FUDO PAM

IN THE CONTEXT OF GDPR IMPLEMENTATION

Fudo Security
A brand of Wheel Systems Sp. z o.o.
Aleje Jerozolimskie 178
02 - 486 Warszawa

VAT no.:524-25-21-745 KRS no.:0000224900
the Regional Court for the city of Warsaw in Warsaw,
XIII Commercial Division of the National Court Register,
Initial Capital: 50 000,00 PLN

EMEA: +48 22 100 67 00
www: **fudosecurity.com**
info@fudosecurity.com

According to the "Verizon Data Breach Report 2017" up to 51% of data breaches last year were connected with the use of privileged accounts. Out of these, more than 60% of the incidents were due to mistakes of the administrators themselves. Privileged access does not only provide great power but a great deal of responsibility.

Privileged accounts enable unrestricted access to essential IT resources: main servers, networking equipment or users' workstations. They also provide the tools necessary to cover up possible administrator errors.

A lack of control over privileged users puts the integrity and security of a company's data at risk, especially in the case of outsourcing IT services. Taking over a privileged account by an unauthorized person may lead e.g. to a data leak and damaging an enterprise's reputation

The recently adopted GDPR law acknowledges that monitoring and recording the administrators' behavior is crucial while managing data leaks and modifications of personal databases.

"In the case of IT security, simple human trust has to be replaced with control. When the company isn't able to monitor an employee's activity, control is out of the picture. – according to Paweł Dawidek, CTO Fudo Security – Sometimes it may lead to a situation, when an employer becomes hostage of the administrator, who abuses his position. Another frequent problem is an administrator leaving a company without transferring knowledge about a specific network. It poses the risk of a breach but also delays the handover of responsibilities to the new administrator."

GDPR obligates companies to detect personal data leaks, then to immediately inform proper institutions about the security incident in that area, and eventually document every action (preventive, as well as active defense against the attack). That's why it is essential to implement trustworthy solutions, which allow management of privileged architecture continuously.

First of all, it refers to the users, accounts and remote sessions. Such documentation enables preparation of proper forensic analysis, indicating the possible attack sources or those responsible for the incident. Last but not least, it may help to prove, that the company exercised due diligence to abide by every procedure and implement the most suitable technology solutions, required by the GDPR.

Sealing an organization's security from the inside is not the only advantage of using Fudo PAM.

A step ahead of the cybercriminals – defending the underbelly of the security architecture

Fudo PAM responds to the security needs of modern companies, concerning not only the external threat but also complying with various regulations. Fudo PAM is dedicated to the institutions that are aware of the fact, that criminals are also driven by business intuition, so they strike in the areas which are most vulnerable to attack. That means they disguise themselves as remote IT consultants, taking over administrative accounts, or exploiting weaknesses in password management procedures within critical sectors of the organization's infrastructure.

Developing existing technologies and adding new features resulted in creating a new, effective system, which – on one hand – allows combating cybercriminals, and on the other hand – providing important business data. The latter makes it possible to optimize business processes, perfecting professional skills of the administrators and meeting the requirements of GDPR.

Wheel Fudo PAM comprises four supplementing modules:

- Secret Manager – a feature managing privileged accounts' passwords. They are stored safely, not visible to privileged users. The advantage of the solution is the ability to define the validity of the password, its complexity and length. Secret Manager stores password history to ensure access to managed accounts in an emergency. Enhancing the security level of stored passwords is guaranteed by an advanced mechanism, checking if a password change has been authorized.

- Privileged Session Monitoring – privileged session monitoring, recording and detailed live analysis. This tool is extremely helpful in providing quick forensic analysis or error reporting. What's more, session previews take place without delays and additional loss on session quality. The tool also allows super administrators and users to collaborate on a single session, and providing it quickly to non-Fudo administrators. This gives companies the chance to interact with external specialists needed to analyze selected session elements. The integrity of an IT infrastructure will also be maintained by a definable security policy designed to interrupt suspicious sessions.

- Efficiency Analyzer – a solution for analyzing the productivity of remote subcontractors/consultants by setting the appropriate parameters in the form of clear graphs presenting the number of sessions, time of activity and inactivity of the user or organization. Only few solutions allow you to generate detailed reports showing the effectiveness of your work within recorded privileged sessions.

- Application to Application Password Manager - a password management mechanism for brokering passwords to selected applications, avoiding human contact. Standard passwords stored by the application and used for authentication can facilitate an attack on the system with which the application connects to. The use of the AAPM module, along with the Secret Manager feature, significantly enhances security.

Fudo PAM delivers benefits far beyond security

Fudo is – first and foremost – a security system, providing convenient and effective monitoring. It also simplifies forensic analysis of remote sessions. Instant access to suspicious sessions enables a live video preview.

This is essential when it is necessary to prove that the company has made every effort to comply with GDPR rules. By automatically creating an administrative session documentation, identifying the person responsible for the leak or proving that the leak was independent of the organization and unavoidable under given conditions is not a problem. Fudo archives provide the ability to effectively defend an organization in the event of an inspection or investigation of personal data protection, but also of any other European regulation (such as the NIS Critical Infrastructure Directive).

Fudo PAM provides an unmatched shield against attacks on older operating systems and network protocols. Fudo uses the time marking mechanism and records sessions as raw material. This makes it possible to use recorded sessions as evidence in court. The recording is also evidence for the suspected administrator or other privileged user that the error was not caused by his actions.

Secret Manager is not only about password protection. It also saves money on password management and enables defining policies that change in accordance with ISO27000 or European regulations. This puts an end to password sharing, as well as additional administrator work in fixing and recovering passwords.

The Efficiency Analyzer functionality is a unique business intelligence module that allows you to analyze the activity of remote consultants and subcontractors. It is an excellent tool for verifying service contracts and monitoring maintenance contracts. It is also another element in documenting your organization's activities to minimize the risk of personal data leakage in the GDPR aspect.

Fudo's unique advantage is the fact that it is an all-in-one solution. There are no agents or licensing requirements for other software. Fudo as a standalone device or virtual appliance can start working within hours.

A modern, intuitive administrative interface shortens the time needed for the user to become familiar with the system. Fudo keeps to Fudo Security mission, that using Fudo Security solutions ensures seamless deployment and convenient maintenance. This is of great importance to the enormous pressure from the GDPR, which provisions European organizations should have implemented by May 2018.

Considering the time constraint, it's critical to choose a trustworthy security solution which can be set up right away. One that will help protect your organization from the massive penalties provided by GDPR in the event of a lack of readiness to prevent leaks and handling incidents.

FUDO
SECURITY

We understand business

and that’s why we look after the end users when designing our solutions.

Using the strongest security mechanisms is supposed to support business processes and not limit them.

Security is just the beginning. We always go further.

Attention to detail, product quality and competent technical support are what differentiates us from the competition.

Fudo Security
A brand of Wheel Systems Sp. z o.o.
Aleje Jerozolimskie 178
02 - 486 Warszawa

Sales:
sales@fudosecurity.com
EMEA: +48 22 100 67 00

LinkedIn: **fudosecurity**
Facebook: **FudoSec**
Twitter: **FudoSecurity**