Privileged Access Management schafft Zugriffssicherheit

Die sensiblen Daten im Gesundheitswesen, in Verbindung mit einer Vielzahl von Akteuren, erfordern einen besonders strengen Umgang mit Zugriffsberechtigungen und Passwörtern sowie eine umfassende Visibilität über alle Vorgänge im Netzwerk. Privileged-Access-Management-Lösungen (PAM) gewährleisten die nötige Kontrolle und Nachvollziehbarkeit und unterstützen die Einhaltung von Compliance- und gesetzlichen Vorgaben.

Spitäler und andere Healthcare-Einrichtungen sind hochkomplexe Umgebungen, in denen unterschiedlichste Akteure mit den wohl sensibelsten Daten umgehen, die überhaupt denkbar sind: persönliche Informationen zu den Patienten, ihren Diagnosen und Therapien. Angesichts dessen ist die gezielte Absicherung der IT-Systeme vor unerlaubten Zugriffen unerlässlich.

Zugriffsmanagement mit PAM

Die IT-Security-Industrie hat für die Kontrolle der Zugriffe durch privilegierte Nutzer sogenannte Privileged-Access-Management-Lösungen (PAM) entwickelt. Ursprünglich ging es dabei primär um die Überwachung von Systemadministratoren sowie externen IT-Dienstleistern mit Zugriffsberechtigungen auf systemnahe Ebenen der IT-Infrastruktur. PAM-Lösungen sind jedoch geradezu dafür prädestiniert, sämtliche Zugriffe und Aktivitäten aller Nutzer abzudecken und die gesamte Zugriffsverwaltung zentralisiert zu ermöglichen. Denn in manchen Unternehmen und damit auch in vielen Spitälern werden die Nutzerkonten bisher nicht zentral gemanagt, Zugriffe kaum überwacht und ein Konto womöglich sogar durch mehrere Mitarbeitende parallel genutzt. Solche Missstände lassen sich mit PAM elegant und rechtzeitig beheben: Ohne stringentes Zugriffsmanagement dauert es oftmals Monate, bis ein Missbrauch entdeckt wird.

PAM-Lösungen überwachen alle Zugriffe und erlauben nur den Zugang zu Systemen und Daten, für die der jeweilige Nutzer eine Berechtigung besitzt. Weitere PAM-Funktionen sind die Live-Supervision (Session Monitoring) und die Aufzeichnung von User Sessions – wichtig für die Nachvollziehbarkeit bei Sicherheitsvorfällen sowie missbräuchlichen oder bösartigen Nutzeraktivitäten. Damit unterstützt Privileged Access Management die Einhaltung der organisationsinternen Compliance-Regeln und gesetzlicher Datenschutzvorschriften und Standards wie DSGVO, HIPAA, NIST und ISO 27001. PAM verhilft darüber hinaus zu einem umfassenden Überblick über alle Aktivitäten im Netz.

PAM aus Europa für optimalen Datenschutz

Nebst zahlreichen in den USA beheimateten Anbietern von PAM-Lösungen stechen im PAM-Markt zwei europäische Unternehmen heraus, die sich mit den behördlichen Compliance-Anforderungen in Europa bestens auskennen: WALLIX ist ein französischer Anbieter, Fudo Security stammt aus Polen. Beide führen ein umfassendes PAM-Angebot mit jeweils leicht unterschiedlicher Ausrichtung.

Am Beispiel von WALLIX lassen sich die Funktionen und Eigenschaften einer PAM-Lösung gut aufzeigen. WALLIX zählt mit seiner Gründung im Jahr 2003 zu den PAM-Pionieren der ersten Stunde und fokussiert sich bis heute auf Privileged Access Management und verwandte Themen wie Multi-Faktor-Authentifizierung. Alles zusammen wird unter dem Motto «PAM4ALL» vermarktet. Die zentrale PAM-Lösung Bastion setzt sich aus den drei Hauptkomponenten Session Manager, Access Manager und Password Manager sowie zusätzlich PEDM für Genehmigungen nach dem Prinzip des kleinsten Privilegs und AAPM für das interapplikatorische Passwortmanagement in DevOps-Szenarien zusammen. Bastion ist modular aufgebaut und kann nach den Anforderungen skalierbar bereitgestellt werden, wobei sich einzelne Merkmale bedarfsgerecht freigeben lassen.

Elemente der PAM-Lösung von WALLIX

Der Session Manager ist das Kernstück der WALLIX-Lösung mit den Funktionen Zugriffskontrolle, Session Management, Monitoring, lückenlose Aufzeichnung von RDP/TSE-, VNC-, SSH- und Telnet-Sitzungen sowie Supervision-Modus zur

Livebegleitung durch Administratoren mit der Möglichkeit, eine Session jederzeit abzubrechen, oder auch durch Instruktoren für Lernzwecke. IT-Führungskräfte erhalten so eine Lösung für Administration, Kontrolle und Auditing von Zugriffen auf Netzwerksysteme mit starkem Sicherheitsstatus und rechtswirksamen Prüfpfaden. Zugriffe können auch für bestimmte Anwendungen oder Server, Zeitfenster oder Protokolle gewährt oder verweigert werden. Damit ist gewährleistet, dass nur die richtige Person zum passenden Zeitpunkt auf die korrekten IT-Ressourcen zugreifen kann.

Der Access Manager dient dem zentralisierten Management, Monitoring und Audit externer Zugriffe und erlaubt SSH/RDP-Zugriff via HTML5, kommt also ohne spezielle Client-Software auf den Endgeräten aus und minimiert die Angriffsfläche mithilfe eines einzigen gesicherten HTTPS-Eintrittspunkts für den externen Zugriff. Zudem ist der Access Manager eng mit der WALLIX-Lösung Trustelem für SSO und Directory-Integration sowie der Multi-Faktor-Authentifizierungslösung WALLIX Authenticator verzahnt und unterstützt Standardprotokolle für den Zugang auf MFA-Lösungen von Drittanbietern.

Mit dem Password Manager von WALLIX lassen sich Passwörter verwalten und in einem konsolidierten Tresor speichern. Dadurch wird gewährleistet, dass Passwörter nicht mehr weitergegeben oder gestohlen werden können. Dabei hilft optional auch die automatische Rotation von Passwörtern nach jeder Benutzung. Bei der Vergabe von Passwörtern sorgt der Password Manager für die Einhaltung der geltenden Passwortrichtlinien – generische Admin- oder Root-Passwörter werden eliminiert. Des Weiteren lässt sich festlegen, dass Passwörter in vorgegebenen Intervallen oder nach Bedarf geändert werden müssen.

Auch Fudo mit starken PAM-Funktionen

Die PAM-Lösung Fudo Enterprise von Fudo Security bietet vergleichbare Funktionalität, basiert jedoch nicht auf einzelnen Bastion-Servern, sondern auf einer Hardware- oder Virtual-Appliance. Mit der Funktion Remote Session Monitoring beinhaltet sie einen leistungsstarken Videorecorder, der das aufgezeichnete Material im RAW-Format abspeichert. Dies ermöglicht es, die aufgezeichneten Videos innert Sekunden zu untersuchen (dank OCR-Technologie auch nach Texteingaben) und dabei von User-Aktion zu User-Aktion zu springen.

Die Funktion Sessionsharing ermöglicht es, weitere Administratoren in eine Session einzuladen und bereits aufgezeichnete Sessions zu Schulungszwecken weiterzuleiten. Dank Merkmalen wie Just-in-time-Zugang durch individuelle Anfrage vor jedem Zugriff, Zugangsportal für externe Lieferanten, integrierter Multi-Faktor-Authentifizierung, KI-gestützter Analyse des Nutzerverhaltens, Passwort Changer und Effizienzanalysator zur Überwachung von produktiver Aktivität und Leerlaufzeiten – zum Beispiel bei externen Auftragnehmern – ist auch die Fudo-Lösung eine mächtige PAM-Plattform.

Die Fudo-Enterprise-PAM-Lösung ist komplett agentenlos und in einem halben Tag aufgesetzt, beziehungsweise in den produktiven Betrieb implementiert. Die All-in-one-Lizenz beinhaltet sämtliche von Fudo angebotene Funktionen.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch