untersucht Kaspersky Endpoint Security alle Dateien, die sich auf dem Wechseldatenträger befinden, einschließlich eingebetteter Dateien in zusammengesetzten Objekten.

   - **Schnelle Untersuchung**.

     In diesem Modus untersucht Kaspersky Endpoint Security nur infizierbare Dateien. Außerdem werden zusammengesetzte Objekte nicht entpackt.

4. Führen Sie eine der folgenden Aktionen aus:

   - Damit Kaspersky Endpoint Security nur Wechseldatenträger untersucht, deren Größe den festgelegten Wert nicht überschreitet, aktivieren Sie das Kontrollkästchen **Maximale Größe des Wechseldatenträgers** und geben Sie im nebenstehenden Feld einen Wert in Megabyte an.
   - Damit Kaspersky Endpoint Security alle Festplatten untersucht, deaktivieren Sie das Kontrollkästchen **Maximale Größe des Wechseldatenträgers**.

5. Führen Sie eine der folgenden Aktionen aus:

   - Damit Kaspersky Endpoint Security den Fortschritt der Untersuchung von Wechseldatenträgern in einem separaten Fenster anzeigt, aktivieren Sie das Kontrollkästchen **Untersuchungsfortschritt anzeigen**.
   - Damit Kaspersky Endpoint Security die Untersuchung von Wechseldatenträgern im Hintergrundmodus ausführt, deaktivieren Sie das Kontrollkästchen **Untersuchungsfortschritt anzeigen**.

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Arbeit mit aktiven Bedrohungen

Dieser Abschnitt enthält eine Anleitung zum Umgang mit infizierten Dateien, die bei der Untersuchung des Computers auf Viren und andere Schadprogramme nicht von Kaspersky Endpoint Security verarbeitet wurden.

Über aktive Bedrohungen

Kaspersky Endpoint Security protokolliert Informationen über Dateien, die aus bestimmten Gründen nicht verarbeitet wurden. Diese Informationen werden als Ereignisse in die Liste der aktiven Bedrohungen eingetragen.

Eine infizierte Datei gilt dann als *verarbeitet*, wenn Kaspersky Endpoint Security diese Datei im Zuge der Untersuchung des Computers auf Viren und andere Schadprogramme gemäß den Programmeinstellungen einer der folgenden Aktionen unterzogen hat:

- Desinfizieren.
- Löschen
- Löschen, wenn Desinfektion nicht möglich

Kaspersky Endpoint Security setzt die Datei auf die Liste der aktiven Bedrohungen, falls Kaspersky Endpoint Security bei der Untersuchung des Computers auf Viren und andere bedrohliche Programme mit dieser Datei eine Aktion ausgeführt hat, welche nicht in den Programmeinstellungen vorgesehen ist.

Dies ist in folgenden Fällen möglich:

- Die zu untersuchende Datei ist nicht verfügbar (Sie befindet sich beispielsweise auf einem Netzlaufwerk oder einem externen Laufwerk ohne Schreibrechte).
- In den Programmeinstellungen ist für Untersuchungsaufgaben im Abschnitt **Aktion beim Fund einer Bedrohung** die Aktion **Informieren** ausgewählt, und der Benutzer hat nach Anzeige der Meldung über eine infizierte Datei die Option **Überspringen** ausgewählt.

Sie können die Aufgabe zur benutzerdefinierten Untersuchung der Dateien aus der Liste mit aktiven Bedrohungen manuell starten, nachdem die Datenbanken und Programm-Module aktualisiert wurden. Nach der Untersuchung kann sich der Dateistatus ändern. Je nach Status können Sie die Dateien selbstständig den entsprechenden Aktionen unterziehen.

Sie können beispielsweise folgende Aktionen vornehmen:

- Löschen von Dateien mit dem Status *Infiziert*
- Wiederherstellen von infizierten Dateien, die wichtige Informationen enthalten, sowie von Dateien mit dem Status *Desinfiziert* und *Nicht infiziert*.

Arbeit mit der Liste der aktiven Bedrohungen

Die Liste der aktiven Bedrohungen ist eine Tabelle mit Ereignissen, die mit infizierten Dateien zusammenhängen, welche bisher nicht verarbeitet wurden.

Mit Dateien aus der Liste mit aktiven Bedrohungen können Sie folgende Aktionen ausführen:

- Liste der aktiven Bedrohungen anzeigen
- Dateien aus der Liste mit aktiven Bedrohungen unter Verwendung der aktuellen Version der Datenbanken und Module von Kaspersky Endpoint Security untersuchen
- Dateien aus der Liste mit aktiven Bedrohungen im Ursprungsordner oder in einem anderen Ordner Ihrer Wahl (falls der ursprüngliche Ordner der Datei nicht zum Schreiben verfügbar ist) wiederherstellen
- Dateien aus der Liste mit aktiven Bedrohungen löschen
- Ordner, in welchem eine Datei aus der Liste mit aktiven Bedrohungen ursprünglich gespeichert war, öffnen

Wenn Sie mit den Tabellendaten arbeiten, können Sie außerdem folgende Aktionen ausführen:

- aktive Bedrohungen nach den Spaltenwerten oder mithilfe eines komplexen Filters filtern
- Suchfunktion für aktive Bedrohungen verwenden
- aktive Bedrohungen sortieren
- Reihenfolge und Auswahl der Spalten, welche in der Liste mit aktiven Bedrohungen angezeigt werden, ändern
- aktive Bedrohungen gruppieren

Die Informationen über die ausgewählten aktiven Bedrohungen können erforderlichenfalls in die Zwischenablage kopiert werden.

Start der Aufgabe zur benutzerdefinierten Untersuchung von Dateien, die zur Liste der aktiven Bedrohungen gehören

Sie können die Aufgabe zur benutzerdefinierten Untersuchung von infizierten Dateien, die noch nicht verarbeitet wurden, manuell starten. Die Untersuchung kann beispielsweise gestartet werden, wenn die vorhergehende Untersuchung abgebrochen wurde oder wenn Sie nach einem Update der Datenbanken und Programm-Module die Dateien aus der Liste der aktiven Bedrohungen erneut untersuchen möchten.

Um die Aufgabe zur benutzerdefinierten Untersuchung von Dateien, die zur Liste der aktiven Bedrohungen gehören, zu starten, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf den Block **<...> aktive Bedrohungen**.

   Das Fenster **Aktive Bedrohungen** wird geöffnet.

3. Wählen Sie in der Tabelle im Fenster **Aktive Bedrohungen** ein oder mehrere Ereignisse aus, die sich auf Dateien beziehen, welche Sie untersuchen möchten.

   Zur Auswahl mehrerer Ereignisse halten Sie die Taste **STRG** gedrückt.

4. Starten Sie die Aufgabe zur benutzerdefinierten Untersuchung der Dateien nach einer der folgenden Methoden:

   - Klicken Sie auf die Schaltfläche **Erneut untersuchen**.
   - Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Erneut untersuchen**.

Dateien aus der Liste mit aktiven Bedrohungen löschen

Um Dateien aus der Liste mit aktiven Bedrohungen zu löschen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf den Block **<...> aktive Bedrohungen**.

   Das Fenster **Aktive Bedrohungen** wird geöffnet.
3. Wählen Sie in der Tabelle im Fenster **Aktive Bedrohungen** ein oder mehrere Ereignisse aus, die sich auf Dateien beziehen, welche Sie löschen möchten.

   Zur Auswahl mehrerer Ereignisse halten Sie die Taste **STRG** gedrückt.
4. Löschen Sie die Dateien nach einer der folgenden Methoden:

   - Klicken Sie auf **Löschen**.
   - Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Löschen**.

Integritätsprüfung für Programm-Module

Dieser Abschnitt informiert über die Besonderheiten und Einstellungen der Aufgabe zur Integritätsprüfung.

Über die Aufgabe zur Integritätsprüfung

Kaspersky Endpoint Security überprüft, ob die Programm-Module, die sich im Installationsordner des Programms befinden, Beschädigungen oder Änderungen aufweisen. Besitzt ein Programm-Modul eine inkorrekte digitale Signatur, so gilt das Modul als beschädigt.

Nach dem Start der Aufgabe zur Integritätsprüfung wird der Fortschritt in der Zeile unter dem Aufgabennamen im Fenster **Aufgaben** angezeigt.

Informationen über die Ausführungsergebnisse für die Aufgabe zur Integritätsprüfung werden in Berichten protokolliert.

Aufgabe zur Integritätsprüfung starten und abbrechen

Die Aufgabe zur Integritätsprüfung kann unabhängig vom gewählten Startmodus jederzeit gestartet oder abgebrochen werden.

Um die Aufgabe zur Integritätsprüfung zu starten oder abzubrechen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Aufgaben**, die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Aufgaben** wird geöffnet.
3. Wählen Sie mit der linken Maustaste den Block mit dem Namen der Aufgabe zur Integritätsprüfung.

   Der ausgewählte Block wird geöffnet.
4. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Aufgabe zur Integritätsprüfung starten möchten, klicken Sie auf **Start**.

     Der Status der Aufgabenausführung, der unter dem Namen der Aufgabe zur Integritätsprüfung angezeigt wird, ändert sich in *Wird ausgeführt*.
   - Wenn Sie die Aufgabe zur Integritätsprüfung abbrechen möchten, wählen Sie im Kontextmenü den Punkt **Abbrechen**.

     Der Status der Aufgabenausführung, der unter dem Namen der Aufgabe zur Integritätsprüfung angezeigt wird, ändert sich in *Abgebrochen*.

Um von der einfachen Programmoberfläche aus die Aufgabe zur Integritätsprüfung zu starten oder abzubrechen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Führen Sie im Kontextmenü in der Dropdown-Liste **Aufgaben** eine der folgenden Aktionen aus:

   - Wählen Sie eine nicht gestartete Aufgabe zur Integritätsprüfung aus, um sie zu starten.
   - Wählen Sie eine laufende Aufgabe zur Integritätsprüfung aus, um sie abzubrechen.
   - Wählen Sie eine angehaltene Aufgabe zur Integritätsprüfung aus, um sie erneut zu starten.

Startmodus für die Aufgabe zur Integritätsprüfung wählen

Um einen Startmodus für die Aufgabe zur Integritätsprüfung zu wählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Aufgaben** den Unterabschnitt **Integritätsprüfung**.

   Im rechten Fensterbereich werden die Einstellungen für die Aufgabe zur Integritätsprüfung angezeigt.
3. Wählen Sie im Abschnitt **Startmodus** eine der folgenden Varianten:

- Wählen Sie die Variante**Manuell**, wenn Sie die Aufgabe zur Integritätsprüfung manuell starten möchten.

- Wählen Sie die Variante **Nach Zeitplan**, um einen Startzeitplan für die Aufgabe zur Integritätsprüfung anzupassen.

4. Wenn Sie beim vorherigen Schritt die Variante **Nach Zeitplan** gewählt haben, legen Sie einen Startzeitplan für die Aufgabe zur Integritätsprüfung fest. Gehen Sie dazu folgendermaßen vor:

   a. Legen Sie in der Dropdown-Liste **Frequenz** fest, wann die Aufgabe zur Integritätsprüfung gestartet werden soll. Wählen Sie eine der folgenden Varianten: **Minuten**, **Stunden**, **Tage**, **Jede Woche**, **Zum festgelegten Zeitpunkt**, **Jeden Monat**, **Nach dem Programmstart**.

   b. Legen Sie abhängig von dem Element, das in der Dropdown-Liste **Frequenz** gewählt ist, den genauen Zeitpunkt für den Aufgabenstart fest.

   c. Aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, damit Kaspersky Endpoint Security eine Aufgabe zur Integritätsprüfung, die nicht nach Zeitplan ausgeführt wurde, zum nächstmöglichen Zeitpunkt ausführt.

      Ist in der Dropdown-Liste **Frequenz** das Element **Nach dem Programmstart**, **Minuten** oder **Stunden** gewählt, so ist das Kontrollkästchen **Übersprungene Aufgaben starten** nicht verfügbar.

   d. Aktivieren Sie das Kontrollkästchen **Nur bei Computerleerlauf ausführen**, damit Kaspersky Endpoint Security die Aufgabe anhält, wenn die Computerressourcen ausgelastet sind.

      Diese Zeitplanvariante erlaubt einen sparsamen Umgang mit der Rechnerleistung.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Arbeit mit Berichten

Dieser Abschnitt informiert darüber, wie Sie Berichtseinstellungen anpassen und mit Berichten arbeiten können.

Über Berichte

In den Berichten werden protokolliert: Informationen über Ausführung der einzelnen Komponenten von Kaspersky Endpoint Security, über die Ausführung der einzelnen Untersuchungsaufgaben, der Update-Aufgabe und der Aufgabe zur Integritätsprüfung, sowie über die allgemeine Programmausführung.

Die Berichte werden im Ordner ProgramData\Kaspersky Lab\KES\Report gespeichert.

Die Berichte können die folgenden Benutzerdaten enthalten:

- Pfade von Dateien, die mithilfe von Kaspersky Endpoint Security untersucht wurden

- Pfade von Registrierungsschlüsseln, die von Kaspersky Endpoint Security geändert wurden

- Benutzername für Microsoft Windows
- Adressen von Webseiten, die vom Benutzer geöffnet wurden

Die Daten im Bericht sind in Form einer Tabelle dargestellt, die eine Liste der Ereignisse enthält. Jede Tabellenzeile enthält Informationen über ein einzelnes Ereignis, wobei sich die Attribute des Ereignisses in den Tabellenspalten befinden. Einige Spalten sind nochmals unterteilt und enthalten Unterspalten mit zusätzlichen Attributen. Um die zusätzlichen Attribute anzuzeigen, klicken Sie auf die Schaltfläche ⊞ neben dem Namen der Spalte. Die Ereignisse, die bei der Ausführung von Komponenten oder bei der Ausführung von Aufgaben registriert werden, besitzen unterschiedliche Attribute.

Folgende Berichte sind verfügbar:

- Bericht **Systemaudit**. Enthält Informationen über Ereignisse, welche bei der Interaktion zwischen Benutzer und Programm eintreten, sowie Ereignisse, welche den generellen Programmbetrieb betreffen und sich nicht auf bestimmte Komponenten oder Aufgaben von Kaspersky Endpoint Security beziehen.
- Bericht über die Ausführung einer Komponente oder über die Ausführung einer Aufgabe von Kaspersky Endpoint Security
- Bericht **Verschlüsselung**. Enthält Informationen über die Ereignisse, welche bei der Verschlüsselung und Entschlüsselung von Daten auftreten.

In Berichten werden folgenden Prioritätsstufen für Ereignisse verwendet:

- **Informative Ereignisse**. Symbol  . Ereignisse mit informativem Charakter, welche in der Regel keine wichtigen Informationen enthalten.
- **Wichtige Ereignisse**. Symbol  . Ereignisse, die beachtet werden müssen, da sie auf wichtige Situationen bei der Ausführung von Kaspersky Endpoint Security hinweisen.
- **Kritische Ereignisse**. Symbol  . Ereignisse mit kritischer Priorität, die auf Probleme bei der Ausführung von Kaspersky Endpoint Security oder auf Schwachstellen im Schutz des Benutzercomputers hinweisen.

Zur Vereinfachung der Arbeit mit Berichten können Sie die Darstellung der Daten auf dem Bildschirm wie folgt ändern:

- Ereignisliste nach verschiedenen Kriterien filtern
- Funktion zur Suche nach einem bestimmten Ereignis verwenden
- Ausgewähltes Ereignis in einem separaten Block anzeigen
- Ereignisliste nach einer bestimmten Spalte des Berichts sortieren
- Ereignisse, die mithilfe eines Filters gruppiert sind, anzeigen und ausblenden
- Reihenfolge und Zusammensetzung der im Bericht angezeigten Spalten ändern

Bei Bedarf können Sie den erstellten Bericht in einer Textdatei speichern.

Außerdem können Sie Informationen aus den Berichten löschen. Dazu können die Informationen nach den Komponenten und Aufgaben von Kaspersky Endpoint Security gruppiert werden. Kaspersky Endpoint Security löscht alle Einträge der gewählten Berichte, von den ältesten bis zu den aktuellen Einträgen.

Wenn Kaspersky Endpoint Security mit Kaspersky Security Center verwaltet wird, können Informationen über Ereignisse an den Administrationsserver von Kaspersky Security Center übertragen werden. Details über die Arbeit mit Berichten in Kaspersky Security Center finden Sie im Hilfesystem zu Kaspersky Security Center.

Berichte konfigurieren

Zur Konfiguration der Berichte stehen Ihnen die folgenden Aktionen zur Verfügung:

- Maximale Speicherdauer für Berichte bestimmen

  Die standardmäßige Speicherdauer für Berichte über die von Kaspersky Endpoint Security protokollierten Ereignisse beträgt 30 Tage. Nach Ablauf dieses Zeitraums löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei. Sie können diese Zeitbeschränkung aufheben oder die maximale Speicherdauer für Berichte ändern.

- Maximale Größe der Berichtsdatei bestimmen

  Sie können für die Datei, die den Bericht enthält, eine maximale Größe festlegen. Die maximale Größe der Berichtsdatei beträgt standardmäßig 1024 MB. Nach Erreichen der maximalen Berichtsdateigröße löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei, womit ein Überschreiten der maximalen Berichtsdateigröße vermieden wird. Sie können die Größenbeschränkung für die Berichtsdatei aufheben oder einen anderen Wert festlegen.

Maximale Speicherdauer für Berichte anpassen

Gehen Sie folgendermaßen vor, um eine maximale Speicherdauer für Ereignisberichte festzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Berichte und Speicher** aus.

3. Führen Sie im rechten Fensterbereich im Block **Berichte** eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Berichte speichern für maximal**, um die Speicherdauer für Berichte zu beschränken. Legen Sie im Feld **Berichte speichern für maximal**, das sich rechts vom Kontrollkästchen befindet, eine maximale Speicherdauer für Berichte fest.

     Die maximale Speicherdauer für Berichte beträgt standardmäßig 30 Tage.

   - Deaktivieren Sie das Kontrollkästchen **Berichte speichern für maximal**, um die Speicherdauer für Berichte nicht zu beschränken.

   Die Beschränkung der Speicherdauer für Berichte ist standardmäßig aktiviert.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Maximale Größe der Berichtsdatei anpassen

Gehen Sie folgendermaßen vor, um die maximale Größe einer Berichtsdatei festzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Berichte und Speicher** aus.
3. Führen Sie im rechten Fensterbereich im Block **Berichte** eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Maximale Dateigröße**, wenn Sie die Größe der Berichtsdatei beschränken möchten. Geben Sie im Feld rechts vom Kontrollkästchen **Maximale Dateigröße** die maximale Größe der Berichtsdatei an.

     Die maximale Größe der Berichtsdatei ist standardmäßig auf 1024 MB begrenzt.
   - Deaktivieren Sie das Kontrollkästchen **Maximale Dateigröße**, wenn Sie die Größenbeschränkung für die Berichtsdatei aufheben möchten.

   Die Größenbeschränkung für die Berichtsdatei ist standardmäßig aktiviert.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Berichte anzeigen

Ist für einen Benutzer die Anzeige der Berichte verfügbar, so kann dieser Benutzer alle Ereignisse, die in den Berichten vorhanden sind, einsehen.

Um Berichte anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Berichte**, die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Berichte** wird geöffnet.
3. Wählen Sie im linken Bereich des Fensters **Berichte** in der Liste mit Komponenten und Aufgaben eine Komponente oder eine Aufgabe aus.

   Im rechten Fensterbereich wird ein Bericht angezeigt, der eine Liste mit Ereignissen für die Ausführungsergebnisse der ausgewählten Komponente oder der ausgewählten Aufgabe von Kaspersky Endpoint Security enthält.

   Die Ereignisse können im Bericht nach den Werten in den Zellen aus einer der Spalten sortiert werden.

Standardmäßig sind die Ereignisse im Bericht in aufsteigender Reihenfolge nach den Werten in den Zellen der Spalte **Ereignisdatum** sortiert.

Informationen über ein Ereignis im Bericht anzeigen

Im Bericht können Sie Detailinformationen über jedes einzelne Ereignis einsehen.

Um im Bericht Detailinformationen über ein Ereignis einzusehen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Berichte**, die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Berichte** wird geöffnet.
3. Wählen Sie im linken Fensterbereich den betreffenden Bericht für eine Komponente oder Aufgabe.

   Im rechten Fensterbereich werden in einer Tabelle die Ereignisse angezeigt, die zu diesem Bericht gehören. Um in einem Bericht nach bestimmten Ereignissen zu suchen, können die Funktionen zur Filterung, Suche und Sortierung verwendet werden.
4. Wählen Sie im Bericht das erforderliche Ereignis.

Im unteren Fensterbereich wird ein Abschnitt mit zusammenfassenden Informationen über das Ereignis angezeigt.

Bericht in Datei speichern

Der Benutzer ist selbst verantwortlich für die Sicherheit der Informationen, welche aus dem Bericht in einer Datei gespeichert werden, und insbesondere für die Kontrolle und Beschränkung des Zugriffs auf diese Informationen.

Der erstellte Bericht kann im Textformat als txt- oder csv-Datei gespeichert werden.

Kaspersky Endpoint Security speichert das Ereignis im Bericht in der gleichen Form, in welcher das Ereignis auf dem Bildschirm angezeigt wird. Die Zusammensetzung und die Reihenfolge der Ereignisattribute bleiben also unverändert.

Gehen Sie folgendermaßen vor, um einen Bericht in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Berichte**, die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Berichte** wird geöffnet.
3. Wählen Sie im linken Bereich des Fensters **Berichte** in der Liste mit Komponenten und Aufgaben eine Komponente oder eine Aufgabe aus.

   Im rechten Fensterbereich wird ein Bericht angezeigt, der eine Liste mit Ereignissen über die Ausführung der gewählten Komponente oder Aufgabe von Kaspersky Endpoint Security enthält.
4. Die Darstellung der Berichtsdaten kann bei Bedarf mit folgenden Methoden geändert werden:

   - Ereignisse filtern

- Ereignisse suchen
- Anordnung der Spalten ändern
- Ereignisse sortieren

5. Klicken Sie auf die Schaltfläche **Bericht speichern**, die sich rechts oben im Fenster befindet.

   Das Kontextmenü wird geöffnet.

6. Wählen Sie im Kontextmenü, mit welcher Codierung die Berichtsdatei gespeichert werden soll: **Als ANSI speichern** oder **Als Unicode speichern**.

   Das Standardfenster **Speichern unter** von Microsoft Windows wird geöffnet.

7. Geben Sie im Fenster **Speichern unter** den Ordner an, in dem die Berichtsdatei gespeichert werden soll.
8. Geben Sie im Feld **Dateiname** einen Namen für die Berichtsdatei an.
9. Wählen Sie im Feld **Dateityp** ein Format für die Berichtsdatei: TXT oder CSV.
10. Klicken Sie auf **Speichern**.

Berichte löschen

Gehen Sie folgendermaßen vor, um Informationen aus den Berichten zu löschen.

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Berichte und Speicher** aus.
3. Klicken Sie im rechten Fensterbereich im Block **Berichte** auf **Berichte löschen**.

   Das Fenster **Berichte löschen** wird geöffnet.

4. Aktivieren Sie die Kontrollkästchen für die Berichte, die gelöscht werden sollen:

   - **Alle Berichte**
   - **Bericht über die Schutzkomponenten**. Er enthält Informationen über die Ausführung der folgenden Komponenten von Kaspersky Endpoint Security:
     - Verhaltensanalyse
     - Exploit-Prävention
     - Programm-Überwachung.
     - Schutz vor bedrohlichen Dateien
     - Schutz vor Web-Bedrohungen

- Schutz vor E-Mail-Bedrohungen
- Schutz vor Netzwerkbedrohungen
- Schutz vor modifizierten USB-Geräten

- **Bericht für die Kontrollkomponenten**. Er enthält Informationen über die Ausführung der folgenden Komponenten von Kaspersky Endpoint Security:
  - Programmkontrolle
  - Gerätekontrolle
  - Web-Kontrolle
- **Bericht für die Datenverschlüsselung** Enthält Informationen über die ausgeführten Aufgaben zur Datenverschlüsselung.
- **Bericht über Untersuchungsaufgaben**. Enthält Informationen über die folgenden ausgeführten Untersuchungsaufgaben:
  - Vollständige Untersuchung
  - Untersuchung wichtiger Bereiche
  - Benutzerdefinierte Untersuchung

  Die Informationen über die Ausführung der Aufgabe zur Integritätsprüfung werden nur gelöscht, wenn das Kontrollkästchen **Alle Berichte** aktiviert ist.
- **Bericht über Update-Aufgaben**. Er enthält Informationen über ausgeführte Update-Aufgaben.
- **Bericht für die Komponente Firewall**. Er enthält Informationen über die Firewall.

5. Klicken Sie auf **OK**.

Benachrichtigungsdienst

Dieser Abschnitt informiert über den Benachrichtigungsdienst, welcher den Benutzer auf Ereignisse bei der Ausführung von Kaspersky Endpoint Security hinweist. Außerdem wird hier erklärt, wie die Benachrichtigungseinstellungen angepasst werden.

Über Meldungen von Kaspersky Endpoint Security

Während der Ausführung von Kaspersky Endpoint Security treten unterschiedliche Ereignisse ein. Benachrichtigungen über diese Ereignisse können rein informativ sein oder wichtige Informationen enthalten. Benachrichtigungen können beispielsweise über die erfolgreiche Aktualisierung der Datenbanken und Programm-Module informieren oder auf eine Funktionsstörung einer bestimmten Komponente hinweisen, deren Behebung aussteht.

Kaspersky Endpoint Security bietet die Möglichkeit, Informationen über Ereignisse, die im Programm eintreten, im Microsoft Windows-Ereignisbericht und/oder im Bericht für Kaspersky Endpoint Security aufzuzeichnen.

Kaspersky Endpoint Security bietet folgende Optionen für die Zustellung von Benachrichtigungen:

- mithilfe von Pop-up-Benachrichtigungen im Infobereich der Microsoft-Windows-Taskleiste
- per E-Mail

Die Benachrichtigungsmethoden können angepasst werden. Die Benachrichtigungsmethode wird für jeden Ereignistyp konfiguriert.

Einstellungen für den Benachrichtigungsdienst anpassen

Der Benachrichtigungsdienst kann wie folgt angepasst werden:

- Anpassen der Einstellungen für die Ereignisberichte, in denen Kaspersky Endpoint Security die Ereignisse speichert
- Anpassen der Bildschirmanzeige von Benachrichtigungen
- Anpassen des Versands von Benachrichtigungen per E-Mail

Wenn Sie mit der Ereignistabelle arbeiten, um den Benachrichtigungsdienst anzupassen, können Sie folgende Aktionen ausführen:

- Filtern der Ereignisse des Benachrichtigungsdienstes nach den Spaltenwerten oder anhand eines komplexen Filters
- Verwenden der Suchfunktion für Ereignisse des Benachrichtigungsdienstes
- Sortieren der Ereignisse des Benachrichtigungsdienstes
- Ändern der Reihenfolge und der Auswahl von Spalten, welche in der Ereignisliste des Benachrichtigungsdienstes angezeigt werden

Einstellungen der Ereignisberichte anpassen

Gehen Sie folgendermaßen vor, um die Einstellungen der Ereignisberichte anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Benutzeroberfläche** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Benutzeroberfläche von Kaspersky Endpoint Security angezeigt.
3. Klicken Sie unter **Meldungen** auf **Einstellungen**.

   Das Fenster **Meldungen** wird geöffnet.

Im linken Fensterbereich werden die Komponenten und Aufgaben von Kaspersky Endpoint Security angezeigt. Im rechten Fensterbereich befindet sich eine Ereignisliste für die gewählte Komponente oder für die gewählte Aufgabe.

4. Wählen Sie im linken Fensterbereich die Komponente oder Aufgabe aus, deren Ereignisberichte Sie konfigurieren möchten.

5. Aktivieren Sie für die entsprechenden Ereignisse die Kontrollkästchen in den Spalten **Lokal protokollieren** und **Im Windows-Ereignisprotokoll speichern**.

   Ereignisse, für welche das Kontrollkästchen in der Spalte **Lokal protokollieren** aktiviert ist, werden in **Anwendungs- und Dienstprotokollen** im Abschnitt **Kaspersky Event Log** angezeigt. Ereignisse, für welche das Kontrollkästchen in der Spalte **Im Windows-Ereignisprotokoll speichern** aktiviert ist, werden in **Windows-Protokollen** im Abschnitt **Anwendung** angezeigt. Um die Ereignisprotokolle zu öffnen, wählen Sie **Start** → **Systemsteuerung** → **Verwaltung** → **Ereignisanzeige** aus.

   > Ereignisse können die folgenden Benutzerdaten enthalten: Pfade von Dateien, die mithilfe von Kaspersky Endpoint Security untersucht wurden; Pfade von Registrierungsschlüsseln, die von Kaspersky Endpoint Security geändert wurden; Benutzername für Microsoft Windows; Adressen von Webseiten, die vom Benutzer geöffnet wurden

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Anzeige und Versand von Benachrichtigungen anpassen

Um die Anzeige und den Versand von Benachrichtigungen anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Benutzeroberfläche** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Benutzeroberfläche von Kaspersky Endpoint Security angezeigt.

3. Klicken Sie unter **Meldungen** auf **Einstellungen**.

   Das Fenster **Meldungen** wird geöffnet.

   Im linken Fensterbereich werden die Komponenten und Aufgaben von Kaspersky Endpoint Security angezeigt. Im rechten Fensterbereich befindet sich eine Ereignisliste für die gewählte Komponente oder für die gewählte Aufgabe.

4. Wählen Sie im linken Fensterbereich die Komponente oder Aufgabe aus, für die der Versand von Meldungen angepasst werden soll.

5. Aktivieren Sie in der Spalte **Auf dem Bildschirm anzeigen** die Kontrollkästchen der entsprechenden Ereignisse.

   Informationen über die gewählten Ereignisse werden auf dem Bildschirm im Infobereich der Microsoft-Windows-Taskleiste als Pop-up-Benachrichtigungen angezeigt.

6. Aktivieren Sie in der Spalte **Per E-Mail benachrichtigen** die Kontrollkästchen der entsprechenden Ereignisse.

   Informationen über die gewählten Ereignisse werden als E-Mail-Nachricht gesendet, wenn die Einstellungen für den Versand von E-Mail-Benachrichtigungen festgelegt sind.

   > Ereignisse können die folgenden Benutzerdaten enthalten: Pfade von Dateien, die mithilfe von Kaspersky Endpoint Security untersucht wurden; Pfade von Registrierungsschlüsseln, die von Kaspersky Endpoint Security geändert wurden; Benutzername für Microsoft Windows; Adressen von Webseiten, die vom Benutzer geöffnet wurden

7. Klicken Sie auf **E-Mail-Benachrichtigungen anpassen**.

   Das Fenster **E-Mail-Benachrichtigungen anpassen** wird geöffnet.

8. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigungen senden**, um den Versand zu aktivieren. Benachrichtigungen erfolgen für die in Kaspersky Endpoint Security eingetretenen Ereignisse, die in der Spalte **Per E-Mail benachrichtigen** markiert sind.

9. Passen Sie den Versand von E-Mail-Meldungen an.

10. Klicken Sie im Fenster **E-Mail-Benachrichtigungen anpassen** auf **OK**.

11. Klicken Sie im Fenster **Meldungen** auf **OK**.

12. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Anzeige von Warnungen über den Programmstatus im Infobereich anpassen

Um die Anzeige von Warnungen über den Programmstatus im Infobereich der Taskleiste anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Benutzeroberfläche** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Benutzeroberfläche von Kaspersky Endpoint Security angezeigt.

3. Aktivieren Sie im Abschnitt **Warnungen** die Kontrollkästchen für jene Ereigniskategorien, über die im Infobereich der Microsoft-Windows-Taskleiste Benachrichtigungen angezeigt werden sollen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Treten Ereignisse auf, die zu den ausgewählten Kategorien gehören, so ändert sich das Programmsymbol im Infobereich der Taskleiste je nach Priorität der Warnung in  oder  .

Arbeit mit dem Backup

Dieser Abschnitt erklärt, wie die Backup-Einstellungen angepasst werden und wie das Backup funktioniert.

Über das Backup

Das *Backup* ist eine Liste mit Backup-Kopien von Dateien, die gelöscht oder bei der Desinfektion verändert wurden. Eine *Backup-Kopie* ist die Kopie einer Datei, die vor der Desinfektion oder dem Löschen dieser Datei angelegt wird. Die Backup-Kopien von Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Backup-Kopien von Dateien werden im Ordner ProgramData\Kaspersky Lab\KES\QB gespeichert.

Zum Zugriff auf diesen Ordner sind die Benutzer der Gruppe Administrators berechtigt. Beschränkte Zugriffsrechte für diesen Ordner besitzt der Benutzer, unter dessen Benutzerkonto die Installation von Kaspersky Endpoint Security ausgeführt wurde.

In Kaspersky Endpoint Security können die Zugriffsrechte für Benutzer auf die Backup-Kopien von Dateien nicht angepasst werden.

Es kann vorkommen, dass Dateien bei der Desinfektion nicht vollständig erhalten bleiben. Wenn wichtige Informationen, die in einer Datei enthalten waren, aufgrund einer Desinfektion vollständig oder teilweise verloren gegangen sind, können Sie versuchen, die Datei aus ihrer Backup-Kopie in den ursprünglichen Ordner der Datei wiederherzustellen.

Wenn Kaspersky Endpoint Security mit Kaspersky Security Center verwaltet wird, können Backup-Kopien für Dateien an den Administrationsserver von Kaspersky Security Center übertragen werden. Details über die Arbeit mit Backup-Kopien für Dateien in Kaspersky Security Center finden Sie im Hilfesystem zu Kaspersky Security Center.

Backup-Einstellungen anpassen

Um die Backup-Einstellungen anzupassen, können Sie können folgende Aktionen ausführen:

- Maximale Speicherdauer für Dateikopien im Backup festlegen.

  Die maximale Speicherdauer für Backup-Kopien im Backup beträgt standardmäßig 30 Tage. Nach Ablauf der maximalen Speicherdauer löscht Kaspersky Endpoint Security die ältesten Dateien aus dem Backup. Sie können diese Zeitbeschränkung aufheben oder die maximale Speicherdauer für Dateien ändern.

- Maximale Größe des Backups anpassen.

  Standardmäßig beträgt die maximale Größe für das Backup 100 MB. Nach Erreichen der maximalen Größe löscht Kaspersky Endpoint Security automatisch die ältesten Dateien aus dem Backup. Sie können die Größenbeschränkung für das Backup aufheben oder die maximale Größe ändern.

Maximale Speicherdauer für Dateien im Backup anpassen

Um eine maximale Speicherdauer für Dateien im Backup festzulegen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Berichte und Speicher** aus.
3. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie im rechten Fensterbereich im Block **Backup** das Kontrollkästchen **Objekte speichern für maximal**, um die Speicherdauer für Dateikopien im Backup zu beschränken. Geben Sie im Feld rechts vom Kontrollkästchen **Objekte speichern für maximal** an, wie lange Dateikopien im Backup maximal aufbewahrt werden sollen. Die maximale Speicherdauer für Backup-Kopien im Backup beträgt standardmäßig 30 Tage.
   - Deaktivieren Sie im rechten Fensterbereich im Block **Backup** das Kontrollkästchen **Objekte speichern für maximal**, um die Beschränkung der Speicherdauer für Dateikopien im Backup aufzuheben.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Maximale Größe für das Backup anpassen

Um die maximale Größe für das Backup anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Berichte und Speicher** aus.
3. Führen Sie eine der folgenden Aktionen aus:
   - Um die Gesamtgröße des Backups zu beschränken, aktivieren Sie das Kontrollkästchen **Maximale Speichergröße** im rechten Fensterbereich im Abschnitt **Backup** und geben Sie im Feld rechts vom Kontrollkästchen **Maximale Speichergröße** die maximale Größe für das Backup an.

     Die maximale Größe des Datenspeichers beträgt standardmäßig 100 MB, einschließlich der Backup-Kopien für Dateien.
   - Um die Größenbeschränkung für das Backup aufzuheben, deaktivieren Sie das Kontrollkästchen **Maximale Speichergröße** im rechten Fensterbereich im Abschnitt **Backup-Einstellungen**.

   Die Größe des Backups ist standardmäßig nicht beschränkt.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Dateien aus dem Backup wiederherstellen und löschen

Wird in einer Datei schädlicher Code gefunden, so blockiert Kaspersky Endpoint Security die Datei, weist Ihr den Status *Infiziert* zu, legt im Backup eine Backup-Kopie an und führt einen Desinfektionsversuch aus. War die Desinfektion erfolgreich, ändert sich der Status der Sicherungskopie in *Desinfiziert*. Die Datei ist ursprünglichen Speicherordner wieder verfügbar. Falls die Datei nicht desinfiziert werden kann, wird sie von

Kaspersky Endpoint Security aus dem Ursprungsordner gelöscht. Sie können die Datei aus einer desinfizierten Backup-Kopie im ursprünglichen Ordner wiederherstellen.

Wenn schädlicher Code in einer Datei gefunden wird, die zu einer Anwendung aus dem Windows Store gehört, kopiert Kaspersky Endpoint Security die Datei nicht ins Backup, sondern löscht die Datei sofort. Die Integrität einer Anwendung aus dem Windows Store kann mithilfe von Microsoft Windows 8 wiederhergestellt werden (Details über die Wiederherstellung einer Anwendung aus dem Windows Store finden Sie im *Hilfesystem für Microsoft Windows 8*).

Backup-Kopien, deren maximale Speicherdauer verstrichen ist, werden unabhängig von ihrem Status automatisch aus dem Backup gelöscht. Die Speicherdauer ist in den Programmeinstellungen festgelegt.

Sie können eine beliebige Kopie einer Datei auch selbst aus dem Backup löschen.

Die Backup-Kopien werden in einer Liste angezeigt.

Bei der Arbeit mit dem Backup stehen Ihnen für die Sicherungskopien der Dateien die folgenden Aktionen zur Verfügung:

- Auswahl von Backup-Kopien für Dateien anzeigen

  Für die Backup-Kopie einer Datei wird der Pfad des Ordners, an dem diese Datei ursprünglich gespeichert war, angezeigt. Der Pfad des ursprünglichen Ordners der Datei kann persönliche Daten enthalten.

- Dateien aus Backup-Kopien in die ursprünglichen Ordner wiederherstellen
- Backup-Kopien von Dateien aus dem Backup löschen

Wenn Sie mit den Tabellendaten arbeiten, können Sie außerdem folgende Aktionen ausführen:

- Backup-Kopien nach Spalten filtern, u. a. nach komplexen Filterbedingungen
- Suchfunktion für Backup-Kopien verwenden
- Backup-Kopien sortieren
- Ändern der Reihenfolge und der Auswahl für die Spalten, welche in der Tabelle der Backup-Dateien angezeigt werden

Sie können Informationen über die ausgewählten Backup-Ereignisse in die Zwischenablage kopieren. Um mehrere Backup-Dateien zu wählen, öffnen Sie durch Rechtsklick das Kontextmenü einer beliebigen Datei und wählen Sie den Punkt **Alle markieren**. Um die Markierung für bestimmte Dateien aufzuheben, halten Sie dann die **STRG**-Taste gedrückt und klicken Sie auf die entsprechenden Dateien.

Dateien aus dem Backup wiederherstellen

Wenn sich in einem Backup-Ordner mehrere Dateien mit identischen Namen und unterschiedlichen Inhalten befinden, so kann nur jene Datei wiederhergestellt werden, die zuletzt ins Backup verschoben wurde.

Gehen Sie folgendermaßen vor, um Dateien aus dem Backup wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Datenverwaltung**, die sich im unteren Bereich des Programmhauptfensters befindet.

   Das Fenster **Backup** wird geöffnet.
3. Um alle Dateien aus dem Backup wiederherzustellen, wählen Sie im Fenster **Backup** im Kontextmenü einer beliebigen Datei den Punkt **Alle wiederherstellen** aus.

   Kaspersky Endpoint Security stellt alle Dateien aus ihren Backup-Kopien in den ursprünglichen Ordnern wieder her.
4. Gehen Sie folgendermaßen vor, um eine oder mehrere Dateien aus dem Backup wiederherzustellen:

   a. Wählen Sie in der Tabelle im Fenster **Backup** eine oder mehrere Backup-Dateien aus.

   Um mehrere Backup-Dateien zu wählen, öffnen Sie durch Rechtsklick das Kontextmenü einer beliebigen Datei und wählen Sie den Punkt **Alle markieren**. Um die Markierung für bestimmte Dateien aufzuheben, halten Sie dann die **STRG**-Taste gedrückt und klicken Sie auf die entsprechenden Dateien.

   b. Stellen Sie die Dateien nach einer der folgenden Methoden wieder her:

   - Klicken Sie auf die Schaltfläche **Wiederherstellen**.
   - Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Wiederherstellen**.

   Kaspersky Endpoint Security stellt die Dateien aus den ausgewählten Backup-Kopien in den ursprünglichen Ordnern wieder her.

Backup-Kopien von Dateien aus dem Backup löschen

Gehen Sie folgendermaßen vor, um Backup-Kopien aus dem Backup zu löschen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Datenverwaltung**, die sich im unteren Bereich des Programmhauptfensters befindet.
3. Das Fenster **Backup** wird geöffnet.
4. Um alle Dateien aus dem Backup zu löschen, führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie im Kontextmenü einer beliebigen Datei den Punkt **Alle löschen**.

- Klicken Sie auf **Speicher leeren**.

Kaspersky Endpoint Security löscht alle Backup-Kopien aus dem Backup.

5. Um eine oder mehrere Dateien aus dem Backup zu löschen, gehen Sie wie folgt vor:

   a. Wählen Sie in der Tabelle im Fenster **Backup** eine oder mehrere Backup-Dateien aus.

   Um mehrere Backup-Dateien zu wählen, öffnen Sie durch Rechtsklick das Kontextmenü einer beliebigen Datei und wählen Sie den Punkt **Alle markieren**. Um die Markierung für bestimmte Dateien aufzuheben, halten Sie dann die **STRG**-Taste gedrückt und klicken Sie auf die entsprechenden Dateien.

   b. Löschen Sie die Dateien nach einer der folgenden Methoden:

   - Klicken Sie auf **Löschen**.
   - Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Löschen**.

Kaspersky Endpoint Security löscht die gewählten Backup-Kopien aus dem Backup.

Erweiterte Programmeinstellungen

Dieser Abschnitt informiert über die allgemeinen Einstellungen für Kaspersky Endpoint Security.

Vertrauenswürdige Zone

Dieser Abschnitt informiert über die vertrauenswürdige Zone und erklärt die Einrichtung von Untersuchungsausnahmen sowie die Erstellung einer Liste mit vertrauenswürdigen Programmen.

Über die vertrauenswürdige Zone

Die *vertrauenswürdige Zone* ist eine Liste mit Objekten und Programmen, die nicht von Kaspersky Endpoint Security untersucht werden. Diese Liste wird vom Systemadministrator erstellt. Anders ausgedrückt, handelt es sich hierbei um ein Paket von Untersuchungsausnahmen.

Die vertrauenswürdige Zone wird manuell vom Systemadministrator angelegt. Berücksichtigt werden dabei die Besonderheiten von Objekten, die für die Arbeit erforderlich sind, sowie die Programme, die auf dem Computer installiert sind. Die Aufnahme von Objekten und Programmen in die vertrauenswürdige Zone kann beispielsweise erforderlich sein, wenn Kaspersky Endpoint Security den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt oder Programm unschädlich ist.

Sie können folgende Elemente von der Untersuchung ausschließen:

- Dateien eines bestimmten Formats
- Dateien nach Maske
- bestimmte Dateien
- Ordner

- Programmprozesse

Untersuchungsausnahmen

Eine *Untersuchungsausnahme* ist eine Kombination von Bedingungen. Sind diese Bedingungen erfüllt, so untersucht Kaspersky Endpoint Security ein Objekt nicht auf Viren und andere bedrohliche Programme.

Die Untersuchungsausnahmen ermöglichen es, mit legalen Programmen zu arbeiten, die von Angreifern für eine Beschädigung des Computers oder der Benutzerdaten verwendet werden können. Solche Programme haben zwar selbst keine schädlichen Funktionen, können aber von schädlichen Programmen als Hilfskomponenten missbraucht werden. Zu diesen Programmen gehören beispielsweise Programme zur Remote-Administration, IRC-Clients, FTP-Server, diverse Hilfsprogramme zum Beenden und zum Verstecken von Prozessen, Keylogger, Programme zur Kennwortermittlung und Programme zur automatischen Einwahl auf kostenpflichtige Websites. Solche Software wird nicht als Virus klassifiziert. Nähere Informationen zu legalen Programmen, die von Angreifern missbraucht werden können, um den Computer oder die Daten des Anwenders zu beschädigen, erhalten Sie auf der Webseite der Viren-Enzyklopädie von Kaspersky Lab unter https://de.securelist.com/threats/entdeckte-objekte/ .

Derartige Programme können bei der Ausführung von Kaspersky Endpoint Security gesperrt werden. Sie können Untersuchungsausnahmen anpassen, um eine Sperrung von notwendigen Programmen zu verhindern. Dazu muss der vertrauenswürdigen Zone der Name oder eine Namensmaske hinzugefügt werden, die der Klassifikation der Viren-Enzyklopädie von Kaspersky Lab entspricht. Es kann beispielsweise sein, dass Sie häufig mit dem Programm Remote Administrator arbeiten. Dabei handelt es sich um ein Remote-Management-System, das die Arbeit auf einem Remote-Computer erlaubt. Eine solche Programmaktivität wird von Kaspersky Endpoint Security als schädlich eingestuft und kann blockiert werden. Um zu verhindern, dass ein Programm gesperrt wird, muss eine Untersuchungsausnahme erstellt werden. In dieser Ausnahme wird ein Name oder eine Namensmaske angegeben, die der Klassifikation der Viren-Enzyklopädie von Kaspersky Lab entspricht.

Ist auf Ihrem Computer ein Programm installiert, das Informationen sammelt und zur Verarbeitung weiterleitet, so kann das Programm von Kaspersky Endpoint Security als schädlich eingestuft werden. Um dies zu vermeiden, können Sie das Programm von der Untersuchung ausschließen. Die entsprechenden Einstellungen für Kaspersky Endpoint Security werden im vorliegenden Dokument beschrieben.

Untersuchungsausnahmen können von folgenden Komponenten und Programmaufgaben verwendet werden, die vom Systemadministrator erstellt wurden:

- Verhaltensanalyse
- Exploit-Prävention
- Programm-Überwachung.
- Schutz vor bedrohlichen Dateien
- Schutz vor Web-Bedrohungen
- Schutz vor E-Mail-Bedrohungen
- Untersuchungsaufgaben

Liste der vertrauenswürdigen Programme

Die *Liste der vertrauenswürdigen Programme* ist eine Liste mit Programmen, deren Datei- oder Netzwerkaktivität nicht von Kaspersky Endpoint Security überwacht wird (selbst wenn diese schädlich ist). Gleiches gilt für den Zugriff dieser Programme auf die Systemregistrierung. Kaspersky Endpoint Security untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden, und kontrolliert die Aktivität aller Programme sowie den von ihnen erzeugten Netzwerkverkehr. Programme, die auf der Liste der vertrauenswürdigen Programme stehen, werden von Kaspersky Endpoint Security aus der Untersuchung ausgeschlossen.

Wenn Sie beispielsweise die Objekte, die von dem Microsoft-Windows-Programm Editor verwendet werden, für ungefährlich und eine Untersuchung dieser Objekte für nicht erforderlich halten, so vertrauen Sie diesem Programm und sollten das Programm Editor zur Liste der vertrauenswürdigen Programme hinzufügen. Die Objekte, die dieses Programm verwendet, werden dann nicht untersucht.

Außerdem können spezielle Aktionen, die von Kaspersky Endpoint Security als schädlich klassifiziert werden, im Rahmen bestimmter Programme ungefährlich sein. So ist das Abfangen eines Textes, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (z. B. Punto Switcher) ein normaler Vorgang. Es wird empfohlen, solche Programme in die Liste der vertrauenswürdigen Programme aufzunehmen, um ihre speziellen Funktionen zu berücksichtigen und sie von der Aktivitätskontrolle auszuschließen.

Wenn vertrauenswürdige Programme von der Untersuchung ausgeschlossen werden, lassen sich Kompatibilitätsprobleme von Kaspersky Endpoint Security mit anderen Programmen vermeiden (beispielsweise Probleme einer doppelten Untersuchung des Netzwerkverkehrs eines anderen Computers durch Kaspersky Endpoint Security und durch ein anderes Antiviren-Programm). Außerdem wird dadurch die Leistung des Computers erhöht, was speziell bei der Verwendung von Serverprogrammen wichtig ist.

Die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms werden jedoch weiterhin auf Viren und andere Schadprogramme untersucht. Verwenden Sie Untersuchungsausnahmen, um ein Programm vollständig aus der Untersuchung durch Kaspersky Endpoint Security auszuschließen.

Erstellung von Untersuchungsausnahmen

Ein Objekt wird nicht von Kaspersky Endpoint Security untersucht, wenn beim Start einer Untersuchungsaufgabe das Laufwerk, auf dem sich das Objekt befindet, oder der Ordner, in dem sich das Objekt befindet, zum Untersuchungsbereich gehört. Wenn jedoch beim Start einer benutzerdefinierten Untersuchungsaufgabe dieses Objekt ausdrücklich ausgewählt wird, so bleibt die Untersuchungsausnahme unberücksichtigt.

Gehen Sie folgendermaßen vor, um Untersuchungsausnahmen zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.
3. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Zone** auf **Einstellungen**.

   Das Fenster **Vertrauenswürdige Zone** wird auf der Registerkarte **Untersuchungsausnahmen** geöffnet.
4. Klicken Sie auf **Hinzufügen**.

Das Fenster **Untersuchungsausnahme** wird geöffnet. In diesem Fenster können Sie eine Untersuchungsausnahme festlegen. Dazu können ein oder mehrere Kriterien aus dem Block **Eigenschaften** verwendet werden.

5. Um eine Datei oder einen Ordner von der Untersuchung auszuschließen, gehen Sie wie folgt vor:

   a. Aktivieren Sie unter **Eigenschaften** das Kontrollkästchen **Datei oder Ordner**.

   b. Öffnen Sie mit dem Link **Datei oder Ordner wählen**, der sich im Block **Beschreibung der Untersuchungsausnahme** befindet, das Fenster **Datei- oder Ordnername**.

   c. Geben Sie entweder den Datei- oder Ordnernamen oder die Maske eines Datei- oder Ordnernamens ein, oder klicken Sie auf **Durchsuchen** und wählen Sie in der Ordnerstruktur eine Datei oder einen Ordner aus.

   d. Klicken Sie im Fenster **Datei- oder Ordnername** auf **OK**.

   Im Fenster **Untersuchungsausnahme** erscheint im Abschnitt **Beschreibung der Untersuchungsausnahme** ein Link für die hinzugefügte Datei oder den Ordner.

6. Um Objekte mit einem bestimmten Namen von der Untersuchung auszuschließen, gehen Sie wie folgt vor:

   a. Aktivieren Sie im Abschnitt **Eigenschaften** das Kontrollkästchen **Objektname**.

   b. Öffnen Sie mit dem Link **Objektnamen eingeben**, der sich im Abschnitt **Beschreibung der Untersuchungsausnahme** befindet, das Fenster **Objektname**.

   c. Geben Sie in diesem Fenster denNamen oder eine Namensmaske des Objekts ein, welche der Klassifikation der Kaspersky-Lab-Viren-Enzyklopädie entspricht.

   d. Klicken Sie im Fenster **Objektname** auf **OK**.

   Im Fenster **Untersuchungsausnahme** erscheint unter **Beschreibung der Untersuchungsausnahme** ein Link für den hinzugefügten Objektnamen.

7. Um ein Objekt mit einem bestimmten Hash von der Untersuchung auszuschließen, gehen Sie wie folgt vor:

   a. Aktivieren Sie im Block **Eigenschaften** das Kontrollkästchen **Hash des Objekts**.

   b. Öffnen Sie mit dem Link **Objektnamen eingeben**, der sich im Block **Beschreibung der Untersuchungsausnahme** befindet, das Fenster **Hash des Objekts**.

   c. Geben Sie den SHA256-Hash des Objektes ein, welcher der Klassifikation der Viren-Enzyklopädie von Kaspersky Lab entspricht, oder wählen Sie mithilfe der Schaltfläche **Durchsuchen** eine Datei aus.

   d. Klicken Sie im Fenster **Hash des Objekts** auf **OK**.

   Im Fenster **Untersuchungsausnahme** erscheint im Block **Beschreibung der Untersuchungsausnahme** ein Link für den hinzugefügten Hash des Objektes.

8. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

9. Legen Sie die Komponenten von Kaspersky Endpoint Security fest, für die eine Untersuchungsausnahme verwendet werden soll.

   a. Aktivieren Sie mit dem Link **alle** im Abschnitt **Beschreibung der Untersuchungsausnahme** den Link **Komponenten wählen**.

   b. Öffnen Sie mit dem Link **Komponenten wählen** das Fenster **Schutzkomponenten**.

   c. Aktivieren Sie die Kontrollkästchen für jene Komponenten, für welche die Untersuchungsausnahme gelten soll.

   d. Klicken Sie im Fenster **Schutzkomponenten** auf**OK**.

   Werden in den Einstellungen einer Untersuchungsausnahme bestimmte Komponenten angegeben, so wird die Ausnahme nur von den gewählten Komponenten von Kaspersky Endpoint Security verwendet.

   Wenn in den Einstellungen einer Untersuchungsausnahme keine bestimmten Komponenten angegeben werden, wird diese Ausnahme von allen Komponenten von Kaspersky Endpoint Security verwendet.

10. Klicken Sie im Fenster **Untersuchungsausnahme** auf **OK**.

    Die hinzugefügte Untersuchungsausnahme erscheint in der Tabelle auf der Registerkarte **Untersuchungsausnahmen** des Fensters **Vertrauenswürdige Zone**. Im Abschnitt **Beschreibung der Untersuchungsausnahme** werden die für diese Untersuchungsausnahme festgelegten Einstellungen angezeigt.

11. Klicken Sie im Fenster **Vertrauenswürdige Zone** auf **OK**.

12. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Änderung von Untersuchungsausnahmen

Gehen Sie folgendermaßen vor, um Untersuchungsausnahmen zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.

3. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Zone** auf **Einstellungen**.

   Das Fenster **Vertrauenswürdige Zone** wird auf der Registerkarte **Untersuchungsausnahmen** geöffnet.

4. Wählen Sie die entsprechende Untersuchungsausnahme aus der Liste aus.

5. Ändern Sie die Einstellungen der Untersuchungsausnahme. Dafür gibt es folgende Methoden:

   - Klicken Sie auf **Ändern**.

     Das Fenster **Untersuchungsausnahmen** wird geöffnet.

- Klicken Sie im Feld **Beschreibung der Untersuchungsausnahme** auf einen Link, um im folgenden Fenster die entsprechende Einstellung zu ändern.

6. Wenn Sie beim vorherigen Schritt auf **Ändern** geklickt haben, klicken Sie nun im Fenster **Untersuchungsausnahme** auf **OK**.

   Im Abschnitt **Beschreibung der Untersuchungsausnahme** werden die geänderten Einstellungen der Untersuchungsausnahme angezeigt.

7. Klicken Sie im Fenster **Vertrauenswürdige Zone** auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Löschen von Untersuchungsausnahmen

Gehen Sie folgendermaßen vor, um Untersuchungsausnahmen zu löschen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.

3. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Zone** auf **Einstellungen**.

   Das Fenster **Vertrauenswürdige Zone** wird auf der Registerkarte **Untersuchungsausnahmen** geöffnet.

4. Wählen Sie die entsprechende Untersuchungsausnahme aus der Liste der Untersuchungsausnahmen aus.

5. Klicken Sie auf **Löschen**.

   Die gelöschte Untersuchungsausnahme wird aus der Liste entfernt.

6. Klicken Sie im Fenster **Vertrauenswürdige Zone** auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktivierung und Deaktivierung von Untersuchungsausnahmen

Gehen Sie wie folgt vor, um die Anwendung einer Untersuchungsausnahme zu starten oder zu beenden:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.

3. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Zone** auf **Einstellungen**.

   Das Fenster **Vertrauenswürdige Zone** wird auf der Registerkarte **Untersuchungsausnahmen** geöffnet.

4. Wählen Sie die entsprechende Ausnahme aus der Liste der Untersuchungsausnahmen aus.

5. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen neben der jeweiligen Untersuchungsausnahme, damit diese Ausnahme angewandt wird.

   - Deaktivieren Sie das Kontrollkästchen neben der jeweiligen Untersuchungsausnahme, damit diese Ausnahme vorübergehend nicht angewandt wird.

6. Klicken Sie auf **OK**.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Liste mit vertrauenswürdigen Programmen erstellen

Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Programmen anzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.

3. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Zone** auf **Einstellungen**.

   Es öffnet sich das Fenster **Vertrauenswürdige Zone**.

4. Wählen Sie im Fenster **Vertrauenswürdige Zone** die Registerkarte **Vertrauenswürdige Programme**.

5. Gehen Sie folgendermaßen vor, um ein Programm zur Liste für vertrauenswürdige Programme hinzuzufügen:

   a. Klicken Sie auf **Hinzufügen**.

   b. Führen Sie im Kontextmenü eine der folgenden Aktionen aus:

      - Wählen Sie den Punkt **Programme**, um in der Liste der Programme, die auf dem Computer installiert sind, nach einem Programm zu suchen.

        Das Fenster **Programm wählen** wird geöffnet.

      - Wählen Sie den Punkt **Durchsuchen**, um den Pfad der ausführbaren Datei eines Programms anzugeben.

        Das Windows-Standardfenster **Öffnen** wird geöffnet.

   c. Wählen Sie ein Programm. Dafür gibt es folgende Methoden:

      - Wenn Sie beim vorherigen Schritt den Punkt **Programme** gewählt haben, wählen Sie in der Liste der auf dem Computer installierten Programme ein Programm und klicken Sie im Fenster **Programm wählen** auf **OK**.

- Wenn Sie beim vorherigen Schritt den Punkt **Durchsuchen** gewählt haben, geben Sie den Pfad der ausführbaren Datei des entsprechenden Programms an und klicken Sie im Microsoft-Windows-Standardfenster **Öffnen** auf die Schaltfläche **Öffnen**.

Nach dem Abschluss dieser Schritte wird das Fenster **Untersuchungsausnahmen für das Programm** geöffnet.

a. Aktivieren Sie die Kontrollkästchen für die erforderlichen Regeln der vertrauenswürdigen Zone für das gewählte Programm:

- **Zu öffnende Dateien nicht untersuchen**
- **Programmaktivität nicht kontrollieren**
- **Beschränkungen des übergeordneten Prozesses (Programms) nicht übernehmen**
- **Aktivität der Unterprogramme nicht kontrollieren**
- **Interaktion mit der Programmoberfläche nicht blockieren**
- **Netzwerkverkehr nicht untersuchen**

b. Klicken Sie im Fenster **Untersuchungsausnahmen für das Programm** auf **OK**.

Das hinzugefügte vertrauenswürdige Programm erscheint in der Liste der vertrauenswürdigen Programme.

6. Gehen Sie folgendermaßen vor, um die Einstellungen für ein vertrauenswürdiges Programm zu ändern:

a. Wählen Sie ein vertrauenswürdiges Programm aus der Liste der vertrauenswürdigen Programme.

b. Klicken Sie auf **Ändern**.

c. Das Fenster **Untersuchungsausnahmen für das Programm** wird geöffnet.

d. Aktivieren oder deaktivieren Sie die Kontrollkästchen für die erforderlichen Regeln der vertrauenswürdigen Zone für das gewählte Programm.

> Wurde im Fenster **Untersuchungsausnahmen für das Programm** keine Regel der vertrauenswürdigen Zone für das Programm gewählt, so wird das vertrauenswürdige Programm in die Untersuchung aufgenommen. Das vertrauenswürdige Programm wird nicht aus der Liste für vertrauenswürdige Programme entfernt, nur das entsprechende Kontrollkästchen wird deaktiviert.

e. Klicken Sie im Fenster **Untersuchungsausnahmen für das Programm** auf **OK**.

7. Gehen Sie folgendermaßen vor, um ein vertrauenswürdiges Programm aus der Liste der vertrauenswürdigen Programme zu entfernen:

a. Wählen Sie ein vertrauenswürdiges Programm aus der Liste der vertrauenswürdigen Programme.

b. Klicken Sie auf **Löschen**.

8. Klicken Sie im Fenster **Vertrauenswürdige Zone** auf **OK**.

9. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktivieren und Deaktivieren von Regeln der vertrauenswürdigen Zone für ein Programm aus der Liste der vertrauenswürdigen Programm

Um Regeln der vertrauenswürdigen Zone für ein Programm aus der Liste der vertrauenswürdigen Programm zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.

3. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Zone** auf **Einstellungen**.

   Es öffnet sich das Fenster **Vertrauenswürdige Zone**.

4. Wählen Sie im Fenster **Vertrauenswürdige Zone** die Registerkarte **Vertrauenswürdige Programme**.

5. Wählen Sie in der Liste der vertrauenswürdigen Programme das entsprechende vertrauenswürdige Programm aus.

6. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen neben dem Namen des vertrauenswürdigen Programms, das Sie aus der Untersuchung durch Kaspersky Endpoint Security ausschließen wollen.

   - Deaktivieren Sie das Kontrollkästchen neben dem Namen des vertrauenswürdigen Programms, das Sie zukünftig durch Kaspersky Endpoint Security untersuchen lassen wollen.

7. Klicken Sie auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Vertrauenswürdigen Zertifikatspeicher des Systems verwenden

Durch die Verwendung des Zertifikatspeichers des Systems können Programme, die eine vertrauenswürdige digitale Signatur besitzen, von der Untersuchung auf Viren ausgeschlossen werden.

Um mit der Verwendung des vertrauenswürdigen Zertifikatspeichers des Systems zu beginnen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.

3. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Zone** auf **Einstellungen**.

   Es öffnet sich das Fenster **Vertrauenswürdige Zone**.

4. Wählen Sie im Fenster **Vertrauenswürdige Zone** die Registerkarte **Vertrauenswürdiger Zertifikatspeicher des Systems**.

5. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdigen Zertifikatspeicher des Systems verwenden**.

6. Wählen Sie in der Dropdown-Liste **Vertrauenswürdiger Zertifikatspeicher des Systems**, welchen Systemspeicher Kaspersky Endpoint Security als vertrauenswürdig betrachten soll.

7. Klicken Sie im Fenster **Vertrauenswürdige Zone** auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Kontrolle des Netzwerkverkehrs

Dieser Abschnitt informiert über die Kontrolle des Netzwerkverkehrs und erklärt die Einstellungen für zu kontrollierendeNetzwerkports.

Über die Kontrolle des Netzwerkverkehrs

Während der Ausführung von Kaspersky Endpoint Security überwachen die Komponenten Schutz vor E-Mail-Bedrohungen und Schutz vor Web-Bedrohungen die Datenströme, die über bestimmte Protokolle und bestimmte offene TCP- und UDP-Ports des Benutzercomputers übertragen werden. So analysiert die Komponente Schutz vor E-Mail-Bedrohungen beispielsweise die Informationen, die per SMTP-Protokoll übertragen werden, während die Komponente Schutz vor Web-Bedrohungen die per HTTP- und FTP-Protokolle übertragenen Informationen analysiert.

Kaspersky Endpoint Security teilt TCP- und UDP-Ports des Betriebssystems je nach Angriffswahrscheinlichkeit in mehrere Gruppen ein. Netzwerkports, die für möglicherweise anfällige Dienste reserviert sind, sollten genauer überwacht werden, da für sie ein höheres Risiko besteht, Ziel eines Netzwerkangriffs zu werden. Wenn Sie außergewöhnliche Dienste verwenden, denen außergewöhnliche Netzwerkports zugewiesen sind, so können diese Netzwerkports angreifenden Computern ebenfalls als Ziel dienen. Sie können eine Liste der Netzwerkports und eine Liste der Programme erstellen, die Netzwerkzugriff erfragen, damit die Komponente Schutz vor E-Mail-Bedrohungen und die Komponente Schutz vor Web-Bedrohungen den entsprechenden Netzwerkverkehr besonders genau überwachen.

Kontrolleinstellungen für den Netzwerkverkehr anpassen

Zur Konfiguration der Kontrolleinstellungen für den Netzwerkverkehr stehen Ihnen die folgenden Aktionen zur Verfügung:

- Aktivieren der Kontrolle aller Netzwerkports

- Erstellen einer Liste der zu kontrollierenden Netzwerkports
- Erstellen einer Liste der Programme, für die alle Netzwerkports überwacht werden

Kontrolle aller Netzwerkports aktivieren

Gehen Sie folgendermaßen vor, um die Kontrolle aller Netzwerkports zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.
3. Wählen Sie im Block **Kontrollierte Ports** die Variante **Alle Netzwerkports kontrollieren** aus.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Liste der zu kontrollierenden Netzwerkports erstellen

Gehen Sie folgendermaßen vor, um eine Liste der zu kontrollierenden Netzwerkports zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.
3. Wählen Sie im Block **Kontrollierte Ports** die Variante **Nur ausgewählte Ports kontrollieren** aus.
4. Klicken Sie auf **Einstellungen**.

   Das Fenster **Netzwerkports** wird geöffnet. Im Fenster **Netzwerkports** befindet sich eine Liste der Netzwerkports, die normalerweise für die Übertragung von E-Mails und Netzwerkverkehr verwendet werden. Diese Liste mit Netzwerkports gehört zum Lieferumfang von Kaspersky Endpoint Security.
5. Führen Sie in der Liste der Netzwerkports folgende Schritte aus:
   - Aktivieren Sie die Kontrollkästchen für die Netzwerkports, die in die Liste der kontrollierten Netzwerkports aufgenommen werden sollen.

     Standardmäßig sind die Kontrollkästchen für alle Netzwerkports aktiviert, die im Fenster **Netzwerkports** genannt werden.
   - Deaktivieren Sie die Kontrollkästchen für die Netzwerkports, die aus der Liste der kontrollierten Netzwerkports ausgeschlossen werden sollen.
6. Gehen Sie folgendermaßen vor, um einen Netzwerkport zur Liste der Netzwerkports hinzuzufügen:
   a. Öffnen Sie mit dem Link **Hinzufügen**, der sich unter der Liste der Netzwerkports befindet, das Fenster **Netzwerkport**.

b. Geben Sie im Feld **Port** die Nummer des Netzwerkports an.

c. Geben Sie im Feld **Beschreibung** den Namen des Netzwerkports an.

d. Klicken Sie auf **OK**.

Das Fenster **Netzwerkport** wird geschlossen. Der von Ihnen hinzugefügte Netzwerkport wird am Ende der Liste der Netzwerkports angezeigt.

7. Klicken Sie im Fenster **Netzwerkports** auf **OK**.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Wenn der passive FTP-Modus verwendet wird, kann die Verbindung über einen beliebigen Netzwerkport hergestellt werden, der nicht auf der Liste der kontrollierten Ports steht. Zum Schutz solcher Verbindungen muss entweder im Abschnitt **Kontrollierte Ports** das Kontrollkästchen **Alle Netzwerkports kontrollieren** aktiviert werden oder die Überwachung aller Ports für Programme muss angepasst werden, mit denen eine FTP-Verbindung hergestellt wird.

Liste der Programme erstellen, für die alle Netzwerkports überwacht werden

Sie können eine Liste mit Programmen erstellen, für die Kaspersky Endpoint Security alle Netzwerkports kontrollieren soll.

Es wird empfohlen, in die Liste der Programme, für die Kaspersky Endpoint Security alle Netzwerkports kontrollieren soll, jene Programme aufzunehmen, die Daten über das FTP-Protokoll empfangen oder senden.

Gehen Sie folgendermaßen vor, um eine Liste der Programme anzulegen, für die alle Netzwerkports kontrolliert werden sollen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.

3. Wählen Sie im Block **Kontrollierte Ports** die Variante **Nur ausgewählte Ports kontrollieren** aus.

4. Klicken Sie auf **Einstellungen**.

   Das Fenster **Netzwerkports** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Alle Ports für die angegebenen Programme kontrollieren**.

6. Führen Sie in der Programmliste, die sich unter dem Kontrollkästchen **Alle Ports für die angegebenen Programme kontrollieren** befindet, folgende Schritte aus:

- Aktivieren Sie die Kontrollkästchen der Programme, für die alle Netzwerkports kontrolliert werden sollen.

  Standardmäßig sind die Kontrollkästchen für alle Programme aktiviert, die im Fenster **Netzwerkports** genannt werden.

- Deaktivieren Sie die Kontrollkästchen der Programme, für die nicht alle Netzwerkports kontrolliert werden sollen.

7. Wenn ein Programm nicht auf der Programmliste steht, können Sie es wie folgt hinzufügen:

   a. Öffnen Sie mit dem Link **Hinzufügen** unter der Programmliste das Kontextmenü.

   b. Wählen Sie im Kontextmenü eine Methode, mit der das Programm zur Programmliste hinzugefügt werden soll:

      - Wählen Sie den Punkt **Programme**, um ein Programm aus der Liste der auf dem Computer installierten Programme zu wählen. Das Fenster **Programm wählen** wird geöffnet. Dort können Sie den Namen eines Programms angeben.

      - Wählen Sie den Punkt **Durchsuchen**, um den Ort der ausführbaren Programmdatei anzugeben. Das Windows-Standardfenster **Öffnen** wird geöffnet. Dort können Sie den Namen der ausführbaren Programmdatei angeben.

      Nach der Auswahl eines Programms wird das Fenster **Programm** geöffnet.

   c. Geben Sie im Feld **Name** den Namen des gewählten Programms an.

   d. Klicken Sie auf **OK**.

      Das Fenster **Programm** wird geschlossen. Das hinzugefügte Programm erscheint am Ende der Programmliste.

8. Klicken Sie im Fenster **Netzwerkports** auf **OK**.

9. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Selbstschutz für Kaspersky Endpoint Security

Dieser Abschnitt informiert über den Selbstschutz-Mechanismus für Kaspersky Endpoint Security und über den Mechanismus zum Schutz vor externer Steuerung von Kaspersky Endpoint Security und erklärt die Einstellungen dieser Mechanismen.

Über den Selbstschutz für Kaspersky Endpoint Security

Kaspersky Endpoint Security bietet dem Computer Sicherheit vor schädlichen Programmen. Dazu zählen auch Schadprogramme, die versuchen, die Funktion von Kaspersky Endpoint Security zu blockieren oder das Programm zu deinstallieren.

Die Stabilität des Sicherheitssystems auf dem Benutzercomputer wird in Kaspersky Endpoint Security durch Mechanismen zum Selbstschutz und zum Schutz vor externer Steuerung gewährleistet.

Der *Selbstschutz-Mechanismus* verhindert, dass Dateien des Programms auf der Festplatte, Prozesse im Arbeitsspeicher und Einträge in der Systemregistrierung verändert oder gelöscht werden.

Der *Mechanismus zum Schutz vor externer Steuerung* kann alle Versuche, die Programmdienste von einem anderen Computer aus fernzusteuern, blockieren.

Für 64-Bit-Betriebssysteme steht der Selbstschutzmechanismus von Kaspersky Endpoint Security nur im Hinblick auf das Ändern oder Löschen von Programmdateien auf der Festplatte und das Ändern oder Löschen von Einträgen in der Systemregistrierung zur Verfügung.

Selbstschutz-Mechanismus aktivieren und deaktivieren

Der Selbstschutz-Mechanismus von Kaspersky Endpoint Security ist standardmäßig aktiviert. Bei Bedarf können Sie den Selbstschutz-Mechanismus ausschalten.

Gehen Sie folgendermaßen vor, um den Selbstschutz-Mechanismus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Programmeinstellungen** aus.

   Im rechten Fensterbereich werden die erweiterten Einstellungen für Kaspersky Endpoint Security angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Selbstschutz aktivieren**, um den Selbstschutz-Mechanismus einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Selbstschutz aktivieren**, um den Selbstschutz-Mechanismus auszuschalten.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Mechanismus zum Schutz vor externer Steuerung aktivieren und deaktivieren

Der Mechanismus zum Schutz vor externer Steuerung ist standardmäßig aktiviert. Bei Bedarf können Sie den Mechanismus zum Schutz vor externer Steuerung ausschalten.

Gehen Sie folgendermaßen vor, um den Mechanismus zum Schutz vor externer Steuerung zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Programmeinstellungen** aus.

Im rechten Fensterbereich werden die erweiterten Einstellungen für Kaspersky Endpoint Security angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Externe Steuerung von Systemdiensten deaktivieren**, um den Mechanismus zum Schutz vor externer Steuerung einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Externe Steuerung von Systemdiensten deaktivieren**, um den Mechanismus zum Schutz vor externer Steuerung auszuschalten.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Gewährleistung der Funktion von Programmen für Remote-Administration

Es kann vorkommen, dass Programme für Remote-Administration eingesetzt werden sollen, während der Schutz vor Fernsteuerung aktiviert ist.

Gehen Sie folgendermaßen vor, um Remote-Administrationsprogramme verwenden zu können:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.

3. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Zone** auf **Einstellungen**.

   Es öffnet sich das Fenster **Vertrauenswürdige Zone**.

4. Wählen Sie im Fenster **Vertrauenswürdige Zone** die Registerkarte **Vertrauenswürdige Programme**.
5. Klicken Sie auf **Hinzufügen**.
6. Führen Sie im Kontextmenü eine der folgenden Aktionen aus:

   - Wählen Sie den Punkt **Programme**, um aus der Liste der Programme, die auf dem Computer installiert sind, ein Remote-Verwaltungsprogramm zu wählen.

     Das Fenster **Programm wählen** wird geöffnet.

   - Wählen Sie den Punkt **Durchsuchen**, um den Pfad der ausführbaren Datei eines Remote-Verwaltungsprogramms anzugeben.

     Das Windows-Standardfenster **Öffnen** wird geöffnet.

7. Wählen Sie ein Programm. Dafür gibt es folgende Methoden:

   - Wenn Sie beim vorherigen Schritt den Punkt **Programme** gewählt haben, wählen Sie in der Liste der auf dem Computer installierten Programme ein Programm und klicken Sie im Fenster **Programm wählen** auf **OK**.

- Wenn Sie beim vorherigen Schritt den Punkt **Durchsuchen** gewählt haben, geben Sie den Pfad der ausführbaren Datei des entsprechenden Programms an und klicken Sie im Microsoft-Windows-Standardfenster **Öffnen** auf die Schaltfläche **Öffnen**.

Nach dem Abschluss dieser Schritte wird das Fenster **Untersuchungsausnahmen für das Programm** geöffnet.

8. Aktivieren Sie das Kontrollkästchen **Programmaktivität nicht kontrollieren**.

9. Klicken Sie im Fenster **Untersuchungsausnahmen für das Programm** auf **OK**.

   Das hinzugefügte vertrauenswürdige Programm erscheint in der Liste der vertrauenswürdigen Programme.

10. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Leistung von Kaspersky Endpoint Security und Kompatibilität mit anderen Programmen

Dieser Abschnitt informiert über die Leistung von Kaspersky Endpoint Security und über die Kompatibilität mit anderen Programmen. Außerdem wird erklärt, wie Sie den Typ der erkennbaren Objekte und den Funktionsmodus von Kaspersky Endpoint Security wählen können.

Über die Leistung von Kaspersky Endpoint Security und die Kompatibilität mit anderen Programmen

Leistung von Kaspersky Endpoint Security

Unter der Leistung von Kaspersky Endpoint Security sind die Anzahl der erkennbaren Objekttypen, die dem Computer Schaden zufügen können, sowie der Energieverbrauch und die benötigten Computerressourcen zu verstehen.

Erkennbare Objekttypen wählen

Kaspersky Endpoint Security erlaubt es, den Computerschutz flexibel anzupassen und die Objekttypen auszuwählen, die das Programm bei seiner Ausführung erkennen soll. Kaspersky Endpoint Security untersucht das Betriebssystem stets auf Viren, Würmer und trojanische Programme. Die Untersuchung dieser Objekttypen kann nicht deaktiviert werden. Diese Programme können dem Computer erheblichen Schaden zufügen. Um das Schutzniveau zu erhöhen, können Sie die Liste der erkennbaren Objekttypen erweitern. Aktivieren Sie dazu die Kontrolle der Aktionen legaler Programme, die von Angreifern zur Beschädigung des Computers und der Benutzerdaten genutzt werden können.

Energiesparmodus nutzen

Bei mobilen Computern ist der Energieverbrauch, der von Programmen verursacht wird, ein wichtiges Thema. Häufig beanspruchen die von Kaspersky Endpoint Security nach Zeitplan ausgeführten Aufgaben erhebliche Ressourcen. Läuft der Computer im Akkubetrieb, können Sie zur Gewährleistung einer längeren Akkulaufzeit den Energiesparmodus nutzen.

Der Energiesparmodus ermöglicht eine automatische Verschiebung von Aufgaben, für die ein Start nach Zeitplan festgelegt ist:

- Update-Aufgabe
- Aufgabe zur vollständigen Untersuchung
- Aufgabe zur Untersuchung wichtiger Bereiche
- Aufgabe zur benutzerdefinierten Untersuchung
- Aufgabe zur Integritätsprüfung

Unabhängig davon, ob der Energiesparmodus aktiviert ist oder nicht, hält Kaspersky Endpoint Security laufende Verschlüsselungsaufgaben an, wenn ein Laptop in den Batteriebetrieb wechselt. Wenn der Laptop aus dem Batteriebetrieb in den Netzbetrieb wechselt, setzt das Programm die Verschlüsselungsaufgaben fort.

Computerressourcen für andere Programme freigeben

Der von Kaspersky Endpoint Security verursachte Verbrauch von Computerressourcen kann sich auf die Leistung anderer Programme auswirken. Um Probleme zu vermeiden, die bei gleichzeitiger Verwendung mit anderen Programmen aufgrund erhöhter Auslastung des Prozessors und der Laufwerksubsysteme auftreten können, kann Kaspersky Endpoint Security die Ausführung geplanter Untersuchungsaufgaben anhalten und Ressourcen für andere Programme freigeben.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und im Hintergrundmodus arbeiten. Wenn die Untersuchung von der Ausführung solcher Programme unabhängig sein soll, sollten ihnen keine Betriebssystemressourcen überlassen werden.

Bei Bedarf können Sie diese Aufgaben auch manuell starten.

Technologie zur Desinfektion aktiver Infektionen nutzen

Moderne schädliche Programme können in die tiefste Ebene des Betriebssystems eindringen, wodurch es praktisch unmöglich wird, sie zu löschen. Bei Erkennen einer schädlichen Aktivität im Betriebssystem nimmt Kaspersky Endpoint Security eine erweiterte Desinfektion vor, wobei eine spezielle Technologie zur Desinfektion aktiver Infektionen zum Einsatz kommt. Die *Technologie zur Desinfektion aktiver Infektionen* dient dazu, schädliche Programme aus dem Betriebssystem zu entfernen, falls diese ihre Prozesse bereits im Arbeitsspeicher gestartet haben und Kaspersky Endpoint Security daran hindern, sie auf reguläre Weise zu neutralisieren. Dadurch wird die Bedrohung neutralisiert. Es wird davon abgeraten, während der aktiven Desinfektion neue Prozesse zu starten oder Änderungen an der Registrierung des Betriebssystems vorzunehmen. Die Technologie zur Desinfektion aktiver Infektionen beansprucht erhebliche Betriebssystemressourcen, wodurch die Ausführung anderer Programme verlangsamt werden kann.

Nachdem die aktive Desinfektion auf einem Computer mit Microsoft Windows Workstation abgeschlossen wurde, fragt Kaspersky Endpoint Security den Benutzer um Erlaubnis für einen Neustart des Computers. Nach dem Neustart des Computers löscht Kaspersky Endpoint Security die Schadsoftware-Dateien und startet eine vereinfachte vollständige Untersuchung des Computers.

Auf einem Computer mit Microsoft Windows für Dateiserver ist eine Abfrage für den Neustart des Computers nicht möglich. Dies ist durch Besonderheiten des Programms Kaspersky Endpoint Security für

Dateiserver bedingt. Ein ungeplanter Neustart des Dateiservers kann zu Problemen führen. Es kann zu einer vorübergehenden Nichtverfügbarkeit der Dateiserverdaten oder zum Verlust von nicht gespeicherten Daten kommen. Es wird empfohlen, den Neustart eines Dateiservers streng nach Zeitplan auszuführen. Aus diesem Grund ist die Technologie zur aktiven Desinfektion für Dateiserver standardmäßig deaktiviert.

Wird auf einem Dateiserver eine aktive Infektion erkannt, so wird ein Ereignis an Kaspersky Security Center gesendet, das über die Notwendigkeit einer aktiven Desinfektion informiert. Damit auf einem Dateiserver eine aktive Desinfektion möglich ist, muss die Technologie zur aktiven Desinfektion für Dateiserver aktiviert sein und die Gruppenaufgabe *Virensuche* gestartet werden. Dafür sollte ein für die Benutzer des Dateiservers günstiger Zeitpunkt gewählt werden.

Erkennbare Objekttypen wählen

Gehen Sie folgendermaßen vor, um die Typen der erkennbaren Objekte zu wählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Ausnahmen** aus.

   Im rechten Fensterbereich werden die Einstellungen für Ausnahmen angezeigt.
3. Klicken Sie im Block **Zu erkennende Objekte** auf **Einstellungen**.

   Das Fenster **Zu erkennende Objekte** wird geöffnet.
4. Aktivieren Sie die Kontrollkästchen für die Objekttypen, die Kaspersky Endpoint Security erkennen soll:
   - **Schädliche Tools**
   - **Adware**
   - **Dialer**
   - **Andere**
   - **Gepackte Dateien, die Schaden verursachen können**
   - **Mehrfach gepackte Dateien**
5. Klicken Sie auf **OK**.

   Das Fenster **Zu erkennende Objekte** wird geschlossen. Im Abschnitt **Zu erkennende Objekte** werden unter **Die Erkennung folgender Objekttypen ist aktiviert** die von Ihnen ausgewählten Objekttypen angezeigt.
6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Technologie zur aktiven Desinfektion für Workstations aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um die Technologie zur aktiven Desinfektion für Workstations zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Programmeinstellungen** aus.

   Im rechten Fensterbereich werden die erweiterten Einstellungen für Kaspersky Endpoint Security angezeigt.

3. Führen Sie im rechten Fensterbereich eine der folgenden Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**, um die Technologie zur aktiven Desinfektion einzuschalten.

   - Deaktivieren Sie das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**, um die Technologie zur aktiven Desinfektion auszuschalten.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Wenn die Aufgabe zur aktiven Desinfektion über Kaspersky Security Center gestartet wird, steht dem Benutzer nur eine eingeschränkte Auswahl der Betriebssystemfunktionen zur Verfügung. Nach Abschluss der Aufgabe wird die Workstation neu gestartet.

Technologie zur aktiven Desinfektion für Dateiserver aktivieren und deaktivieren

Um die Technologie zur aktiven Desinfektion für Dateiserver zu aktivieren, führen Sie eine der folgenden Aktionen aus:

- Aktivieren Sie die Technologie zur aktiven Desinfektion in den Eigenschaften der aktiven Richtlinie für Kaspersky Security Center. Gehen Sie dazu folgendermaßen vor:

  a. Öffnen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Programmeinstellungen**.

  b. Aktivieren Sie das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**.

  c. Klicken Sie im Eigenschaftenfenster der Richtlinie auf **OK**, um die vorgenommenen Änderungen zu speichern.

- Aktivieren Sie in den Eigenschaften der Gruppenaufgabe für Kaspersky Security Center "Virensuche" das Kontrollkästchen **Aktive Desinfektion sofort ausführen**.

Führen Sie eine der folgenden Aktionen aus, um die Technologie zur aktiven Desinfektion für Dateiserver zu deaktivieren:

- Deaktivieren Sie die Technologie zur aktiven Desinfektion in den Eigenschaften der Richtlinie für Kaspersky Security Center. Gehen Sie dazu folgendermaßen vor:

a. Öffnen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Programmeinstellungen**.

b. Deaktivieren Sie das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**.

c. Klicken Sie im Eigenschaftenfenster der Richtlinie auf **OK**, um die vorgenommenen Änderungen zu speichern.

- Deaktivieren Sie in den Eigenschaften der Gruppenaufgabe für Kaspersky Security Center "Virensuche" das Kontrollkästchen **Aktive Desinfektion sofort ausführen**.

Energiesparmodus aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um den Energiesparmodus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Programmeinstellungen** aus.

   Im rechten Fensterbereich werden die erweiterten Einstellungen für Kaspersky Endpoint Security angezeigt.

3. Gehen Sie im Abschnitt **Leistung** wie folgt vor:

   - Aktivieren Sie das Kontrollkästchen **Geplante Aufgaben bei Akkubetrieb aufschieben**, um den Energiesparmodus zu aktivieren.

     Ist der Energiesparmodus aktiviert, so werden bei Akkubetrieb folgende Aufgaben auch dann nicht gestartet, wenn ein Startzeitplan dafür vorhanden ist:

     - Update-Aufgabe
     - Aufgabe zur vollständigen Untersuchung
     - Aufgabe zur Untersuchung wichtiger Bereiche
     - Aufgabe zur benutzerdefinierten Untersuchung
     - Aufgabe zur Integritätsprüfung

   - Deaktivieren Sie das Kontrollkästchen **Geplante Aufgaben bei Akkubetrieb aufschieben**, um den Energiesparmodus zu deaktivieren. In diesem Fall führt Kaspersky Endpoint Security geplante Aufgaben aus, ohne die Stromversorgungsquelle des Computers zu berücksichtigen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Freigabe von Ressourcen für andere Programme aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um den Modus zu aktivieren oder zu deaktivieren, in dem Ressourcen für andere Programme freigegeben werden:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Programmeinstellungen** aus.

   Im rechten Fensterbereich werden die erweiterten Einstellungen für Kaspersky Endpoint Security angezeigt.

3. Gehen Sie im Abschnitt **Leistung** wie folgt vor:

   - Aktivieren Sie das Kontrollkästchen **Ressourcen für andere Programme freigeben**, um den Modus zu aktivieren, in dem Ressourcen für andere Programme freigegeben werden.

     Ist der Modus zur Freigabe von Ressourcen für andere Programme aktiviert, schiebt Kaspersky Endpoint Security die Ausführung von Aufgaben auf, wenn sie nach Zeitplan gestartet werden sollen und ihre Ausführung andere Programme verlangsamt:

     - Update-Aufgabe
     - Aufgabe zur vollständigen Untersuchung
     - Aufgabe zur Untersuchung wichtiger Bereiche
     - Aufgabe zur benutzerdefinierten Untersuchung
     - Aufgabe zur Integritätsprüfung

   - Deaktivieren Sie das Kontrollkästchen **Ressourcen für andere Programme freigeben**, um den Modus zu deaktivieren, in dem Ressourcen für andere Programme freigegeben werden. In diesem Fall führt Kaspersky Endpoint Security geplante Aufgaben aus, ohne andere Programme zu berücksichtigen.

   Der Modus zur Freigabe von Ressourcen für andere Programme ist standardmäßig aktiviert.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Kennwortschutz

Dieser Abschnitt informiert darüber, wie der Zugriff auf Kaspersky Endpoint Security mit einem Kennwort beschränkt werden kann.

Über die Beschränkung des Zugriffs auf Kaspersky Endpoint Security

Es kann sein, dass ein Computer von mehreren Benutzern verwendet wird, deren Fertigkeiten im Umgang mit Computern sich unterscheiden. Der uneingeschränkte Zugriff der Benutzer auf Kaspersky Endpoint Security und dessen Einstellungen kann das Sicherheitsniveau des Computers insgesamt beeinträchtigen.

Um den Zugriff auf Kaspersky Endpoint Security zu beschränken, können Sie einen Benutzernamen und ein Kennwort festlegen, und die Vorgänge festlegen, für die das Programm diese Daten abfragen soll:

Beim Programm-Upgrade auf Kaspersky Endpoint Security 11 für Windows wird ein zuvor festgelegtes Kennwort beibehalten. Um die Einstellungen für den Kennwortschutz zum ersten Mal zu ändern, muss der standardmäßige Benutzername KLAdmin verwendet werden.

Kennwortschutz aktivieren und deaktivieren

Es empfiehlt sich, bei der Verwendung von Kennwörtern zur Beschränkung des Zugriffs auf das Programm Vorsicht walten zu lassen. Sollten Sie das Kennwort vergessen haben, so wenden Sie sich an den Technischen Support von Kaspersky Lab und fragen Sie nach einer Anleitung zum Aufheben des Kennwortschutzes.

Um den Kennwortschutz zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Benutzeroberfläche** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Benutzeroberfläche von Kaspersky Endpoint Security angezeigt.
3. Klicken Sie im Abschnitt **Kennwortschutz** auf **Einstellungen**.

   Das Fenster **Kennwortschutz** wird geöffnet.
4. Aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren**.
5. Geben Sie im Feld **Benutzername** den Benutzernamen ein, der im Fenster **Kennwortprüfung** angegeben werden muss, wenn künftig kennwortgeschützte Vorgänge ausgeführt werden sollen.
6. Geben Sie im Feld **Neues Kennwort** das Kennwort für den Zugriff auf das Programm ein.
7. Wiederholen Sie das Kennwort im Feld **Kennwort bestätigen**.
8. Um den Zugriff für alle Vorgänge mit dem Programm zu beschränken, klicken Sie im Abschnitt **Gültigkeitsbereich des Kennworts** auf **Alle auswählen**.
9. Um den Zugriff des Benutzers nur für bestimmte Vorgänge zu beschränken, aktivieren Sie im Abschnitt **Gültigkeitsbereich des Kennworts** die Kontrollkästchen für die entsprechenden Vorgänge:
   - Programmeinstellungen anpassen
   - Programm beenden
   - Schutzkomponenten deaktivieren
   - Kontrollkomponenten deaktivieren
   - Schlüssel löschen

- Programm entfernen / ändern / reparieren
- Zugriffswiederherstellung für Daten auf verschlüsselten Geräten
- Berichte anzeigen.

10. Klicken Sie auf **OK**.

    Das Programm überprüft die eingegebenen Kennwörter. Stimmen die Kennwörter überein, so übernimmt das Programm dieses Kennwort. Falls die Kennwörter nicht identisch sind, werden Sie vom Programm aufgefordert, das Kennwort erneut im Feld **Kennwort bestätigen** einzugeben.

11. Klicken Sie im Programmkonfigurationsfenster auf **Speichern**, um die vorgenommenen Änderungen zu speichern.

Nachdem der Kennwortschutz aktiviert wurde, fragt das Programm jedes Mal nach dem Kennwort, wenn ein Vorgang ausgeführt werden soll, der in den Gültigkeitsbereich des Kennworts fällt. Sie können das Kontrollkästchen **Kennwort für diese Sitzung speichern** im Fenster **Kennwortprüfung** aktivieren, damit das Programm während der laufenden Sitzung nicht mehr nach dem Kennwort fragt, wenn ein geschützter Vorgang ausgeführt wird.

Ist das Kontrollkästchen **Kennwort für diese Sitzung speichern** deaktiviert, so fragt das Programm jedes Mal das Kennwort ab, wenn versucht wird, einen geschützten Vorgang auszuführen.

Um den Kennwortschutz zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Benutzeroberfläche** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Benutzeroberfläche von Kaspersky Endpoint Security angezeigt.
3. Klicken Sie im Abschnitt **Kennwortschutz** auf **Einstellungen**.

   Das Fenster **Kennwortschutz** wird geöffnet.
4. Deaktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren**.
5. Klicken Sie auf **OK**.
6. Klicken Sie im Programmkonfigurationsfenster auf **Speichern**, um die vorgenommenen Änderungen zu speichern.

   Das Fenster **Kennwortprüfung** wird geöffnet.
7. Tragen Sie im Feld **Benutzername** den Benutzernamen ein.
8. Tragen Sie im Feld **Kennwort** das Kennwort für den Zugriff auf Kaspersky Endpoint Security ein.
9. Klicken Sie auf **OK**.

Kennwort für den Zugriff auf Kaspersky Endpoint Security ändern

Gehen Sie folgendermaßen vor, um das Kennwort für den Zugriff auf Kaspersky Endpoint Security zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Benutzeroberfläche** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Benutzeroberfläche von Kaspersky Endpoint Security angezeigt.
3. Klicken Sie im Abschnitt **Kennwortschutz** auf **Einstellungen**.

   Das Fenster **Kennwortschutz** wird geöffnet.
4. Tragen Sie im Feld **Benutzername** den Benutzernamen ein.
5. Geben Sie im Feld **Neues Kennwort** das neue Kennwort für den Zugriff auf das Programm ein.
6. Wiederholen Sie das neue Kennwort im Feld **Kennwort bestätigen**.
7. Klicken Sie auf **OK**.

   Das Programm überprüft die eingegebenen Kennwörter. Wenn die Kennwörter übereinstimmen, wird das neue Kennwort übernommen und das Fenster **Kennwortschutz** wird geschlossen. Falls die Kennwörter nicht identisch sind, werden Sie vom Programm aufgefordert, das Kennwort erneut im Feld **Kennwort bestätigen** einzugeben.
8. Klicken Sie im Programmkonfigurationsfenster auf **Speichern**, um die vorgenommenen Änderungen zu speichern.

   Das Fenster **Kennwortprüfung** wird geöffnet.
9. Tragen Sie im Feld **Benutzername** den Benutzernamen ein.
10. Tragen Sie im Feld **Kennwort** das alte Kennwort für den Zugriff auf Kaspersky Endpoint Security ein.
11. Klicken Sie auf **OK**.

Über die Verwendung eines temporären Kennworts

Bei der Arbeit auf Client-Computern, die einer Richtlinie für Kaspersky Security Center unterliegen, kann es vorkommen, dass die Benutzer mit dem Programm Kaspersky Endpoint Security Vorgänge ausführen müssen, die auf Richtlinienebene durch ein Kennwort geschützt sind. Ist der Kennwortschutz aktiviert, so kann nur der Administrator für Kaspersky Security Center kennwortgeschützte Vorgänge ausführen. Sobald aber keine Verbindung mit Kaspersky Security Center besteht (wenn sich der Benutzer z. B. außerhalb des Unternehmensnetzwerks befindet), so ist die Verwendung der lokalen Benutzeroberfläche von Kaspersky Endpoint Security beschränkt.

Um dem Benutzer zu ermöglichen, die erforderlichen Vorgänge auszuführen, ohne dabei das in den Richtlinieneinstellungen hinterlegte Kennwort zu nennen, kann der Administrator für Kaspersky Security Center ein temporäres Kennwort erstellen. Die Gültigkeit eines temporären Kennworts ist zeitlich und im Hinblick auf den Gültigkeitsbereich beschränkt. Nachdem das temporäre Kennwort auf der lokalen Benutzeroberfläche des Programms eingegeben wurde, werden die Vorgänge freigegeben, die der Administrator für Kaspersky Security Center erlaubt hat.

Nach Ablauf des temporären Kennworts richtet sich Kaspersky Endpoint Security wieder nach den Einstellungen der Richtlinie für Kaspersky Security Center. Der Benutzer kann die Vorgänge nicht mehr ausführen, die auf Richtlinienebene durch ein Kennwort geschützt sind.

Temporäres Kennwort mithilfe der Verwaltungskonsole von Kaspersky Security Center erstellen

Um ein temporäres Kennwort zu erstellen und an den Benutzer zu übermitteln, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der Computer des Benutzers gehört, der ein temporäres Kennwort angefordert hat.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Wählen Sie im Kontextmenü des Computers des Benutzers, der ein temporäres Kennwort angefordert hat, den Punkt **Eigenschaften**.

   Das Fenster **Eigenschaften: <Computername>** wird geöffnet.
5. Wählen Sie im Fenster **Eigenschaften: <Computername>** den Abschnitt **Programme**.
6. Wählen Sie **Kaspersky Endpoint Security für Windows** aus und öffnen Sie das Fenster mit den Programmeigenschaften. Dafür gibt es folgende Methoden:
   - Klicken Sie am unteren Bildschirmrand auf **Eigenschaften**.
   - Wählen Sie im Kontextmenü des Programms den Punkt **Eigenschaften**.

   Das Fenster **Programmeinstellungen "<Programmname>"** wird geöffnet.
7. Wählen Sie im Fenster **Programmeinstellungen "<Programmname>"** im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Benutzeroberfläche** aus.
8. Klicken Sie im Abschnitt **Kennwortschutz** auf **Einstellungen**.

   Das Fenster **Kennwortschutz** wird geöffnet.
9. Klicken Sie im Fenster **Kennwortschutz** im Abschnitt **Temporäres Kennwort** auf **Einstellungen**.

   Die Schaltfläche ist verfügbar, wenn in der Richtlinie für Kaspersky Security Center, welcher der Computer unterliegt, der Kennwortschutz für das Programm Kaspersky Endpoint Security

aktiviert ist.

Das Fenster **Temporäres Kennwort erstellen** wird geöffnet.

10. Legen Sie im Feld **Ablaufdatum** das Datum fest, bis zu dem der Benutzer das temporäre Kennwort verwenden kann.

    Nach diesem Datum wird das temporäre Kennwort ungültig. Um die Freigabe abzuschließen, muss auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security ein neues temporäres Kennwort erstellt werden.

11. Aktivieren Sie in der Tabelle **Gültigkeitsbereich des temporären Kennworts** die Kontrollkästchen für jene Vorgänge, auf welche der Benutzer während der Gültigkeitsdauer des temporären Kennworts zugreifen kann.

12. Klicken Sie auf die Schaltfläche **Erstellen**.

    Das Fenster **Temporäres Kennwort** mit einem verschlüsselten Kennwort wird geöffnet.

13. Kopieren Sie das Kennwort und übertragen Sie es zusammen mit den Verwendungshinweisen an den Benutzer.

Konfigurationsdatei erstellen und verwenden

Mithilfe der Konfigurationsdatei für die Einstellungen von Kaspersky Endpoint Security lassen sich folgende Aufgaben lösen:

- Ausführen einer lokalen Installation von Kaspersky Endpoint Security über die Befehlszeile mit zuvor festgelegten Einstellungen.

  Dazu muss die Konfigurationsdatei im gleichen Ordner gespeichert werden, in dem sich das Programmpaket befindet.

- Ausführen einer Remote-Installation von Kaspersky Endpoint Security über Kaspersky Security Center mit zuvor festgelegten Einstellungen.

- Einstellungen für Kaspersky Endpoint Security von einem Computer auf einem anderen übertragen.

Um eine Konfigurationsdatei zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Einstellungen verwalten**.

   Im rechten Fensterbereich werden die Funktionen der Konfigurationsverwaltung angezeigt.

3. Klicken Sie im Block **Einstellungen verwalten** auf **Speichern**.

   Das standardmäßige Microsoft-Windows-Fenster **Konfigurationsdatei wählen** wird geöffnet.

4. Geben Sie den Pfad an, unter dem die Konfigurationsdatei gespeichert werden soll, und legen Sie einen Dateinamen fest.

Um eine Konfigurationsdatei für die lokale Installation oder für die Remote-Installation von Kaspersky Endpoint Security zu verwenden, muss die Datei install.cfg genannt werden.

5. Klicken Sie auf **Speichern**.

Um die Einstellungen für Kaspersky Endpoint Security aus einer Konfigurationsdatei zu importieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Einstellungen verwalten**.

   Im rechten Fensterbereich werden die Funktionen der Konfigurationsverwaltung angezeigt.
3. Klicken Sie im Block **Einstellungen verwalten** auf **Laden**.

   Das standardmäßige Microsoft-Windows-Fenster **Konfigurationsdatei wählen** wird geöffnet.
4. Geben Sie den Pfad der Konfigurationsdatei an.
5. Klicken Sie auf **Öffnen**.

Alle Werte für die Einstellungen von Kaspersky Endpoint Security werden gemäß der ausgewählten Konfigurationsdatei festgelegt.

Programm über Kaspersky Security Center verwalten

Dieser Abschnitt informiert über die Verwaltung des Programms Kaspersky Endpoint Security über Kaspersky Security Center.

Über die Verwaltung des Programms mit Kaspersky Security Center

Mit Kaspersky Security Center können folgende Funktionen ferngesteuert werden: Kaspersky Endpoint Security installieren und entfernen, starten und beenden; Programmeinstellungen anpassen, Auswahl der Programmkomponenten ändern, Schlüssel hinzufügen, Update- und Untersuchungsaufgaben starten.

Der Abschnitt über die Programmkontrolle bietet Informationen über die Verwaltung von Regeln der Programmkontrolle mithilfe von Kaspersky Security Center.

Weitere Informationen zur Programmverwaltung über Kaspersky Security Center, welche nicht in dieser Hilfe enthalten sind, finden Sie im Administratorhandbuch zu Kaspersky Security Center.

Das Programm Kaspersky Security Center wird mithilfe des Verwaltungs-Plug-ins von Kaspersky Endpoint Security verwaltet.

Die Version des Verwaltungs-Plug-ins kann sich von der Version von Kaspersky Endpoint Security unterscheiden, die auf dem Client-Computer installiert ist. Verfügt die installierte Version des Verwaltungs-Plug-ins über weniger Funktionen als die installierte Version von Kaspersky Endpoint Security, so werden die fehlenden Funktionen nicht mit dem Verwaltungs-Plug-in verwaltet. Solche Einstellungen können vom Benutzer auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security geändert werden.

Besonderheiten für die Verwendung unterschiedlicher Versionen des Verwaltungs-Plug-ins

Mithilfe des Verwaltungs-Plug-ins können Sie die folgenden Elemente ändern:

- Richtlinien
- Richtlinienprofile
- Gruppenaufgaben
- lokalen Aufgaben
- lokale Einstellungen des Programms Kaspersky Endpoint Security

Um das Programm Kaspersky Endpoint Security über Kaspersky Security Center zu verwalten, ist das Verwaltungs-Plug-in erforderlich. Die Version des Plug-ins muss gleich oder höher sein, wie in den Informationen zur Kompatibilität von Kaspersky Endpoint Security und dem Verwaltungs-Plug-in angegeben. Die mindestens erforderliche Version des Verwaltungs-Plug-ins können Sie der Datei installer.ini entnehmen, die zum Lieferumfang gehört.

Wenn ein beliebiges Element geöffnet wird, überprüft das Verwaltungs-Plug-in die Kompatibilitätsinformationen. Wenn die Version des Verwaltungs-Plug-ins mit der in den Kompatibilitätsinformationen angegeben Version übereinstimmt oder höher ist, können Sie die Einstellungen dieses Elements ändern. Andernfalls kann das gewählte Element mithilfe des Verwaltungs-Plug-ins nicht geändert werden. Es wird empfohlen, das Verwaltungs-Plug-in zu aktualisieren.

Früher festgelegte Einstellungen mithilfe mit einer neueren Version des Verwaltungs-Plug-ins ändern

Mithilfe einer neueren Version des Verwaltungs-Plug-ins können Sie alle früher festgelegten Einstellungen ändern und neue Einstellungen anpassen, die in einer früher verwendeten Version des Verwaltungs-Plug-ins noch nicht vorhanden waren.

Für neue Einstellungen legt die neuere Version des Verwaltungs-Plug-ins Standardwerte fest, wenn eine Richtlinie, ein Richtlinienprofil oder eine Aufgabe zum ersten Mal gespeichert wird.

Nachdem Sie die Einstellungen einer Richtlinie, eines Richtlinienprofils oder einer Gruppenaufgabe mithilfe einer neueren Version des Verwaltungs-Plug-ins geändert haben, sind diese Elemente für ältere Versionen des Verwaltungs-Plug-ins nicht mehr verfügbar. Die lokalen Einstellungen des Programms Kaspersky Endpoint Security und die Einstellungen für lokale Aufgaben stehen weiterhin für ältere Versionen des Verwaltungs-Plug-ins zur Verfügung.

Kaspersky Endpoint Security auf Client-Computern starten und beenden

Um das Programm auf einem Client-Computer zu starten oder zu beenden, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Wählen Sie den Computer, auf dem Sie das Programm starten oder beenden möchten.
5. Öffnen Sie durch Rechtsklick das Kontextmenü des Client-Computers und wählen Sie den Punkt **Eigenschaften**.

   Das Eigenschaftenfenster des Client-Computers wird geöffnet.
6. Wählen Sie im Eigenschaftenfenster des Client-Computers den Abschnitt **Programme**.

   Im rechten Teil des Eigenschaftenfensters des Client-Computers wird eine Liste der auf dem Client-Computer installierten Kaspersky-Lab-Programme angezeigt.
7. Wählen Sie das Programm Kaspersky Endpoint Security für Windows aus.
8. Gehen Sie wie folgt vor:

   - Wenn Sie das Programm starten möchten, klicken Sie rechts von der Liste der Kaspersky-Lab-Programme auf die Schaltfläche oder gehen Sie wie folgt vor:

     a. Wählen Sie im Kontextmenü des Programms Kaspersky Endpoint Security den Punkt **Eigenschaften** oder klicken Sie auf die Schaltfläche **Eigenschaften**, die sich unter der Liste der Kaspersky-Lab-Programme befindet.

     Das Fenster **Programmeinstellungen "Kaspersky Endpoint Security für Windows (11.0.0)"** wird geöffnet.

     b. Klicken Sie im rechten Fensterbereich im Abschnitt **Allgemein** auf **Start**.

   - Wenn Sie das Programm beenden möchten, klicken Sie rechts von der Liste der Kaspersky-Lab-Programme auf die Schaltfläche oder gehen Sie wie folgt vor:

     a. Wählen Sie im Kontextmenü des Programms Kaspersky Endpoint Security den Punkt **Eigenschaften** oder klicken Sie auf die Schaltfläche **Eigenschaften**, die sich unter der Liste der Kaspersky-Lab-Programme befindet.

     Das Fenster **Programmeinstellungen "Kaspersky Endpoint Security für Windows (11.0.0)"** wird geöffnet.

     b. Klicken Sie im rechten Fensterbereich im Abschnitt **Allgemein** auf **Beenden**.

Kaspersky Endpoint Security konfigurieren

Gehen Sie folgendermaßen vor, um die Einstellungen von Kaspersky Endpoint Security zu konfigurieren:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Wählen Sie den Computer, für den Sie Kaspersky Endpoint Security anpassen möchten.
5. Wählen Sie im Kontextmenü des Client-Computers den Punkt **Eigenschaften** aus.

   Das Eigenschaftenfenster des Client-Computers wird geöffnet.
6. Wählen Sie im Eigenschaftenfenster des Client-Computers den Abschnitt **Programme**.

   Im rechten Teil des Eigenschaftenfensters des Client-Computers wird eine Liste der auf dem Client-Computer installierten Kaspersky-Lab-Programme angezeigt.
7. Wählen Sie das Programm Kaspersky Endpoint Security für Windows aus.
8. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie im Kontextmenü des Programms Kaspersky Endpoint Security für Windows den Punkt **Eigenschaften** aus.
   - Klicken Sie unter der Liste der Kaspersky-Lab-Programme auf **Eigenschaften**.

   Das Fenster **Programmeinstellungen "Kaspersky Endpoint Security für Windows"** wird geöffnet.
9. Passen Sie im Abschnitt **Allgemeine Einstellungen** die Einstellungen von Kaspersky Endpoint Security sowie die Einstellungen für Berichte und Speicher an.

   Die übrigen Abschnitte des Fensters **Programmeinstellungen "Kaspersky Endpoint Security für Windows"** sind für das Programm Kaspersky Security Center standardmäßig. Eine Beschreibung dieser Abschnitte finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

   > Wurde für das Programm eine Richtlinie erstellt, durch die eine Änderung bestimmter Einstellungen untersagt ist, so können diese Einstellungen nicht geändert werden, während die Programmeinstellungen im Abschnitt **Allgemeine Einstellungen** angepasst werden.
10. Um die vorgenommenen Änderungen zu speichern, klicken Sie im Fenster **Programmeinstellungen "Kaspersky Endpoint Security Windows"** auf **OK**.

Aufgabenverwaltung

Dieser Abschnitt informiert über die Verwaltung von Aufgaben für Kaspersky Endpoint Security. Weitere Informationen zum Konzept der Aufgabenverwaltung über Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Über Aufgaben für Kaspersky Endpoint Security

Kaspersky Security Center verwaltet die Kaspersky-Lab-Programme, die auf den Client-Computern installiert sind, mithilfe von Aufgaben. Anhand der Aufgaben werden die wichtigsten Verwaltungsfunktionen umgesetzt, wie beispielsweise Hinzufügen eines Schlüssels, Untersuchung des Computers, und Aktualisierung der Datenbanken und Programm-Module.

Für die Arbeit mit Kaspersky Endpoint Security über Kaspersky Security Center können Sie folgende Aufgabentypen erstellen:

- lokale Aufgaben für einen einzelnen Client-Computer
- Gruppenaufgaben für Client-Computer, die zu Administrationsgruppen gehören
- Aufgaben für bestimmte Computer, die nicht zu Administrationsgruppen gehören

> Aufgaben für bestimmte Computer, die nicht zu Administrationsgruppen gehören, werden nur für jene Client-Computer ausgeführt, die in den Aufgabeneinstellungen angegeben sind. Werden der Gruppe von Computern, für welche die Aufgabe erstellt wurde, neue Client-Computer hinzugefügt, wird die Aufgabe für diese nicht ausgeführt. In diesem Fall muss entweder eine neue Aufgabe erstellt werden oder die Einstellungen der bestehenden Aufgabe müssen geändert werden.

Für die Remote-Verwaltung des Programms Kaspersky Endpoint Security können Sie eine der folgenden Aufgaben verwenden. Die Aufgabe kann einen beliebigen aufgezählten Typ besitzen:

- **Schlüssel hinzufügen**. Kaspersky Endpoint Security fügt einen Schlüssel zur Programmaktivierung bzw. einen Reserveschlüssel hinzu.
- **Auswahl der Programmkomponenten ändern**. Kaspersky Endpoint Security installiert oder löscht Komponenten auf den Client-Computern. Dabei wird nach der Komponentenliste verfahren, die in den Aufgabeneinstellungen angegeben ist.
- **Inventarisierung**. Kaspersky Endpoint Security erhält Informationen über alle ausführbaren Programmdateien, die auf dem Computer gespeichert sind.

  Sie können die Inventarisierung von DLL-Modulen und Skriptdateien aktivieren. In diesem Fall erhält Kaspersky Security Center Informationen über DLL-Module, die auf einem Computer geladen sind, auf dem Kaspersky Endpoint Security installiert ist, und Informationen über Dateien, die Skripte enthalten.

  > Wenn die Inventarisierung von DLL-Modulen und Skriptdateien aktiviert ist, erhöhen sich die Ausführungsdauer der Inventarisierungsaufgabe und die Datenbankgröße wesentlich.

  > Falls auf einem Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, die Komponente Programmkontrolle nicht vorhanden ist, so wird die Inventarisierungsaufgabe auf diesem Computer mit einem Fehler abgeschlossen.

- **Update**. Kaspersky Endpoint Security aktualisiert die Datenbanken und Programm-Module gemäß den festgelegten Update-Einstellungen.
- **Update-Rollback**. Kaspersky Endpoint Security setzt das letzte Update der Datenbanken und Module zurück.
- **Virensuche**. Kaspersky Endpoint Security untersucht die Computerbereiche, die in den Aufgabeneinstellungen angegeben sind, auf Viren und andere bedrohliche Programme.
- **KSN-Verfügbarkeit überprüfen**. Kaspersky Endpoint Security sendet eine Anfrage zur Verfügbarkeit der KSN-Server und aktualisiert den KSN-Verbindungsstatus.
- **Integritätsprüfung**. Kaspersky Endpoint Security erhält Daten über die Auswahl der Programm-Module, die auf dem Client-Computer installiert sind, und überprüft die digitale Signatur der einzelnen Module.
- **Authentifizierungsagenten-Konten verwalten**. Bei dieser Aufgabe werden von Kaspersky Endpoint Security Befehle zum Löschen, Hinzufügen und Ändern von Authentifizierungsagenten-Benutzerkonten erstellt.

Für Aufgaben stehen folgende Aktionen zur Verfügung:

- Starten, Beenden, Anhalten und Fortsetzen von Aufgaben
- neue Aufgaben erstellen
- Aufgabeneinstellungen ändern

Die Rechte für den Zugriff auf die Einstellungen der Aufgaben von Kaspersky Endpoint Security (Lesen, Ändern, Ausführen) werden für jeden Benutzer festgelegt, der Zugriff auf den Administrationsserver für Kaspersky Security Center besitzt. Die Rechte werden über die Einstellungen für den Zugriff auf die Funktionsbereiche von Kaspersky Endpoint Security zugeteilt. Um den Zugriff auf die Einstellungen für die Funktionsbereiche von Kaspersky Endpoint Security anzupassen, gehen Sie im Eigenschaftenfenster des Administrationsservers für Kaspersky Security Center zum Abschnitt **Sicherheit**.

Modus für die Verwendung von Aufgaben anpassen

Um den Modus anzupassen, in dem Aufgaben auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security verwendet werden, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie den Verwendungsmodus für Aufgaben auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security anpassen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die entsprechende Richtlinie.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:
    - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.

- Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

6. Wählen Sie im Abschnitt **Lokale Aufgaben** den Unterabschnitt **Aufgabenverwaltung** aus.

7. Gehen Sie im Block **Aufgabenverwaltung** wie folgt vor:

   - Um den Benutzern die Verwendung lokaler Aufgaben auf der Benutzeroberfläche und in der Befehlszeile von Kaspersky Endpoint Security zu erlauben, aktivieren Sie das Kontrollkästchen **Verwendung lokaler Aufgaben erlauben**.

     Ist dieses Kontrollkästchen deaktiviert, so können lokale Aufgaben nicht ausgeführt werden. In diesem Modus werden lokale Aufgaben nicht nach Zeitplan gestartet. Außerdem können lokale Aufgaben auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security und bei Verwendung der Befehlszeile nicht gestartet oder geändert werden.

   - Um den Benutzern zu erlauben, eine Liste mit Gruppenaufgaben anzuzeigen, aktivieren Sie das Kontrollkästchen **Anzeige von Gruppenaufgaben erlauben**.

   - Um den Benutzern zu erlauben, die Einstellungen für Gruppenaufgaben zu ändern, aktivieren Sie das Kontrollkästchen **Verwaltung von Gruppenaufgaben erlauben**.

8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

9. Wenden Sie die Richtlinie an.

   Ausführliche Informationen zum Übernehmen der Richtlinie für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Lokale Aufgaben erstellen

Gehen Sie folgendermaßen vor, um eine lokale Aufgabe zu erstellen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.

4. Wählen Sie den Computer, für den Sie eine lokale Aufgabe erstellen möchten.

5. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie im Kontextmenü des Client-Computers den Punkt **Alle Aufgaben → Aufgabe erstellen**.

   - Wählen Sie im Kontextmenü des Client-Computers den Punkt **Eigenschaften** aus und klicken Sie im folgenden Fenster **Eigenschaften: <Name des Computers>** auf der Registerkarte **Aufgaben** auf **Hinzufügen**.

- Wählen Sie in der Dropdown-Liste **Aktion ausführen** das Element **Aufgabe erstellen**.

Der Assistent für neue Aufgaben wird gestartet.

6. Folgen Sie den Anweisungen des Assistenten für neue Aufgaben.

Gruppenaufgaben erstellen

Gehen Sie folgendermaßen vor, um eine Gruppenaufgabe zu erstellen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Verwaltete Geräte**, wenn Sie eine Gruppenaufgabe für alle Computer erstellen möchten, die über das Programm Kaspersky Security Center verwaltet werden.
   - Wählen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Aufgaben** aus.
4. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**.
   Der Assistent für neue Aufgaben wird gestartet.
5. Folgen Sie den Anweisungen des Assistenten für neue Aufgaben.

Aufgabe für bestimmte Geräte erstellen

Um eine Aufgabe für bestimmte Geräte zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Aufgaben**.
3. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**.
   Der Assistent für neue Aufgaben wird gestartet.
4. Folgen Sie den Anweisungen des Assistenten für neue Aufgaben.

Aufgabenausführung starten, beenden, anhalten und fortsetzen

Wenn Kaspersky Endpoint Security auf dem Client-Computer gestartet wurde, können Sie Aufgaben auf dem Client-Computer über das Kaspersky Security Center
starten / beenden / anhalten / fortsetzen. Ist Kaspersky Endpoint Security angehalten, dann wird die Ausführung gestarteter Aufgaben abgebrochen und das Kaspersky Security Center bietet keine Möglichkeit mehr, Aufgaben zu starten, zu beenden, anzuhalten oder fortzusetzen.

Gehen Sie folgendermaßen vor, um lokale Aufgaben zu starten, zu beenden, anzuhalten oder fortzusetzen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Wählen Sie den Computer, auf dem Sie eine lokale Aufgabe starten, beenden, anhalten oder fortsetzen möchten.
5. Öffnen Sie durch Rechtsklick das Kontextmenü des Client-Computers und wählen Sie den Punkt **Eigenschaften**.

   Das Eigenschaftenfenster des Client-Computers wird geöffnet.
6. Wählen Sie den Abschnitt **Aufgaben** aus.

   Im rechten Fensterbereich wird eine Liste der lokalen Aufgaben angezeigt.
7. Wählen Sie die lokale Aufgabe aus, deren Ausführung Sie starten, beenden, anhalten oder fortsetzen möchten.
8. Führen Sie die notwendige Aktion mit der Aufgabe aus. Dafür gibt es folgende Methoden:

   - Öffnen Sie durch Rechtsklick das Kontextmenü der lokalen Aufgabe und wählen Sie den Punkt **Start** / **Abbrechen** / **Anhalten** / **Fortsetzen**.
   - Klicken Sie auf die Schaltfläche / rechts neben der Liste der lokalen Aufgaben, um die lokale Aufgabe zu starten oder zu beenden.
   - Gehen Sie wie folgt vor:

     a. Klicken Sie unter der Liste der lokalen Aufgaben auf **Eigenschaften** oder wählen Sie im Kontextmenü der Aufgabe den Punkt **Eigenschaften**.

     Das Fenster **Eigenschaften <Aufgabenname>** wird geöffnet.

     b. Klicken Sie auf der Registerkarte **Allgemein** auf die Schaltfläche **Start** / **Abbrechen** / **Anhalten** / **Fortsetzen**.

Gehen Sie folgendermaßen vor, um Gruppenaufgaben zu starten, zu beenden, anzuhalten oder fortzusetzen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie eine Gruppenaufgabe starten, abbrechen, anhalten oder fortsetzen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Aufgaben** aus.

Im rechten Fensterbereich werden die Gruppenaufgaben angezeigt.

4. Wählen Sie die Gruppenaufgabe, die Sie starten, abbrechen, anhalten oder fortsetzen möchten.

5. Führen Sie die notwendige Aktion mit der Aufgabe aus. Dafür gibt es folgende Methoden:

   - Wählen Sie im Kontextmenü der Gruppenaufgabe den Punkt **Start** / **Abbrechen** / **Anhalten** / **Fortsetzen**.
   - Klicken Sie im rechten Fensterbereich auf die Schaltfläche ▶ / ⏹, um die Gruppenaufgabe zu starten oder abzubrechen.
   - Gehen Sie wie folgt vor:

     a. Klicken Sie entweder rechts im Arbeitsbereich der Verwaltungskonsole auf den Link **Aufgabeneinstellungen anpassen** oder wählen Sie im Kontextmenü der Aufgabe den Punkt **Eigenschaften**.

     Das Fenster **Eigenschaften <Aufgabenname>** wird geöffnet.

     b. Klicken Sie auf der Registerkarte **Allgemein** auf die Schaltfläche **Start** / **Abbrechen** / **Anhalten** / **Fortsetzen**.

Um eine Aufgabe für bestimmte Computer zu starten, abzubrechen, anzuhalten oder fortzusetzen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur im Ordner **Aufgaben** die Aufgabe für bestimmte Computer, die Sie starten, abbrechen, anhalten oder fortsetzen möchten.

3. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie im Kontextmenü der Aufgabe den Punkt **Start** / **Abbrechen** / **Anhalten** / **Fortsetzen**.
   - Klicken Sie im rechten Fensterbereich auf die Schaltfläche ▶ / ⏹, um die Aufgabe für bestimmte Computer zu starten oder abzubrechen.
   - Gehen Sie wie folgt vor:

     a. Klicken Sie entweder rechts im Arbeitsbereich der Verwaltungskonsole auf den Link **Aufgabeneinstellungen anpassen** oder wählen Sie im Kontextmenü der Aufgabe den Punkt **Eigenschaften**.

     Das Fenster **Eigenschaften <Aufgabenname>** wird geöffnet.

     b. Klicken Sie auf der Registerkarte **Allgemein** auf die Schaltfläche **Start** / **Abbrechen** / **Anhalten** / **Fortsetzen**.

Aufgabeneinstellungen ändern

Um die Einstellungen einer lokalen Aufgabe zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte**.
4. Wählen Sie den Computer, für den Sie die Programmeinstellungen anpassen möchten.
5. Öffnen Sie durch Rechtsklick das Kontextmenü des Client-Computers und wählen Sie den Punkt **Eigenschaften**.

   Das Eigenschaftenfenster des Client-Computers wird geöffnet.
6. Wählen Sie den Abschnitt **Aufgaben** aus.

   Im rechten Fensterbereich wird eine Liste der lokalen Aufgaben angezeigt.
7. Wählen Sie in der Liste der lokalen Aufgaben die erforderliche lokale Aufgabe aus.
8. Klicken Sie auf **Eigenschaften**.

   Das Fenster **Eigenschaften: <Name der lokalen Aufgabe>** wird geöffnet.
9. Wählen Sie im Fenster **Eigenschaften: <Name der lokalen Aufgabe>** den Abschnitt **Einstellungen**.
10. Ändern Sie die Einstellungen der lokalen Aufgabe.
11. Klicken Sie im Fenster **Eigenschaften: <Name der lokalen Aufgabe>** auf **OK**, um die vorgenommenen Änderungen zu speichern.
12. Klicken Sie im Fenster **Eigenschaften: <Computername>** auf **OK**, um die vorgenommenen Änderungen zu speichern.

Gehen Sie folgendermaßen vor, um die Einstellungen einer Gruppenaufgabe zu ändern:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der entsprechenden Administrationsgruppe.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Aufgaben** aus.

   Im Arbeitsbereich der Verwaltungskonsole werden die Gruppenaufgaben angezeigt.
4. Wählen Sie die entsprechende Gruppenaufgabe.
5. Öffnen Sie durch Rechtsklick das Kontextmenü der Gruppenaufgabe und wählen Sie den Punkt **Eigenschaften** aus.

   Das Fenster **Eigenschaften: <Name der Gruppenaufgabe>** wird geöffnet.
6. Wählen Sie im Fenster **Eigenschaften: <Name der Gruppenaufgabe>** den Abschnitt **Einstellungen**.

7. Ändern Sie die Einstellungen der Gruppenaufgabe.

8. Klicken Sie im Fenster **Eigenschaften: <Name der Gruppenaufgabe>** auf **OK**, um die vorgenommenen Änderungen zu speichern.

Um die Einstellungen einer Aufgabe für bestimmte Computer zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur im Ordner **Aufgaben** die Aufgabe für bestimmte Computer, deren Einstellungen Sie ändern möchten.

3. Öffnen Sie durch Rechtsklick das Kontextmenü der Aufgabe für bestimmte Computer und wählen Sie den Punkt **Eigenschaften** aus.

   Das Fenster **Eigenschaften: <Name der Aufgabe für bestimmte Computer>** wird geöffnet.

4. Wählen Sie im Fenster **Eigenschaften: <Name der Aufgabe für bestimmte Computer>** den Abschnitt **Einstellungen**.

5. Ändern Sie die Einstellungen der Aufgabe für bestimmte Computer.

6. Klicken Sie im Fenster **Eigenschaften: <Name der Aufgabe für bestimmte Computer>** auf **OK**, um die vorgenommenen Änderungen zu speichern.

In Kaspersky Security Center sind alle Abschnitte des Eigenschaftenfensters für Aufgaben, mit Ausnahme des Abschnitts **Einstellungen**, standardmäßig aufgebaut. Eine ausführliche Beschreibung finden Sie im *Administratorhandbuch zu Kaspersky Security Center*. Der Abschnitt **Einstellungen** enthält spezifische Einstellungen für Kaspersky Endpoint Security für Windows. Sein Inhalt ist abhängig von der gewählten Aufgabe und vom Aufgabentyp.

Einstellungen der Inventarisierungsaufgabe

Für die Inventarisierungsaufgabe können Sie die folgenden Einstellungen anpassen:

- **Inventarisierungsbereich**. In diesem Block können Sie die Objekte des Dateisystems angeben, die bei der Inventarisierung untersucht werden sollen. Mögliche Objekte sind lokale Ordner, Netzwerkordner, Wechseldatenträger und Festplatten, oder der gesamte Computer.

- **Einstellungen der Inventarisierungsaufgabe**. In diesem Block können Sie außerdem die folgenden Einstellungen anpassen:

  - **Untersuchung bei Computerleerlauf ausführen**. Dieses Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit der die Inventarisierungsaufgabe angehalten wird, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security hält die Inventarisierungsaufgabe an, wenn der Bildschirmschoner nicht aktiviert und der Computer entsperrt ist.

  - **Inventarisierung von DLL-Modulen**. Das Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit der Daten über DLL-Module analysiert und die Analyseergebnisse an den Administrationsserver übertragen werden.

  - **Inventarisierung von Dateiskripten**. Das Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit der Daten über Dateien, die Skripte enthalten, analysiert und die Analyseergebnisse an den

Administrationsserver übertragen werden.

- **Erweitert**. Mit dieser Schaltfläche wird das Fenster **Erweiterte Einstellungen** geöffnet, in dem Sie die folgenden Einstellungen anpassen können:

  - **Nur neue und veränderte Dateien untersuchen**. Dieses Kontrollkästchen aktiviert/deaktiviert den Modus, in dem nur neue Dateien und Dateien, die seit der letzten Inventarisierung verändert wurden, untersucht werden.

  - **Dateien überspringen, wenn Untersuchung länger dauert als**. Dieses Kontrollkästchen aktiviert / deaktiviert die Begrenzung der Untersuchungsdauer für eine einzelne Datei. Nach Ablauf des Zeitraums, der rechts im Feld festgelegt wird, bricht Kaspersky Endpoint Security die Dateiuntersuchung ab.

  - **Archive untersuchen**. Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung von Archiven der Formate RAR, ARJ, ZIP, CAB, LHA, JAR, ICE auf das Vorhandensein von ausführbaren Dateien.

  - **Programmpakete untersuchen**. Dieses Kontrollkästchen aktiviert/deaktiviert bei der Ausführung der Inventarisierungsaufgabe die Untersuchung von Programmpaketen.

  - **Große zusammengesetzte Dateien nicht entpacken**.

    Ist das Kontrollkästchen aktiviert, untersucht Kaspersky Endpoint Security keine zusammengesetzten Dateien, die größer sind als im Feld **Maximale Dateigröße** festgelegt.

    Ist dieses Kontrollkästchen deaktiviert, untersucht Kaspersky Endpoint Security zusammengesetzte Dateien unabhängig von ihrer Größe.

    > Unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist, werden umfangreiche Dateien beim Extrahieren aus Archiven von Kaspersky Endpoint Security untersucht.

  - **Maximale Dateigröße**. Kaspersky Endpoint Security entpackt nur jene Dateien nicht, deren Größe den in diesem Feld festgelegten Wert überschreitet. Der Wert wird in Megabyte angegeben.

Richtlinienverwaltung

Dieser Abschnitt informiert über das Erstellen und die Konfiguration von Richtlinien für Kaspersky Endpoint Security. Weitere Informationen zum Verwaltungskonzept für Kaspersky Endpoint Security mithilfe von Richtlinien für Kaspersky Security Center finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Über Richtlinien

Mithilfe von Richtlinien können Sie identische Funktionseinstellungen von Kaspersky Endpoint Security für alle Client-Computer festlegen, die zu einer Administrationsgruppe gehören.

Mithilfe von Kaspersky Endpoint Security können Sie richtliniendefinierte Einstellungswerte für einzelne Computer aus einer Administrationsgruppe ändern. Auf lokaler Ebene können Sie nur jene Einstellungen ändern, deren Änderung nicht durch die Richtlinie verboten ist.

Ob die Programmeinstellungen auf einem Client-Computer geändert werden können, hängt davon ab, welchen Status das "Vorhängeschloss" für diese Einstellungen in den Richtlinieneigenschaften besitzt:

- Das abgeschlossene "Vorhängeschloss" () bedeutet Folgendes:
  - Kaspersky Security Center verbietet die Änderung der Einstellungen, auf welche sich dieses Vorhängeschloss bezieht, aus der Benutzeroberfläche von Kaspersky Security Center auf den Client-Computern. Kaspersky Endpoint Security verwendet auf allen Client-Computern identische Werte für diese Einstellungen, d. h. diejenigen, die in den Richtlinieneigenschaften festgelegt sind.
  - Kaspersky Security Center verbietet die Änderung der Einstellungen, auf welche sich dieses Vorhängeschloss bezieht. Dies gilt in den Eigenschaften jener Richtlinien für untergeordnete Administrationsgruppen und untergeordnete Administrationsserver, in denen die Funktion **Einstellungen der Richtlinie der höheren Ebene übernehmen** aktiviert ist. Es werden die Einstellungswerte verwendet, die in den Eigenschaften der Richtlinie der höheren Hierarchieebene festgelegt sind.
- Das offene "Vorhängeschloss" () bedeutet Folgendes:
  - Kaspersky Security Center erlaubt die Änderung der Einstellungen, auf welche sich dieses Vorhängeschloss bezieht, aus der Benutzeroberfläche von Kaspersky Security Center auf den Client-Computern. Auf den einzelnen Client-Computern verwendet Kaspersky Endpoint Security den lokalen Wert für diese Einstellungen, falls die Komponente aktiviert ist.
  - Kaspersky Security Center erlaubt die Änderung der Einstellungen, auf welche sich dieses Vorhängeschloss bezieht. Dies gilt in den Eigenschaften jener Richtlinien für untergeordnete Administrationsgruppen und untergeordnete Administrationsserver, in denen die Funktion **Einstellungen der Richtlinie der höheren Ebene übernehmen** aktiviert ist. Die Werte dieser Einstellungen sind nicht von den Einstellungen in den Eigenschaften der Richtlinie der höheren Hierarchieebene abhängig.

Die lokalen Programmeinstellungen werden nach der ersten Anwendung der Richtlinie gemäß der Einstellungen der Richtlinie geändert.

Die Rechte für den Zugriff auf Richtlinieneinstellungen (Lesen, Ändern, Ausführen) werden für jeden Benutzer festgelegt, der Zugriff auf den Administrationsserver für Kaspersky Security Center besitzt, und zudem separat für jeden Funktionsbereich von Kaspersky Endpoint Security. Um die Rechte für den Zugriff auf Richtlinieneinstellungen anzupassen, gehen Sie im Eigenschaftenfenster des Administrationsservers für Kaspersky Security Center zum Abschnitt **Sicherheit**.

In Kaspersky Endpoint Security gibt es folgende Funktionsbereiche:

- Basisschutz Dieser Funktionsbereich umfasst die Komponenten Schutz vor bedrohlichen Dateien, Schutz vor E-Mail-Bedrohungen, Schutz vor Web-Bedrohungen, Schutz vor Netzwerkbedrohungen, Firewall und Untersuchungsaufgaben.
- Programmkontrolle Dieser Funktionsbereich umfasst die Komponente Programmkontrolle.
- Gerätekontrolle Dieser Funktionsbereich umfasst die Komponente Gerätekontrolle.

- Verschlüsselung. Dieser Funktionsbereich umfasst die Komponenten für die vollständige Festplattenverschlüsselung und für die Verschlüsselung von Dateien.
- Vertrauenswürdige Zone. Dieser Funktionsbereich umfasst die Vertrauenswürdige Zone.
- Web-Kontrolle Dieser Funktionsbereich umfasst die Komponente Web-Kontrolle.
- Erweiterter Schutz Dieser Funktionsbereich umfasst die KSN-Einstellungen sowie die Komponenten Verhaltensanalyse, Exploit-Prävention, Programm-Überwachung und Rollback von schädlichen Aktionen.
- Basisfunktionalität. Dieser Funktionsbereich umfasst allgemeine Programmeinstellungen, die zu anderen Funktionsbereiche gehören. Dazu zählen: Lizenzverwaltung, Inventarisierungsaufgaben und Update für die Datenbanken und Programm-Module, Selbstschutz, erweiterte Programmeinstellungen, Berichte und Speicher, Einstellungen für den Kennwortschutz und die Programmoberfläche.

Für Richtlinien stehen folgende Aktionen zur Verfügung:

- Erstellen von Richtlinien
- Ändern der Richtlinieneinstellungen

  > Wenn das Benutzerkonto, mit dem Sie auf den Administrationsserver zugegriffen haben, nicht zum Ändern von Einstellungen einzelner Funktionsbereiche berechtigt ist, stehen die Einstellungen dieser Funktionsbereiche nicht für Änderungen zur Verfügung.

- Löschen von Richtlinien
- Ändern des Richtlinienstatus

Informationen über die Verwendung von Richtlinien, welche nicht die Interaktion mit Kaspersky Endpoint Security betreffen, finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Richtlinie erstellen

Gehen Sie folgendermaßen vor, um eine Richtlinie zu erstellen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Verwaltete Geräte**, wenn Sie eine Richtlinie für alle Computer erstellen möchten, die vom Programm Kaspersky Security Center verwaltet werden.
   - Wählen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher die entsprechenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf die Schaltfläche **Richtlinie erstellen**.
   - Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Erstellen → Richtlinie**.

   Der Assistent für neue Richtlinien wird gestartet.

5. Folgen Sie den Anweisungen des Assistenten für neue Richtlinien.

Richtlinieneinstellungen ändern

Gehen Sie wie folgt vor, um die Richtlinieneinstellungen zu ändern:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, für welche Sie die Richtlinieneinstellungen ändern möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Wählen Sie die gewünschte Richtlinie aus.
5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:

   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

   Die Einstellungen der Richtlinie für Kaspersky Endpoint Security für Windows umfassen Einstellungen für die Komponenten und Programmeinstellungen. Die Abschnitte **Erweiterter Schutz**, **Basisschutz** und **Sicherheitskontrolle** des Fensters **Eigenschaften: <Name der Richtlinie>** bieten Einstellungen für die Schutz- und Kontrollkomponenten. Der Abschnitt **Datenverschlüsselung** bietet Einstellungen für die vollständige Festplattenverschlüsselung, die Verschlüsselung von Dateien und die Verschlüsselung von Wechseldatenträgern. Der Abschnitt **Endpoint Sensor** bietet Einstellungen für die Komponente Endpoint Sensor. Der Abschnitt **Lokale Aufgaben** bietet Einstellungen für lokale Aufgaben und Gruppenaufgaben. Der Abschnitt **Allgemeine Einstellungen** bietet Einstellungen für das Programm.

   Einstellungen für die Datenverschlüsselung und für die Kontrollkomponenten werden in den Richtlinieneinstellungen angezeigt, wenn in Kaspersky Security Center im Fenster **Programmoberfläche anpassen** das entsprechenden Kontrollkästchen aktiviert ist. Diese Kontrollkästchen sind standardmäßig aktiviert.

6. Ändern Sie die Richtlinieneinstellungen.
7. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf die Schaltfläche **OK**, um die vorgenommenen Änderungen zu speichern.

Indikator des Schutzniveaus im Eigenschaftenfenster der Richtlinie

Im oberen Bereich des Fensters **Eigenschaften: <Name der Richtlinie>** wird der Indikator des Schutzniveaus angezeigt. Der Indikator kann einen der folgenden Werte annehmen:

- **Hohes Schutzniveau**. Der Indikator nimmt diesen Wert an und wird Grün, wenn alle Komponenten, die zu den folgenden Kategorien gehören, aktiviert sind:
  - **Kritisch**. Diese Kategorie umfasst die folgenden Komponenten:
    - Schutz vor bedrohlichen Dateien
    - Verhaltensanalyse
    - Exploit-Prävention
    - Rollback von schädlichen Aktionen
  - **Wichtig**. Diese Kategorie umfasst die folgenden Komponenten:
    - Kaspersky Security Network
    - Schutz vor Web-Bedrohungen
    - Schutz vor E-Mail-Bedrohungen
    - Programm-Überwachung
- **Mittleres Schutzniveau**. Der Indikator nimmt diesen Wert an und wird Gelb, wenn eine wichtige Komponente deaktiviert ist.
- **Niedriges Schutzniveau**. Der Indikator nimmt diesen Wert an und wird Rot, wenn einer der folgenden Fälle eintritt:
  - Eine oder mehrere kritische Komponenten sind deaktiviert.
  - Eine oder mehrere wichtige Komponenten sind deaktiviert.

Wenn der Indikator mit dem Wert **Mittleres Schutzniveau** oder **Niedriges Schutzniveau** angezeigt wird, so befindet sich rechts vom Indikator der Link **Details**, mit welchem das Fenster **Empfohlene Schutzkomponenten** geöffnet werden kann. In diesem Fenster können Sie die empfohlenen Schutzkomponenten aktivieren.

Darstellung der Programmoberfläche anpassen

Um das die Anzeige der Programmoberfläche anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe aus, für welche Sie die Anzeige der Benutzeroberfläche anpassen möchten.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.

4. Wählen Sie die gewünschte Richtlinie aus.

5. Öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>**. Dafür gibt es folgende Methoden:

   - Wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften** aus.
   - Klicken Sie auf den Link **Richtlinieneinstellungen anpassen**, der sich rechts im Arbeitsbereich der Verwaltungskonsole befindet.

6. Wählen Sie im Abschnitt **Allgemeine Einstellungen** den Unterabschnitt **Benutzeroberfläche** aus.

7. Führen Sie im Abschnitt **Interaktion mit dem Benutzer** eine der folgenden Aktionen aus:

   - Damit auf dem Client-Computer folgende Elemente der Benutzeroberfläche angezeigt werden, aktivieren Sie das Kontrollkästchen **Programmoberfläche anzeigen**:
     - Ordner mit dem Namen des Programms im **Startmenü**
     - Symbol für Kaspersky Endpoint Security im Infobereich der Taskleiste von Microsoft Windows
     - Pop-up-Benachrichtigungen

     Ist dieses Kontrollkästchen aktiviert, so kann der Benutzer die Programmeinstellungen über die Programmoberfläche einsehen und bei vorliegender Berechtigung ändern.
   - Um auf dem Client-Computer alle Hinweise für die Arbeit von Kaspersky Endpoint Security zu verbergen, deaktivieren Sie das Kontrollkästchen **Programmoberfläche anzeigen**.

8. Damit auf dem Client-Computer, auf welchem das Programm Kaspersky Endpoint Security installiert ist, die einfache Programmoberfläche angezeigt wird, aktivieren Sie im Block **Interaktion mit dem Benutzer** das Kontrollkästchen **Einfache Programmoberfläche**.

   Dieses Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Programmoberfläche anzeigen** aktiviert ist.

Nachrichten von Benutzern an den Server für Kaspersky Security Center senden

In folgenden Fällen kann es notwendig sein, dass der Benutzer eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken muss:

- Die Gerätekontrolle hat den Zugriff auf ein Gerät blockiert.

  Eine Nachrichtenvorlage mit einer Zugriffsanfrage für ein blockiertes Gerät steht auf der Benutzeroberfläche von Kaspersky Endpoint Security im Abschnitt Gerätekontrolle bereit.

- Die Programmkontrolle hat den Start eines Programms verboten.

  Eine Nachrichtenvorlage mit einer Starterlaubnisanfrage für ein blockiertes Programm steht auf der Benutzeroberfläche von Kaspersky Endpoint Security im Abschnitt Programmkontrolle bereit.

- Die Web-Kontrolle hat den Zugriff auf eine Webressource blockiert.

Eine Nachrichtenvorlage mit einer Zugriffsanfrage für eine blockierte Webressource steht auf der Benutzeroberfläche von Kaspersky Endpoint Security im Abschnitt Web-Kontrolle bereit.

Die Methode für den Nachrichtenversand und die Auswahl der Vorlage hängen davon ab, ob auf dem Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, eine aktive Richtlinie für Kaspersky Security Center vorhanden ist und eine Verbindung mit dem Administrationsserver für Kaspersky Security Center besteht oder nicht. Folgende Szenarien sind möglich:

- Unterliegt der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, keiner Richtlinie für Kaspersky Security Center, so wird vom Benutzer per E-Mail eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks gesendet.

  Die Nachrichtenfelder werden mit den entsprechenden Werten aus der Vorlage ausgefüllt, die auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security angegeben ist.

- Unterliegt der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie für Kaspersky Security Center, so sendet Kaspersky Endpoint Security eine Standardnachricht an den Administrationsserver für Kaspersky Security Center.

  In diesem Fall können die Nachrichten, die von Benutzern stammen, im Ereignisspeicher von Kaspersky Security Center eingesehen werden. Die Nachrichtenfelder werden mit den entsprechenden Werten aus der Vorlage ausgefüllt, die in der Richtlinie für Kaspersky Security Center angegeben ist.

- Unterliegt der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie für Offline-Benutzer für Kaspersky Security Center, so ist die Methode für den Nachrichtenversand davon abhängig, ob eine Verbindung mit Kaspersky Security Center besteht:

  - Besteht eine Verbindung mit Kaspersky Security Center, so sendet Kaspersky Endpoint Security eine Standardnachricht an den Administrationsserver für Kaspersky Security Center.

  - Besteht keine Verbindung mit Kaspersky Security Center, so wird vom Benutzer per E-Mail eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks gesendet.

  In beiden Fällen werden die Nachrichtenfelder mit den entsprechenden Werten aus der Vorlage ausgefüllt, die in der Richtlinie für Kaspersky Security Center angegeben ist.

Nachrichten von Benutzern im Ereignisspeicher von Kaspersky Security Center anzeigen

Die Komponenten Programmkontrolle, Gerätekontrolle und Web-Kontrolle ermöglichen es den Benutzern des lokalen Unternehmensnetzwerks, auf deren Computern das Programm Kaspersky Endpoint Security installiert ist, Nachrichten an den Administrator zu senden.

Es gibt zwei Methoden, mit denen der Benutzer eine Nachricht an den Administrator schicken kann:

- Als Ereignis an den Ereignisspeicher von Kaspersky Security Center.

  Ein Benutzerereignis wird an den Ereignisspeicher von Kaspersky Security Center übertragen, wenn das Programm Kaspersky Endpoint Security auf dem Benutzercomputer installiert ist und einer aktiven Richtlinie unterliegt.

- Als E-Mail-Nachricht.

Die Benutzerinformationen werden als E-Mail-Nachricht gesendet, wenn der Computer, auf welchem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie oder mobilen Richtlinie unterliegt.

Um eine vom Benutzer stammende Nachricht im Ereignisspeicher von Kaspersky Security Center anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse**.

   Im Arbeitsbereich von Kaspersky Security Center werden alle Ereignisse angezeigt, die in Kaspersky Endpoint Security aufgetreten sind. Dazu gehören auch Nachrichten an den Administrator, die von Benutzern des lokalen Unternehmensnetzwerks stammen.
3. Um den Ereignisfilter anzupassen, wählen Sie in der Dropdown-Liste **Ereignisse für Auswahl** das Element **Benutzeranfragen**.
4. Wählen Sie eine Nachricht an den Administrator.
5. Öffnen Sie das Fenster **Ereigniseinstellungen**. Dafür gibt es folgende Methoden:

   - Klicken Sie mit der rechten Maustaste auf das Ereignis und wählen Sie den Punkt **Eigenschaften** aus.
   - Klicken Sie rechts im Arbeitsbereich der Verwaltungskonsole auf **Ereigniseigenschaften öffnen**.

Informationsquellen zum Programm

Seite für Kaspersky Endpoint Security auf der Kaspersky-Lab-Website

Auf der Seite für Kaspersky Endpoint Security finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Die Seite für Kaspersky Endpoint Security enthält einen Link zum Online-Shop. Dort können Sie das Programm kaufen oder das Nutzungsrecht für das Programm verlängern.

Seite für Kaspersky Endpoint Security in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Abschnitt der Website des Technischen Supports.

Auf der Seite für Kaspersky Endpoint Security in der Wissensdatenbank finden Sie nützliche Informationen, Tipps und Antworten auf häufige Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung des Programms behandelt.

Neben Fragen zu Kaspersky Endpoint Security können die Artikel auch andere Kaspersky-Lab-Programme betreffen. Außerdem können die Artikel der Wissensdatenbank Neuigkeiten des Technischen Supports enthalten.

Diskussion über die Programme von Kaspersky Lab im Webforum

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum darüber diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben und neue Themen zur Diskussion stellen.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt beschreibt, wie Sie technische Unterstützung erhalten können, und nennt die Voraussetzungen, die dafür erfüllt sein müssen.

Wie Sie technischen Support erhalten

Wenn Sie in der Dokumentation und in den anderen Informationsquellen zum Programm keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support. Die Support-Mitarbeiter beantworten Ihre Fragen zur Installation und Verwendung des Programms.

Beachten Sie die Regeln für die Nutzung des Technischen Supports, bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- über die Hotline des Technischen Supports
- mit einer Anfrage an den Technischen Support von Kaspersky Lab aus dem Portal Kaspersky CompanyAccount

Technischer Support am Telefon

Die Experten des Technischen Supports sind in vielen Ländern telefonisch erreichbar. Informationen darüber, wie und wo Sie in Ihrer Region technische Unterstützung erhalten können, finden Sie auf der Webseite des Technischen Supports von Kaspersky Lab.

> Beachten Sie die Regeln für die Nutzung des Technischen Supports, bevor Sie sich an den Technischen Support wenden.

Technischer Support über Kaspersky CompanyAccount

Kaspersky CompanyAccount ist ein Portal für Unternehmen, die Kaspersky-Lab-Programme einsetzen. Im Portal Kaspersky CompanyAccount können Benutzer mithilfe von Online-Anfragen mit den Kaspersky-Lab-Experten kommunizieren. Im Portal Kaspersky CompanyAccount kann der Bearbeitungsstatus von Online-Anfragen verfolgt werden, die an den Kaspersky-Support gestellt wurden. Außerdem ist ein Verlauf der Online-Anfragen verfügbar.

Sie können alle Mitarbeiter Ihres Unternehmens mit einem einheitlichen Benutzerkonto für Kaspersky CompanyAccount registrieren. Mithilfe eines einheitlichen Kontos können Sie die Online-Anfragen der bei Kaspersky Lab registrierten Mitarbeiter zentral verwalten und die Berechtigungen dieser Mitarbeiter für Kaspersky CompanyAccount verwalten.

Das Portal Kaspersky CompanyAccount ist in folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch
- Russisch
- Französisch
- Japanisch

Details zum Kaspersky CompanyAccount finden Sie auf der Webseite des Technischen Supports .

Ermittlung von Informationen für den Technischen Support

Nachdem Sie den Technischen Support von Kaspersky Lab über ein Problem informiert haben, kann es sein, dass die Support-Mitarbeiter Sie auffordern, eine *Protokolldatei* zu erstellen. Eine Protokolldatei ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

Der Technische Support benötigt möglicherweise auch weitere Informationen zum Betriebssystem und den auf dem Computer laufenden Prozessen sowie genaue Verlaufsberichte zur Ausführung von Programmkomponenten.

Es kann sein, dass Sie von den Support-Experten dazu aufgefordert werden, die Programmeinstellungen zu Diagnosezwecken zu ändern.

- Funktionalität zur Ermittlung erweiterter Diagnoseinformationen aktivieren
- Vornehmen von Feineinstellungen für bestimmte Programmkomponenten. Diese Einstellungen sind nicht über die standardmäßige Benutzeroberfläche verfügbar.
- Einstellungen für die Speicherung von empfangenen Diagnose-Informationen ändern
- Anpassen von Einstellungen für das Abfangen und für die Speicherung des Netzwerkverkehrs

Alle Informationen, welche für die oben genannten Aktionen erforderlich sind (z. B. Reihenfolge der Schritte, Einstellungsänderungen, Konfigurationsdateien, Skripte, erweiterte Optionen für die Befehlszeile, Debug-Module und spezielle Dienstprogramme) werden Ihnen von den Support-Experten mitgeteilt. Sie erhalten außerdem Informationen über den Umfang der Daten, die im Rahmen der Fehlersuche empfangen werden. Die ermittelten erweiterten Diagnoseinformationen werden auf dem Benutzercomputer gespeichert. Die ermittelten Daten werden nicht automatisch an Kaspersky Lab geschickt.

Die oben genannten Aktionen dürfen nur unter Anleitung der Support-Experten ausgeführt werden. Wenn die Programmeinstellungen auf eine andere Weise geändert werden, als im Administratorhandbuch oder in den Anleitungen der Support-Experten beschrieben, so kann das Betriebssystem verlangsamt oder gestört werden, das Schutzniveau des Computers sinken und der Zugriff auf und die Integrität von Informationen beschädigt werden.

Protokolldatei erstellen

Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im Programmhauptfenster auf **Support**.

   Das Fenster **Support** wird geöffnet.

3. Klicken Sie im Fenster **Support** auf die Schaltfläche **Systemüberwachung**.

   Das Fenster **Informationen für den Support** wird geöffnet.

4. Um den Protokollierungsvorgang zu starten, wählen Sie in der Dropdown-Liste **Protokollierung** eines der folgenden Elemente aus:

   - **Aktiviert**.

     Wählen Sie dieses Element, um die Protokollierung zu aktivieren.

   - **Mit Rotation**.

     Wählen Sie dieses Element aus, um die Protokollierung zu aktivieren und die maximale Anzahl der Protokolldateien und die maximale Größe einer einzelnen Protokolldatei zu beschränken. Wird die maximale Anzahl der Protokolldateien mit der festgelegten maximalen Größe erreicht, so wird die älteste Protokolldatei gelöscht und eine neue Protokolldatei begonnen.

     Wenn dieses Element ausgewählt ist, können Sie Werte für die folgenden Felder angeben:

     - **Maximale Anzahl der Dateien für die Rotation**.

       In diesem Feld können Sie angeben, wie viele Protokolldateien maximal gespeichert werden sollen.

     - **Maximale Dateigröße für eine einzelne Datei**.

       In diesem Feld können Sie angeben, wie groß eine Protokolldatei maximal sein darf.

5. Wählen Sie in der Dropdown-Liste **Stufe** die Protokollierungsstufe.

   Es wird empfohlen, die Support-Experten nach der erforderlichen Protokollierungsstufe zu fragen. Es wird empfohlen, die Stufe **Normal (500)** einzustellen, wenn keine Support-Empfehlungen für die Protokollierungsstufe vorliegen.

6. Wiederholen Sie die Situation, in der das Problem aufgetreten ist.

7. Um den Protokollierungsvorgang zu beenden, kehren Sie ins Fenster **Informationen für den Support** zurück und wählen Sie in der Dropdown-Liste **Protokollierung** den Punkt **Deaktiviert** aus.

Nachdem eine Protokolldatei erstellt wurde, können Sie die Protokollierungsergebnisse auf die Server von Kaspersky Lab hochladen.

Auswahl der Protokolldateien und ihre Speicherung

Bis die erhaltenen Informationen an Kaspersky Lab übertragen werden, trägt der Benutzer selbst die Verantwortung für die Sicherheit der erhaltenen Informationen und insbesondere für die Kontrolle und Beschränkung des Zugriffs auf die erhaltenen Informationen, die auf dem Computer gespeichert sind.

Protokolldateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden endgültig gelöscht, wenn das Programm entfernt wird.

Protokolldateien werden im Ordner ProgramData\Kaspersky Lab abgelegt.

Protokolldateien werden nach folgendem Muster benannt:
`KES<Versionsnummer_dateXX.XX_timeXX.XX_pidXXX.><Typ der Protokolldatei>.log`.

Die Protokolldatei des Authentifizierungsagenten wird im Ordner System Volume Information gespeichert und besitzt den Namen `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Sie können die Daten einsehen, die in Protokolldateien aufgezeichnet wurden.

Alle Protokolldateien enthalten folgende allgemeinen Daten:

- Ereigniszeitpunkt
- Thread-Nummer

  Diese Informationen sind nicht in der Protokolldatei des Authentifizierungsagenten enthalten.

- Programmkomponente, auf die das Ereignis zurückgeht.
- Ereigniskategorie (informativ, Warnung, kritisch, Fehler)
- Ereignisbeschreibung für den Befehl der Programmkomponente und das Ausführungsergebnis für diesen Befehl

Inhalt der Protokolldateien SRV.log, GUI.log und ALL.log

In den Protokolldateien SRV.log, GUI.log und ALL.log können neben allgemeinen Daten auch folgende Informationen aufgezeichnet werden:

- Persönliche Daten wie Nachname und Vorname, falls diese Daten Bestandteil eines Dateipfads auf dem lokalen Computer sind.
- Benutzername und Kennwort, falls diese im Klartext übertragen wurden. Diese Daten können bei der Untersuchung des Internet-Datenverkehrs in den Protokolldateien gespeichert werden. Der

Datenverkehr wird nur aus trafmon2.ppl in Protokolldateien aufgezeichnet.

- Benutzername und Kennwort, falls diese in HTTP-Kopfzeilen enthalten sind.
- Benutzername für die Anmeldung bei Microsoft Windows, falls der Name des Benutzerkontos Bestandteil eines Dateinamens ist.
- Ihre E-Mail-Adresse oder Webadresse mit Benutzername und Kennwort, falls diese im Namen eines gefundenen Objekts enthalten sind.
- Webseiten, die Sie besuchen, sowie Links von diesen Webseiten. Diese Daten werden in Protokolldateien aufgezeichnet, wenn das Programm Webseiten untersucht.
- Adresse des Proxyservers, Computername, Port, IP-Adresse, Benutzername, der bei der Autorisierung auf dem Proxyserver verwendet wird. Diese Daten werden in Protokolldateien aufgezeichnet, wenn das Programm einen Proxyserver verwendet.
- Externe IP-Adressen, mit denen eine Verbindung zu Ihrem Computer aufgebaut wurde
- Nachrichtenbetreff, ID, Name des Absenders und Webadresse des Nachrichtenabsenders in einem sozialen Netzwerk Diese Daten werden in Protokolldateien aufgezeichnet, wenn die Komponente Web-Kontrolle aktiviert ist.

Inhalt der Protokolldateien HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Die Protokolldatei HST.log enthält neben allgemeinen Daten auch Informationen zur Ausführung der Update-Aufgabe für die Datenbanken und Programm-Module.

Die Protokolldatei BL.log enthält neben allgemeinen Daten auch Informationen über Ereignisse, die im Programm auftreten, sowie Daten, die im Programm zur Problembehebung benötigt werden. Diese Datei wird erstellt, wenn das Programm mit dem Parameter avp.exe –bl gestartet wird.

Die Protokolldatei Dumpwriter.log enthält neben allgemeinen Daten auch Verwaltungsinformationen, die zur Behebung von Problemen benötigt werden, die bei der Protokollierung einer Dump-Datei des Programms auftreten.

Die Protokolldatei WD.log enthält neben allgemeinen Daten auch Informationen über Ereignisse, die im Dienst avpsus auftreten. Dazu zählen auch Ereignisse über das Update der Programm-Module.

Die Protokolldatei AVPCon.dll.log enthält neben allgemeinen Daten auch Informationen über Ereignisse, die im Modul auftreten und mit Kaspersky Security Center zusammenhängen.

Inhalt der Protokolldateien für die Programm-Plug-ins

Die Protokolldateien für die Programm-Plug-ins enthalten neben allgemeinen Daten auch folgende Informationen:

- Die Protokolldatei des Plug-ins für den Start der Untersuchungsaufgabe aus dem Kontextmenü shellex.dll.log enthält Informationen über die Ausführung der Untersuchungsaufgabe und Daten, die im Plug-in zur Problembehebung benötigt werden.
- Die Protokolldateien des Plug-ins für die Komponente Schutz vor E-Mail-Bedrohungen mcou.OUTLOOK.EXE kann Teile von E-Mail-Nachrichten enthalten. Dazu können auch E-Mail-

Adressen gehören.

Inhalt der Protokolldatei des Authentifizierungsagenten

Die Protokolldatei des Authentifizierungsagenten enthält neben allgemeinen Daten auch Informationen über die Funktion des Authentifizierungsagenten und über Aktionen, die der Benutzer im Authentifizierungsagenten ausführt.

Über die Zusammensetzung und Speicherung von Dump-Dateien

Der Benutzer ist selbst verantwortlich für die Sicherheit der erhaltenen Informationen und insbesondere für die Kontrolle und Beschränkung des Zugriffs auf die erhaltenen Informationen, die auf dem Computer gespeichert sind.

Dump-Dateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden unwiderruflich gelöscht, wenn das Programm entfernt wird. Dump-Dateien werden im Ordner ProgramData\Kaspersky Lab abgelegt.

Eine Dump-Datei enthält alle Informationen über den Arbeitsspeicher der Prozesse von Kaspersky Endpoint Security zum Zeitpunkt, als diese Dump-Datei erstellt wurde. Eine Dump-Datei kann auch persönliche Daten enthalten.

Dump-Aufzeichnung aktivieren und deaktivieren

Um die Dump-Aufzeichnung zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich den Unterabschnitt **Programmeinstellungen** im Abschnitt **Allgemeine Einstellungen** aus.

   Im rechten Fensterbereich werden die Programmeinstellungen angezeigt.
3. Klicken Sie im Block **Debug-Informationen** auf **Einstellungen**.

   Das Fenster **Debug-Informationen** wird geöffnet.
4. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Dump-Aufzeichnung aktivieren**, damit Programm-Dumps aufgezeichnet werden.
   - Deaktivieren Sie das Kontrollkästchen **Dump-Aufzeichnung aktivieren**, damit keine Programm-Dumps aufgezeichnet werden.
5. Klicken Sie im Fenster **Debug-Informationen** auf **OK**.

6. Klicken Sie im Programmhauptfenster auf **Speichern**, um die vorgenommenen Änderungen zu speichern.

Schutz für Dump-Dateien und Protokolldateien aktivieren und deaktivieren

Dump-Dateien und Protokolldateien enthalten Informationen über das Betriebssystem und können Benutzerdaten enthalten. Um einen unberechtigten Zugriff auf diese Daten zu verhindern, können Sie den Schutz für Dump-Dateien und Protokolldateien aktivieren.

Wenn der Schutz für Dump-Dateien und Protokolldateien aktiviert ist, besitzen folgende Benutzer Zugriff auf die Dateien:

- Zugriff auf Dump-Dateien besitzen der Systemadministrator, der lokale Administrator und der Benutzer, der die Aufzeichnung von Dump-Dateien und Protokolldateien aktiviert hat.
- Zugriff auf Protokolldateien besitzen nur der Systemadministrator und der lokale Administrator.

Um den Schutz für Dump-Dateien und Protokolldateien zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich den Unterabschnitt **Programmeinstellungen** im Abschnitt **Allgemeine Einstellungen** aus.

   Im rechten Fensterbereich werden die Programmeinstellungen angezeigt.
3. Klicken Sie im Block **Debug-Informationen** auf **Einstellungen**.

   Das Fenster **Debug-Informationen** wird geöffnet.
4. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Schutz für Dump-Dateien und Protokolldateien aktivieren**, um den Schutz einzuschalten.
   - Deaktivieren Sie das Kontrollkästchen **Schutz für Dump-Dateien und Protokolldateien aktivieren**, um den Schutz auszuschalten.
5. Klicken Sie im Fenster **Debug-Informationen** auf **OK**.
6. Klicken Sie im Programmhauptfenster auf **Speichern**, um die vorgenommenen Änderungen zu speichern.

Dump-Dateien und Protokolldateien, die bei aktiviertem Schutz aufgezeichnet wurden, bleiben nach dem Ausschalten dieser Funktion geschützt.

Glossar

Administrationsagent

Programmkomponente von Kaspersky Security Center, welche für die Interaktion zwischen dem Administrationsserver und den Kaspersky-Lab-Programmen verantwortlich ist, die auf einem konkreten Netzwerkknoten (Workstation oder Server) installiert sind. Die vorliegende Komponente ist einheitlich für alle Programme von Kaspersky Lab, die unter dem Betriebssystem Windows laufen. Für die Programme, die unter anderen Betriebssystemen laufen, sind spezielle Versionen des Administrationsagenten vorgesehen.

Administrationsagent-Connector

Funktionalität des Programms, die der Verbindung zwischen dem Programm und dem Administrationsagenten dient. Der Administrationsagent ermöglicht eine Remote-Verwaltung des Programms via Kaspersky Security Center.

Administrationsgruppe

Eine Reihe von Geräten, die anhand der auszuführenden Funktionen und der auf ihnen installierten Kaspersky-Lab-Programme zusammengefasst wurden. Die Gruppierung dient zur vereinfachten Verwaltung der Geräte als geschlossene Einheit. Zu einer Gruppe können weitere Gruppen gehören. Für jede in der Gruppe installierte Anwendung können Gruppenrichtlinien angelegt und Gruppenaufgaben erstellt werden.

Administrationsserver

Komponente des Programms Kaspersky Security Center mit folgenden Funktionen: zentrales Speichern von Informationen über die im Unternehmensnetzwerk installierten Kaspersky-Lab-Anwendungen und deren Verwaltung.

Aktiver Schlüssel

Schlüssel, der momentan für das Programm verwendet wird.

Antiviren-Datenbanken

Datenbanken, die Informationen über Bedrohungen für die Computersicherheit enthalten, die Kaspersky Lab im Moment der Veröffentlichung der Antiviren-Datenbanken bekannt sind. Die Einträge der Antiviren-Datenbanken ermöglichen es, bösartigen Code in untersuchten Objekten zu finden. Die Antiviren-Datenbanken werden von den Kaspersky-Lab-Spezialisten erstellt und stündlich aktualisiert.

Archiv

Eine oder mehrere Dateien, die in komprimierter Form in eine Datei aufgenommen wurden. Für die Archivierung und zum Entpacken von Daten ist ein spezielles Archivierungsprogramm erforderlich.

Aufgabe

Funktionen, die das Kaspersky-Lab-Programm ausführen kann und die als Aufgaben realisiert sind. Beispiele: Echtzeitschutz für Dateien, Vollständige Untersuchung des Geräts, Datenbanken-Update.

Aufgabeneinstellungen

Einstellungen für die Ausführung des Programms, die für jeden Aufgabentyp individuell sind.

Authentifizierungsagent

Schnittstelle, welche nach der Verschlüsselung einer bootfähigen Festplatte die Authentifizierung für den Zugriff auf verschlüsselte Festplatten und für das Laden des Betriebssystems ermöglicht.

Backup

Spezielle Ablage für Backup-Kopien von Objekten, die vor einer Desinfektion oder vor dem Löschen angelegt werden.

Dateimaske

Aus allgemeinen Zeichen bestehender Platzhalter für Dateinamen und -erweiterungen.

Zum Erstellen einer Dateimaske können alle für Dateinamen zulässigen Symbole einschließlich folgender Sonderzeichen verwendet werden:

- ***** – Symbol, das null Zeichen oder eine beliebige Anzahl beliebiger Zeichen ersetzt
- **?** – Symbol, das ein beliebiges Einzelzeichen ersetzt

Beachten Sie, dass Name und Erweiterung einer Datei stets durch einen Punkt getrennt werden müssen.

Datenbank für Phishing-Webadressen

Eine Liste der Webressourcen, die von den Spezialisten von Kaspersky Lab als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Lab-Programms.

Datenbank für schädliche Webadressen

Liste der Webressourcen, deren Inhalt als potenziell gefährlich eingestuft wird. Die Liste wurde von den Spezialisten von Kaspersky Lab angelegt, wird regelmäßig aktualisiert und gehört zum Lieferumfang des Programms.

Desinfektion von Objekten

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden. Nicht alle infizierten Objekte können desinfiziert werden.

Exploit

Programmcode, der eine Schwachstelle im System oder in einem Programm ausnutzt. Exploits werden häufig verwendet, um auf einem Computer ohne Wissen des Benutzers Schadsoftware zu installieren.

Fehlalarm

Situation, in der eine virenfreie Datei von der Kaspersky-Lab-Anwendung als infiziert eingestuft wird, da ihr Code Ähnlichkeit mit einem Virus aufweist.

Fingerabdruck des Zertifikats

Informationen, mit denen ein Zertifikatschlüssel identifiziert werden kann. Ein Fingerabdruck wird erstellt, indem eine kryptografische Hash-Funktion auf den Schlüsselwert angewandt wird.

Heuristische Analyse

Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky Lab festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten.

Infizierte Datei

Datei, die schädlichen Code enthält (bei der Untersuchung der Datei wurde der Code eines bekannten bedrohlichen Programms gefunden). Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Dateien zu arbeiten, da dies zur Infektion Ihres Computers führen kann.

Lizenzzertifikat

Dokument, das Sie zusammen mit einer Schlüsseldatei oder einem Aktivierungscode von Kaspersky Lab erhalten. Dieses Dokument enthält Informationen über die Lizenz, die Ihnen zur Verfügung gestellt wird.

Netzwerkdienst

Kombination von Einstellungen, welche die Netzwerkaktivität charakterisieren. Für diese Netzwerkaktivität können Sie eine Netzwerkregel erstellen, welche für die Firewall gelten soll.

Normalisierte Form der Adresse einer Webressource

Als normalisierte Form der Adresse einer Webressource gilt die Textdarstellung der Adresse einer Webressource, die durch eine Normalisierung erreicht wird. Bei der Normalisierung wird die Textdarstellung einer Webadresse nach bestimmten Regeln verändert (z. B. Ausschluss von Benutzername, Kennwort und Verbindungsport aus der Textdarstellung der Webadresse, Umwandlung von in der Webadresse vorkommenden Großbuchstaben in Kleinbuchstaben).

Im Kontext der Schutzkomponenten besteht das Ziel einer Normalisierung der Adressen von Webressourcen darin, syntaktisch unterschiedliche, physisch jedoch äquivalente Adressen von Webadressen nur einmal zu untersuchen.

Beispiel:

Nicht normalisierte Form einer Adresse: www.Example.com\.

Normalisierte Form einer Adresse: www.example.com.

OLE-Objekt

Datei, die an eine andere Datei angehängt oder darin eingebettet ist. Die Programme von Kaspersky Lab gestatten es, OLE-Objekte auf Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

Patch (von engl. "patch" – Flicken)

Geringfügige Ergänzung zu einem Programm, mit der entweder Fehler behoben werden, die beim Einsatz des Programms aufgetreten sind, oder mit der Updates installiert werden.

Phishing

Eine Art des Internetbetrugs, bei der E-Mail-Nachrichten verschickt werden, um vertrauliche Daten (i. d. R. finanziellen Charakters) zu stehlen.

Portabler Dateimanager

Programm, das eine Benutzeroberfläche für die Verwendung verschlüsselter Dateien auf Wechseldatenträgern bietet, wenn die Verschlüsselungsfunktionalität auf einem Computer nicht verfügbar ist.

Potenziell infizierbare Datei

Datei, die aufgrund ihrer Struktur oder ihres Formats von einem Angreifer als "Container" benutzt werden kann, um Schadcode zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie com, exe, dll usw. Für solche Dateien ist das Risiko, dass bösartiger Code eindringt, relativ hoch.

Programm-Module

Dateien, die zum Lieferumfang des Programmpakets für das Kaspersky-Lab-Programms gehören und für die Realisierung der wichtigsten Aufgaben zuständig sind. Jedem Aufgabentyp, der im Programm realisiert ist (Echtzeitschutz, Virensuche, Update), entspricht ein spezielles ausführbares Modul. Wenn Sie die vollständige Untersuchung Ihres Computers aus dem Hauptfenster starten, initiieren Sie den Start des Moduls für diese Aufgabe.

Programmeinstellungen

Einstellungen für die Arbeit des Programms, die für alle Aufgabentypen gleich sind und sich auf das gesamte Programm beziehen (z.B. Leistungseinstellungen für das Programm, Einstellungen für Berichte, Backup-Einstellungen).

Reserveschlüssel

Dieser Schlüssel gewährt das Recht auf die Programmnutzung, wird aber momentan nicht verwendet.

Schutzbereich

Objekte, die permanent von der Komponente für den Basisschutz untersucht werden. Der Schutzbereich besitzt je nach Komponente unterschiedliche Eigenschaften.

Schwarze Liste der Adressen

Liste mit E-Mail-Adressen. Die von diesen Adressen eintreffenden Nachrichten werden vom Kaspersky-Lab-Programm ungeachtet ihres Inhalts blockiert.

Signaturanalyse

Erkennungstechnologie für Bedrohungen unter Einsatz der Datenbanken von Kaspersky Endpoint Security. Die Datenbanken enthalten Beschreibungen bekannter Bedrohungen und entsprechende Desinfektionsmethoden. Der Schutz mithilfe der Signaturanalyse gewährleistet eine minimal erforderliche Sicherheitsstufe. In Übereinstimmung mit den Empfehlungen der Spezialisten von Kaspersky Lab ist diese Analysemethode immer aktiviert.

Subjekt des Zertifikats

Inhaber des privaten Schlüssels, der mit dem Zertifikat verbunden ist Dies kann ein Benutzer, ein Programm, ein beliebiges virtuelles Objekt, ein Computer oder ein Dienst sein.

Trusted Platform Module

Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Das Trusted Platform Module wird gewöhnlich auf dem Mainboard des Computers installiert und interagiert über eine Hardwareschnittstelle mit den übrigen Systemkomponenten.

Untersuchungsbereich

Objekte, die im Rahmen einer Untersuchungsaufgabe von Kaspersky Endpoint Security untersucht werden.

Update

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Update-Servern heruntergeladen.

Zertifikat

Elektronisches Dokument, das einen öffentlichen Schlüssel, Informationen über den Schlüsselinhaber und den Gültigkeitsbereich des Schlüssels enthält, und das bestätigt, dass der öffentliche Schlüssel dem Inhaber gehört. Ein Zertifikat muss von der ausstellenden Zertifizierungsstelle signiert sein.

Zertifikataussteller

Zertifizierungsstelle, die das Zertifikat ausgestellt hat

AO Kaspersky Lab

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor unterschiedlichen Bedrohungstypen schützen. Dazu zählt der Schutz vor Viren und anderer Schadsoftware, Spam, Netzwerk- und Hackerangriffen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach Angaben der IDC ist Kaspersky Lab in Russland der beliebteste Hersteller von Computerschutzsystemen für Heimanwender ("IDC Endpoint Tracker 2014").

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern, der in 33 Ländern über insgesamt 38 Niederlassungen verfügt. Das Unternehmen beschäftigt über

3.000 hochspezialisierte Mitarbeiter.

Produkte. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Programme für die Informationssicherheit von Desktops, Laptops, Tablets, Smartphones und anderen mobilen Geräten.

Das Unternehmen bietet Lösungen und Technologien für den Schutz und die Überwachung von Workstations und mobilen Endgeräten, virtuellen Maschinen, Datei- und Webservern, Mail-Gateways und Firewalls. Im Angebot befinden sich auch spezielle Produkte für den Schutz vor DDoS-Angriffen, für den Schutz von Umgebungen für Automatisierungstechnik und für die Prävention von Finanzbetrug. In Verbindung mit Verwaltungstools ermöglichen es diese Lösungen, für Unternehmen jeder Größenordnung einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderttausende neuer Computerbedrohungen und entwickeln Tools, um diese Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf welche die Kaspersky-Lab-Programme zurückgreifen.

Technologien. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu und ZyXEL. Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

Auszeichnungen. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So erhielt Kaspersky Lab 2014 bei Tests des anerkannten österreichischen Antiviren-Labors AV-Comparatives neben einem anderen Hersteller die meisten Zertifikate "Advanced+" und wurde mit dem Zertifikat "Top Rated" ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 400 Millionen Anwender. Über 270.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Website von Kaspersky Lab:	http://www.kaspersky.com/de
Viren-Enzyklopädie:	https://de.securelist.com/
Virenlabor:	https://virusdesk.kaspersky.de/ (zur Untersuchung verdächtiger Dateien und Websites)
Webforum von Kaspersky Lab:	https://forum.kaspersky.com/index.php?/forum/26-deutschsprachiges-benutzer-forum/

Informationen über den Code von Drittherstellern

Die Informationen über den Code von Drittherstellern sind in der Datei legal_notices.txt enthalten, die sich im Installationsordner des Programms befindet.

Markenrechtliche Hinweise

Eingetragene Marken und Dienstleistungszeichen sind Eigentum der jeweiligen Rechteinhaber.

Adobe, Acrobat, Flash und Shockwave sind Marken oder in den Vereinigten Staaten von Amerika und/oder in anderen Ländern eingetragene Marken von Adobe Systems Incorporated.

Mac ist eine in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragen Marke der Apple Inc.

AutoCAD ist eine Marke oder eine in den Vereinigten Staaten von Amerika und/oder in anderen Ländern eingetragene Marke der Autodesk, Inc. und/oder deren Tochter- bzw. verbundenen Unternehmen.

Die Bluetooth-Wortmarke und die Bluetooth-Logos sind Eigentum der Bluetooth SIG, Inc.

Borland ist eine Marke oder eine in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marke von Borland Software Corporation.

Citrix und Citrix Provisioning Services sind Marken von Citrix Systems, Inc. und/oder deren Tochterunternehmen, die in den Vereinigten Staaten von Amerika und in anderen Ländern als Patent registriert sind.

dBase ist eine Marke der dataBased Intelligence, Inc.

EMC und SecurID sind Marken oder in den Vereinigten Staaten von Amerika und/oder anderen Ländern eingetragene Marken der EMC Corporation.

IBM ist eine Marke der International Business Machines Corporation, die in vielen Ländern registriert ist.

ICQ ist eine Marke und/oder eine Dienstleistungsmarke von ICQ LLC.

Intel und Pentium sind in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marken der Intel Corporation.

Logitech ist eine eingetragene Marke oder eine Marke des Unternehmens Logitech in den Vereinigten Staaten von Amerika und (oder) in anderen Ländern.

Microsoft, Access, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MultiPoint, Outlook, PowerPoint, PowerShell, Visual C++, Visual Basic, Visual FoxPro, Windows, Windows Store und Windows Server sind in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marken der Microsoft Corporation.

Mozilla und Thunderbird sind Marken der Mozilla Foundation.

Java und JavaScript sind eingetragene Marken des Unternehmens Oracle und/oder seiner verbundenen Unternehmen.