Advertorial

Privileged Access Management mit dem gewissen Plus

Die Verwaltung und Überwachung privilegierter Zugriffe – Privileged Access Management (PAM) – gewinnt in Zeiten grassierender Cyberkriminalität immer mehr an Bedeutung. Der PAM-Spezialist WALLIX offeriert eine umfassende Plattform für die Verwaltung, Absicherung und Überwachung solcher Zugriffe.

Der Zugriff auf Systeme, Anwendungen und Services – sowohl durch interne Mitarbeitende mit besonderen Berechtigungen (zum Beispiel Administratoren) als auch externe Dienstleister sowie Softwarekomponenten untereinander – muss besonders strikt überwacht und verwaltet werden. Denn wer erst einmal in einem privilegierten System «drin ist», kann nahezu unbeschränkt nicht nur nützliche, sondern auch bösartige Aktivitäten entfalten. Privileged-Access-Management-Lösungen sorgen dafür, dass nur wirklich berechtigte Zugriffe erfolgen (können), und gewährleisten gleichzeitig die volle Nachvollziehbarkeit aller Vorgänge.

Eine Bastion gegen unbefugte Zugriffe

Das französische, 2003 gegründete Softwareunternehmen WALLIX hat sich unter dem Motto «PAM4ALL» ganz der Absicherung privilegierter Zugriffe verschrieben. Als PAM-Spezialist der ersten Stunde hat sich WALLIX mit über 1800 Mitarbeitenden und drei R&D-Zentren in Frankreich und Spanien als führender europäischer Anbieter einer umfassenden PAM-Plattform etabliert. WALLIX wird im aktuellen Magic Quadrant 2022 von Gartner für PAM-Lösungen als Leader aufgeführt.

Die zentrale Komponente der WALLIX-Plattform namens Bastion deckt alle Aspekte des Privileged Access Management ab. Dazu gehören Themen wie Zugriffsmanagement, Session Management mit Support für Monitoring und lückenlose Aufzeichnung von RDP/TSE-, VNC-, SSH- und Telnet-Sitzungen, Supervision-Modus zur Live-Begleitung von Sessions durch Administratoren sowie Passwortverwaltung mit Passwortsafe und Durchsetzung von Passwortvorschriften inklusive regelmässiger Aktualisierung der Passwörter.

Damit endet der Funktionsumfang von Bastion jedoch keineswegs. Die Lösung eignet sich, nicht zuletzt dank zuverlässigen und rechtswirksamen Prüfpfaden für alle Aktivitäten privilegierter Nutzer, bestens zur Unterstützung der Einhaltung unternehmensinterner Compliance-Vorgaben und gesetzlicher Vorschriften wie PCI-DSS, Basel III und SOX. Darüber hinaus erkennt Bastion ungewöhnliche

und verdächtige Aktivitäten und hilft, diese Bedrohungen rechtzeitig zu blockieren oder im Fall eines erfolgreichen Angriffs nachzuvollziehen und zu dokumentieren. Und mit der Komponente AAPM (Application-to-Application Password Management) sorgt Bastion für sichere, automatisierte und verschlüsselte Zugriffe zwischen Applikationen und Services via API und unterstützt so moderne Entwicklungs- und Betriebsmodelle wie DevOps und RPA (Robotic Process Automation) – sowohl On-Premises als auch in der Cloud, sowohl für IT- als auch für IoT- und OT-Umgebungen.

Endpunktschutz durch Privilege Management

Mit der Option WALLIX Bestsafe bietet WALLIX zahlreiche zusätzliche Features, die der Absicherung und Härtung von Endpunkten mit proaktivem Schutz auf Prozessebene dienen. Bestsafe kommt ohne regelmässige Updates aus, beansprucht als agentenloser Dienst nur minimale Systemressourcen und neutralisiert 95 Prozent aller Malware. Für die Nutzer agiert Bestsafe völlig transparent. Die Lösung ist per White-, Grey- und Blacklisting einfach zu konfigurieren und ermöglicht hochgranulare Einstellungen – so etwa mit ausgefeilten Ransomware-Regeln.

Identity Services aus der Cloud

Mit WALLIX Trustelem bietet der Hersteller nach dem Prinzip «Identity as a Service» einen sicheren und bequemen Zugang an – dies mittels einer kontextbasierten Multi-Faktor-Authentifizierung (MFA) und Identity Federation mit Support für Active Directory, Azure AD, LDAP und Google Workspace. Die integrierte MFA-Lösung ermöglicht einen schnellen Schutz für Cloud-Applikationen und eine unkomplizierte Anmeldung (Single Sign-on) für alle Nutzer.

Die Lösungen von WALLIX, die garantiert keine Backdoors aufweisen, ermöglichen ein umfassendes Security- und Cyberrisikomanagement zur Geschäftsabsicherung – sowohl im Finanzsektor, in der produzierenden Industrie und im Gesundheitswesen als auch in anderen kritischen Infrastrukturen. Sie verfügen über die CSPN-Zertifizierung der ANSSI, dem französischen Pendant zum deutschen BSI, tragen zudem zur Einhaltung von Compliance-Vorgaben bei und liefern Informationen für zuverlässige Audits.

Kontakt

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60, info@boll.ch,
www.boll.ch