Perfekte Sicherheit beim Remote-Zugriff

Was ist Privileged Access Management (PAM), wozu dient es, und wie funktioniert es? Bernhard Aregger, Sales Specialist beim IT-Security-Distributor BOLL, erklärt Funktion und Nutzen von PAM-Lösungen anhand der Lösung Fudo PAM.

Warum braucht es Privileged Access Management (PAM)?
Beim ersten Kontakt mit Interessenten für eine PAM-Lösung stelle ich initial immer die folgende Frage: Wissen Sie genau, wer auf Ihre Systeme wie Firewalls, Server oder Datenbanken zugreift, was dabei geschieht und wann der Zugriff erfolgte? Angesichts der meist zahlreichen Nutzerkonten mit privilegiertem Zugang – zum Beispiel für externe Dienstleister – fehlt oft die Übersicht, und die Unternehmen können das Zugriffsmanagement nicht mehr manuell handhaben.

Und was bringt eine PAM-Lösung konkret?
PAM-Lösungen wie Fudo PAM machen Unsichtbares sichtbar, schaffen vollständige Visibilität über Remote-Sessions, helfen dabei, schädliche Aktivitäten zu erkennen und zu blockieren, und unterstützen so die jeweiligen Compliance-Anforderungen. Fudo PAM ist nicht nur für Grossunternehmen interessant, sondern auch für KMUs, nimmt doch die Zahl der relevanten Systeme stetig zu. Und gerade KMUs setzen vermehrt auf externe Spezialisten, die ihre Systeme aus der Ferne verwalten und warten. Ein Grund mehr, alle privilegierten Zugänge bestmöglich abzusichern.

Wie funktioniert die Lösung von Fudo?
Fudo PAM klinkt sich in Form einer Hardware-Appliance oder als virtuelle Maschine zwischen die Remote-Nutzer und die Systeme des Unternehmens ein und zeichnet von A bis Z sämtliche User-Sessions auf. Das kontinuierliche Session-Monitoring mit Aufzeichnung erlaubt es, auch nachträglich alles nachzuvollziehen, bis zum einzelnen Tastenanschlag. Gleichzeitig analysiert die integrierte KI das Nutzerverhalten und kann so verdächtige Aktivitäten erkennen und unterbinden. Weitere Funktionen sind der Secret Manager zur automatisierten Passwortverwaltung und der Efficiency Manager.

Was ist die Aufgabe des Efficiency Manager?
Dieser analysiert das Aktivitätsniveau während einer Session. So wird beispielsweise erkannt, ob ein Dienstleister stundenlang angemeldet war, aber kaum etwas getan hat. So lässt sich überhöhten Rechnungen, wie dies in der Praxis immer wieder vorkommt, Paroli bieten. Der Efficiency Manager ist eine nützliche Zusatzfunktion. Übrigens: All die erwähnten Funktionen sind in der Lizenz enthalten und müssen nicht separat dazugebucht werden.

Bernhard Aregger ist Sales Specialist beim IT-Security-Distributor BOLL..

Wie unterscheidet sich Fudo von anderen PAM-Lösungen?
Zunächst durch die Aufzeichnungsmethode. Im Gegensatz zu vergleichbaren Lösungen erstellt Fudo PAM nicht etwa eine Videoaufnahme, sondern zeichnet die Rohdaten auf, also die Kommunikation in nativen Protokollen wie RDP, VNC, SSH, Telnet, HTTP/HTTPS sowie Datenbankprotokollen und OT-Protokollen wie Modbus SCADA. Dadurch belegen die Aufzeichnungen massiv weniger Speicherplatz. Eine Session von acht Stunden benötigt in der Regel 20 oder 30 Megabyte versus mehrere Gigabyte bei einer Videoaufnahme.

Welche weiteren Vorteile bringt die Rohdatenaufzeichnung noch?
Die integrierte OCR-Funktion ermöglicht eine schnelle Volltextsuche über alle Sessions hinweg. So findet man innert Sekunden die gesuchten Aktivitäten und muss nicht stundenlang Videomaterial durchforsten. So kann man nach einem Breach viel schneller reagieren. Mithilfe sogenannter Regular Expressions lässt sich zudem definieren, dass eine Session beim Vorkommen bestimmter Begriffe automatisch gestoppt wird oder dass der Administrator eine Warnung erhält. Und die Rohdaten sind mit einem Timecode versehen und so nur schwer manipulierbar.

Das klingt interessant. Welche weiteren Eigenschaften zeichnen Fudo aus?
Fudo, übrigens kein US-Unternehmen, sondern ein europäischer Hersteller mit Haupt- und Entwicklungssitz in Warschau, wollte eine einfache, schlanke Lösung schaffen. Das merkt man auch, wenn man das Produkt näher betrachtet: Es kommt aufgeräumt und strukturiert daher, ist DSGVO-konform und konzentriert sich ganz auf die Sicherung privilegierter Zugriffe, das Management der Zugriffsberechtigungen und das Session-Monitoring. Zusammen mit einer agentenlosen Architektur schlägt sich dies in einer schnellen Implementierung nieder. Fudo PAM lässt sich in wenigen Stunden einrichten, ohne Unterbrechung der IT-Dienste. Das Feintuning erfolgt dann im laufenden Betrieb. Darüber hinaus ist die Lösung als virtuelle Appliance cloudfähig und lässt sich für Managed Services einsetzen.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58 | 5430 Wettingen
Tel. 056 437 60 60 | info@boll.ch | www.boll.ch