

WIE IST DAS THEMA PAM MIT FUDO INTERN AUFGEKOMMEN?

Wir sind grundsätzlich gesetzlich verpflichtet die Dienstleister auf unseren Servern und Systemen zu überwachen. Wir suchten entsprechend eine Lösung, die unsere rechtlichen und technischen Anforderungen erfüllt.

WIE SIND SIE ÜBERHAUPT AUF FUDO GEKOMMEN?

Es gab zwei Möglichkeiten, die wir verglichen haben: Balabit (die Ich aus langjähriger Erfahrung gut kenne) und FUDO. Es war also eine Entscheidung zwischen FUDO und Balabit.

Ich kannte beides, und mir wurde von unserem Partner iKomm die FUDO Lösung empfohlen.

Für uns war es vor allem die Oberfläche von FUDO, die uns besser gefallen hat. Einige Punkte waren besser bei FUDO, z.B. der Password Manager.

WER WAR BEI DER UMSETZUNG BETEILIGT, WAREN NOCH ANDERE ABTEILUNGEN BETEILIGT?

Mein Vorgesetzter (unser IT-Leiter) und Ich (System Admin) haben von der technischen Seite die Entscheidung getroffen. Am Rande hat auch unser Security Beauftragter seine Anforderungen geprüft.

WIE LIEF DIE TESTSTELLUNG UND EINRICHTUNG AB?

Problemlos. Dank meiner Kenntnis von Linux und BSD Themen hatte Ich keine Probleme bei der Einrichtung. Hierbei wurde Ich remote während dem Test und der Produktivschaltung von den Technikern der Firma iKomm GmbH unterstützt.

WIE LANGE DAUERTE DIE EINRICHTUNG VON DER LÖSUNG?

In 2-Stunden Blöcken dauerte es nur 2-3 Tage bis wir alle Funktionen konfiguriert haben.

HABEN SIE DIE LÖSUNG WÄHREND DEM TEST INTERN EINGESETZT ODER HABEN SIE GLEICH DIENSTLEISTERNÜBER DIE LÖSUNG ZUGRIFF AUF DIE SYSTEME GEGEBEN?

Grundsätzlich haben wir die Lösung zuerst nur intern getestet, es durften aber unsere Mitarbeiter von außen die Systeme testen. Nun sind es die Dienstleister die wir überwachen.



Herr Roman Brunka ist bereits seit einigen Jahren für die Administration der Server bei Vivantes zuständig und befasst sich im Rahmen des PAM- Projektes intensiv mit der Einführung einer entsprechenden Lösung.

ZAHLEN UND FAKTEN VIVANTES:



Das Unternehmen wurde zum **1. Januar 2001** gegründet



über 15000 **Mitarbeitern**



Die Einrichtung von Fudo PAM dauerte **2 Tage**

NUTZEN SIE DIE FUDO INTERN BEI EIGENEN PROJEKTEN, SPRICH ZEICHNEN SIE AUCH GEGEBENENFALLS IHRE EIGENEN MITARBEITER AUF?

Grundsätzlich noch nicht aber in Notfällen, wenn z.B. während einer Notbereitschaft ein Netzwerkproblem auftritt und der Bereitschaftsdienst keine Zugänge auf die Switches hat, kann er sich dann über die FUDO anmelden und es werden alle Aktivitäten beobachtet und dokumentiert.

HABEN SIE NACH DEM TEST DIE LÖSUNG DIREKT ÜBERNOMMEN?

Die Testumgebung war eine virtuelle Maschine, eingesetzt in der Produktivumgebung wird die Hardware Appliance. Auch wenn theoretisch eine Übernahme der Konfiguration problemlos möglich ist, habe ich für meine eigene Übersicht die Lösung von vorne konfiguriert.

HABEN SIE SEITDEM SIE FUDO ANWENDEN, AUSREICHEND SUPPORT/ TECHNISCHE UNTERSTÜTZUNG?

Wir haben direkten Kontakt zum FUDO Support und Ich bin sehr zufrieden mit der Unterstützung, sehr positiv.

Vor allem geht es dabei um Funktionserweiterungen die wir brauchen und jene werden integriert. Das läuft dann so, dass wir eine Anfrage einreichen, ob es nicht sinnvoll wäre gewisse Funktionen zu programmieren und in der Regel passiert dann genau das. Zum Beispiel Port Forwarding wurde auf Anfrage integriert.

WELCHE MEHRWERTE HABEN SIE DURCH FUDO?

Wir können beobachten was die Dienstleister machen, aber unser primäres Ziel ist das dokumentieren und im Falle eines großen Problems müssen wir die Nachweispflicht erfüllen und uns sicher sein, dass keine Daten verloren gehen. Das ist natürlich auch gesetzlich gefordert. Als Klinikgruppe mit kritischen Patientendaten sind wir hierfür natürlich selber verantwortlich, auch wenn die Daten oftmals von Dienstleistern auf deren eigenen Servern verwaltet werden, wo wir keine Zugänge haben. Entsprechend erhalten wir gegenseitig Zugriffe dank FUDO und haben im Anschluss ein klares Zuständigkeitsverhältnis, sodass im Notfall eine Schuldzuweisung unproblematisch erfolgen kann.

HATTEN SIE SCHON WELCHE VORFÄLLE?

Nein.

WIE LANGE SETZTEN SIE FUDO SCHON EIN?

Seit dem Frühjahr 2018

WAS IST IHRE MITTLERE SESSION ZEIT?

Die längste Session bisher war 7 Tage lang. Die Sessions dauern sehr lang, deswegen habe ich bei FUDO eine neue Funktion angefragt, die eine Verkürzung der Aufzeichnungsdauer möglich macht.

KAPAZITÄT

Wir haben eine große Kapazität und bisher erst 25 % belegt.

WELCHES FUDO MODELL BENUTZEN SIE?

FUDO F1001 Appliance im Cluster

WIE IST FUDO BEI IHNEN EINGERICHTET? BRIDGE/PROXY?

Proxy Mode ist gut für die Kunden. Die VPN Tunnel wurden so konfiguriert, dass sie alle auf die Proxy IPs umgeleitet werden und somit die Dienstleister den Eindruck haben, dass Sie direkten Zugriff auf die Server auf die Server haben.

WIE VIEL ÜBERZEUGUNGSARBEIT BRAUCHTEN SIE BEI DEM BETRIEBSRAT?

Kann Ich persönlich keine Auskunft dazu geben.Grundsätzlich ging es bisher bei PAM mit FUDO um die Aufzeichnung der Dienstleister und nicht der eigenen Mitarbeiter, weshalb der Betriebsrat entsprechend wenig in die Entscheidung involviert werden musste. Wenn wir in Zukunft die Nutzung auf unsere eigenen Mitarbeiter ausweiten, kommt er wieder ins Spiel.

EFFICIENCY ANALYZER UND USER PORTAL?

Benutzen wir bis jetzt nicht, aber wollen wir in der Zukunft einsetzen.

WIE STUFEN SIE FUDO GEGENÜBER DER KONKURRENZ EIN?

Die wichtigsten Unterschiede waren die Funktionen, insbesondere die einfachere Konfiguration der einzelnen Funktionen. Die intelligente Oberfläche gewährleistet einen klaren Überblick. Dadurch ist der Einstieg für die Kollegen einfacher. Der Umgang und das Zusammenarbeiten mit den Kollegen werden erleichtert.

Was mir besonders gefällt ist die Konfiguration über API, weil unser Unternehmen sehr groß ist. Wir habenderzeit über 300 Server angebunden und Tendenz steigend. Entsprechend kann ein über API verbundenes Skript automatisiert die Konfiguration der neuen Systeme fahren. Das ganze stärkt das Unternehmen und alles geht schneller, einfacher und fehlerfrei.

”

Der Umgang und das Zusammenarbeiten mit den Kollegen werden erleichtert.

WÜRDEN SIE DIE FUDO LÖSUNG WEITEREMPFEHLEN?

Ja ganz bestimmt!

SEHR GEEHRTER HERR BRUNKA, VIELEN DANK FÜR DAS GESPRÄCH!