FUDO SECURITY

# PAM | Privileged Access Management

Eine FUDO Geschichte – Privileged Access Management mit der iKomm GmbH

# EINE FUDO GESCHICHTE
# PRIVILEGED ACCESS MANAGEMENT
# MIT IKOMM GMBH

Das Thema PAM- Privileged Access Management ist historisch aus dem Bankenwesen entstanden. FUDO wurde als Reaktion auf eine konkrete Anforderung aus dem Bankenwesen entwickelt.
Bereits in den frühen 2000ern befassen Sich kritische Infrastrukturen mit der Absicherung Ihrer sensiblen Daten, insbesondere Kundendaten, Knowhow, Geschäftsgeheimnisse usw.
Im Jahr 2018 identifiziert das Gartner Institut das Thema PAM als das wichtigste IT-Sicherheitsthema für CIOs, denn 55% aller Security Lücken sind auf den falschen Gebrauch Privilegierter Accounts zurückzuführen, 60 % aller Sicherheitsvorfälle resultieren aus Fehlkonfigurationen der Admins (vgl. „2015 Data Breach Investigation Report“ von Verizon).

## Die Problematik:

Jeden Tag laufen externe Dienstleister im Unternehmen herum (bzw. warten aus der Ferne die Systeme), haben dabei Zugriffe auf Server, teilweise mit administrativen Rechten und die Unternehmen/Admins selber haben keinen Überblick und können somit nicht sagen: wer, was, wann, wo, wie macht.

Täglich kommt es zu vielen Sicherheitsvorfällen die auf dieses Problem zurückzuführen sind.
Ein einfacher Dienstleister, z.B. ein Klimatechniker mit niedrigen Zugriffsrechten, kann auf den Systemen Malware installieren, die sich dann ungesehen im Unternehmen ausbreitet und Informationen/Daten entwendet. Laut Microsoft dauert die durchschnittliche Zeit für das Entdecken eines solchen Sicherheitsvorfalls 243 Tage, wobei nur in seltenen Fällen Unternehmen selber die Attacke entdecken. Mögliche Schäden können Operationaler Natur sein (Verlust der IT/Unternehmensbereiche), die Reputation betreffen, das Geschäft ruinieren (Entwenden von Plänen/Designs/Kampagnen), richten in jedem Fall einen massiven finanziellen Schaden an und können für die entsprechenden Personen (IT-Leiter, Geschäftsleitung) das Karriere-Ende bedeuten.

Eine PAM-Lösung kommt genau hier ins Spiel. Gängige PAM – Lösungen, regeln die Zugänge und protokollieren also in irgendeiner Art und Weise die Aktivitäten der Dienstleister und sollen somit einen Überblick schaffen und im Schadensfall die Infrastruktur rechtlich absichern. Ebenso aus Dienstleisterperspektive ist eine PAM-Lösung nötig, da Dienstleister sich selber gegenüber Ihren Kunden durch die PAM-Lösung absichern und Ihnen im Schadensfall eine konkrete Beweislage vorliegt (Sie können eine PAM-Lösung von kritischen Infrastrukturen fordern).

Unsere FUDO-Lösung setzt das Thema PAM technologisch um wie keine andere Lösung und schafft durch die technische funktionsweise Mehrwerte, sodass der ursprüngliche „Überwachungsgedanke“ vollkommen in den Hintergrund rückt und sowohl externe Dienstleister, als auch Mitarbeiter die Lösung als intelligentes Tool in Ihre Projekte einbinden.

Einer unserer Bestands- und Referenzkunden, fasst diesen Umstand am besten zusammen:

*„Das ganze Thema beginnt als rechtskonforme Anforderung des Datenschützers, der Compliance, der GL usw. Nachdem allerdings eine FUDO im Flughafenbetrieb eingeführt wurde, geht dieser Gedanke vollkommen im Hintergrund unter. Jeder IT-Mitarbeiter will die Protokollfunktion freiwillig nutzen um Sich selber abzusichern, die externen Dienstleister ebenso, und die Zusammenarbeit wird dadurch massiv intensiviert. Die Angst, dass rechtliche Schwierigkeiten seitens der Mitarbeiter auftreten, ist vollkommen unbegründet, da FUDO eine neue Kultur in dem Unternehmen verankert: Das individuelle Absichern und die intensivere Zusammenarbeit rücken dank FUDO in den Vordergrund, anstatt dem Gefühl von Überwachung. Die externen Dienstleister kommen explizit auf den Flughafen zu und bedanken Sich für die positiven Effekte einer FUDO auf den Workflow.“* (Peter Gabriel, IT-Leiter, Flughafen Nürnberg, langjähriger FUDO-Bestandskunde)

Im Folgenden legen wir den Fokus auf genau diese positiven Effekte/Mehrwerte, die eine FUDO in Ihren täglichen Prozessen mit sich bringt.
Der globale Ansatz bei FUDO ist, dass **die schnittstellenunabhängige Appliance Lösung an einem Tag an Ihre Server angebunden wird**. Sie bringen der Lösung bei welche Dienstleisterarten Sie haben, legen im User Portal einzelne Dienstleistergruppen an, legen deren Zugriffe und ein Regelwerk fest (vereinfacht: wer darf auf welches System und was passiert wenn der Dienstleister Regeln missachtet) und der ganze Spaß kann direkt losgehen.

## Vorteil 1):

Wenn die Dienstleister normalerweise zu Ihnen kommen, geben Sie ihnen direkten Zugriff auf Ihre Server und müssen im Anschluss „eigentlich“ jedes Mal die Credentials ändern.
Hier kommt der erste große FUDO-Vorteil ins Spiel: FUDO liegt über den Systemen. Sie haben wie zuvor beschrieben FUDO beigebracht wer Zugriff auf was hat, also meldet sich der Dienstleister an der FUDO an und wird automatisch von der FUDO auf die entsprechenden Ressourcen weitergeleitet.
FUDO hat an dieser Stelle einen **Secret Manager**, d.h. die Passwörter können jedes Mal von den Dienstleistern (nach Ihren individuellen Komplexitätskriterien) neu generiert werden? Wechselnde Credentials. Gleichzeitig können Sie Ihre vorhandene 2FA-Authentifizierungssysteme bzw. Ihre Authorisierungssysteme in die FUDO integrieren. FUDO als Sicherheitslösung hat selbstverständlich einen viel größeren Schutzfaktor als Ihre Betriebsserver und kann wesentlich schwerer gehackt werden. Die Festplatten sind mit dem höchsten **Sicherheitsstandard AES-XTS-256 verschlüsselt**.

## Vorteil 2):

Ihre Dienstleister haben Sich an der FUDO angemeldet und wurden auf die entsprechenden Systeme weitergeleitet. Sie haben von vornherein ein festes Regelwerk aufgestellt, sodass **im Falle unautorisierter Aktivitäten die PAM auf die Session entsprechend reagiert** (Pausieren, Benachrichtigung des Admins,…).

Ab Log-In **wird „Alles“ was die Person macht aufgezeichnet** (wobei das Aufgezeichnete Material verschlüsselt und mit Timestamping revisionssicher archiviert wird).
Vorteil 2 bezieht Sich hier auf das Wort „Alles“: Während ***alle*** Konkurrenz PAM-Lösungen Videos aufzeichnen (Was übrigens in keiner Weise der rechtskonform geforderten Vieraugenüberwachung entspricht) **arbeitet FUDO mit Rohdaten** (Sprich neben dem zusammengesetzten Bildschirmdaten werden jeder Mausklick, jeder Tastenschlag, jede Mausbewegung usw. separat aufgezeichnet und in einer separaten Leiste wiedergegeben), dies bringt folgende Vorteile mit sich:

| | VIDEO (MITBEWERBER) | ROHDATEN (FUDO) |
|---|---|---|
| Datengröße | Enorme Speicherinanspruchnahme | Entlastung gegenüber Videoformat um Faktor 12 => Niedrige Storage-Kosten |
| Rechtskonformität | Nein (kann manipuliert werden, entspricht keinem Vier-Augen-Prinzip) | Ja, Vier-Augen-Prinzip ist vorhanden => manipulationssicher |
| Auswertung | Auswertung nur durch Tagelanges anschauen der Videos möglich | Auswertung anhand von verkürzter Darstellungsweise, Bspw. Nur Stellen wo Dienstleister aktiv ist (Sprich etwas tippt, Mausklick setzt)<br>=> Forensische Analyse im Video-Format |
| Wiedergabe | Nur in Produktabhängigen Videoprogrammen, nicht auf allen Endgeräten | Auf jedem Internetfähigen Endgerät mit Browser => Produktunabhängig<br>Ansehen der Sessions im Grafik-Modus => Ereigniswiedergabe |
| Protokollfunktion | Nein, bzw. nur „endlose Videos“ | Sinnvolle Protokollfunktion von Arbeitsvorgängen dank verkürzter Darstellungsweisen der Aktivitäten, der Session Player überspringt also inaktive Zeitintervalle, Sessions können getagged werden mit Voll-Text-Search und fortgeschrittenen Filteroptionen |
| Volltextsuche | Keine Suchfunktion | Gezielte Suchfunktion: z.B.: Wann hat Dienstleister auf Vertriebsordner zugegriffen; oder folgenden Befehl eingegeben; … |
| Effektivitätsanalyse | Nein keine Aussage über Effektivität Möglich | FUDO berechnet Verhältnis aus Login Zeit und Aktivität des Dienstleisters; Erstellt detaillierte periodische Reports => Service-Management-Tool |
| Unterstützte Systeme | überwiegend Windows<br>(nicht protokollbasierte Aufzeichnung auf Arbeitsstation führt zu zusätzlichem Risiko) | Windows aber auch alle sonstigen Systeme (Alte Systeme, Jump Host, Netzwerkprotokolle) |
| Wartungskosten | Jährlich Anfallende Lizenzkosten | Einmalige Kosten, Keine Wartung, Recht auf Migration auf aktuellste Version |
| Hersteller Kommunikation | Indirekt | Direkt |
| Nahtlose Zulassung | Nein | Zugriffskontrolle per Web-GUI/E-Mail/ App |
| Live-Monitoring | Nein | Ja, Co-Sharing erlaubt dem Systemadministrator eine gegebene Connection zu besuchen und gemeinsam mit dem Remote User zu arbeiten, er kann Sie auch mit Dritten als URL link teilen |

## Für wen ist also FUDO im Unternehmen relevant?

Rechtlich gesehen betrifft das Thema PAM in der ersten Linie die IT und externe Dienstleister. Dienstleister loggen Sich über die FUDO ein und arbeiten (gemeinsam mit der IT) auf den Systemen. Aber auch andere Bereiche im Unternehmen profitieren dank den zahlreichen Mehrwerten von der FUDO Lösung.

Ihre (IT-)Compliance und der Datenschutz bekommen die Möglichkeit die Einhaltung von Gesetzen, Richtlinien und freiwilligen Kodizes zu verfolgen und zu gestalten.

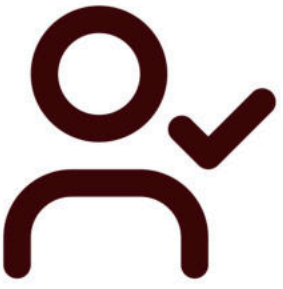
Das Externe Service Management und Personalwesen bekommt mit FUDO die einzigartige Möglichkeit, die Qualität der externen Dienstleistungen (durch Forensische Analysen/Effektivitätsauswertungen) zu prüfen, die Blackbox Dienstleister wird somit aufgemacht. Die Rechtsabteilung bekommt mit FUDO im Krisenfall ein starkes Tool an die Hand und sichert ihr Unternehmen rechtlich.

## FUDO in der Zukunft

Während gängige PAM Unternehmen ihren Fokus auf das Marketing Ihrer Lösung legen, arbeitet FUDO bereits heute an den Technischen Möglichkeiten von Morgen um das volle Potenzial zu nutzen.

Denn eine PAM-Lösung sammelt alle Aktivitäten der aufgezeichneten Sessions und bietet somit mit Blick auf die Zukunftstechnologien ein riesiges Potenzial. Der Hersteller arbeitet folglich bereits heute an einer „User-Behavior-Based artificial intelligence“. Das heißt der FUDO wird in Zukunft „Leben eingehaucht“, eine KI wird in die FUDO eingepflanzt, die FUDO wird anhand der Verhaltensanalysen in der Lage sein Sie aktiv beim Dienstleistungsmanagement zu unterstützen, auf Gefahren präventiv zu reagieren usw. …

**Generieren Sie also bereits heute mit FUDO den höchstmöglichen Sicherheitsschutz mit maximalen Mehrwerten und schauen Sie mit uns auf eine spannende Zukunft!**



ikomm
INNOVATIVE KOMMUNIKATION

HANS-BORNKESSEL-STRAßE 45
90763 FÜRTH

+49 (0) 911 - 30 91 8 - 0

vertrieb@ikomm.de

www.ikomm.de | msp.ikomm.de | dna.ikomm.de