Safeguard von One Identity (OI)

Privilegierte Zugriffe sicher speichern, verwalten und analysieren

Konten mit privilegierten Rechten sind das bevorzugte Angriffsziel von Hackern. Deshalb ist es für Unternehmen von essenzieller Bedeutung, privilegierte Zugriffe effektiv und sicher zu verwalten, denn sie bilden den Kern für IT-Sicherheit und Compliance. Der Safeguard von One Identity ermöglicht, Schäden durch Datenverlust oder -missbrauch zu minimieren und bietet Unternehmen eine sichere Methode zum Schutz privilegierter Konten und nachhaltiger Verbesserung der IT-Sicherheit.

Ein Must-have: Differenzierte Betrachtung von privilegierten Zugriffen

Die graduelle Differenzierung von privilegierten Zugriffen und Konten ist in den meisten Betriebs standardmäßig nicht vorgesehen. Gemäß dem Prinzip „alles oder nichts“ besitzen eine Vielzahl von Usern oftmals enorme Rechte, die sie zu Erledigung ihrer täglichen Aufgaben gar nicht benötigen. Da privilegierte Konten genutzt werden können, um Standardkontrollen und Autorisierungsstufen zu umgehen, hat eine Person mit privilegiertem Konto oft unbegrenzten Zugriff und kann sowohl absichtlich als auch unabsichtlich erheblichen Schaden an Netzwerken, Servern, Anwendungen und Daten anrichten. Ein Risiko, dass sich angesichts der Auslagerung des Identitätsmanagements an externe IT-Dienstleister mit Remote-Zugriff auf das Unternehmensnetzwerk noch erhöht. Ohne eine weitergehende Differenzierung bei den privilegierten Zugriffen, ist es kaum möglich, Verstöße und Fehlverhalten zu analysieren, nachzuverfolgen und entsprechende Konsequenzen und Maßnahmen zur Erhöhung der Sicherheit abzuleiten.

Mehr Sicherheit und Transparenz dank verschiedener Kontrollmechanismen

Bei der Verwaltung privilegierter Konten geht es um das Zusammenwirken von Prozessen, Richtlinien und Technologien, durch die sichergestellt wird, dass privilegierte Benutzer mit Administrationsrechten auch wirklich das Richtige tun. Ähnlich der Gewaltentrennung von Judikative, Legislative und Executive hilft der Safeguard von One Identity, gegenseitige Kontrollmechanismen auch für eine IT-Unternehmenslandschaft bereitzustellen. Zu diesem Zweck unterstützt der Safeguard nicht nur eine differenzierte Betrachtung der Zugriffsnotwendigkeiten durch Administratoren. Er identifiziert auch besonders risikobehaftete Nutzer und gleicht Aktivitäten auf Basis von automatisierten Arbeitsabläufen mit geltenden Richtlinien ab. So lassen sich die Befugnisse und Zugriffsrechte privilegierter Benutzer nicht nur begrenzen, sondern es wird auch die Nachvollziehbarkeit sämtlicher Aktivitäten zu jedem Zeitpunkt sichergestellt. In der Summe wird auf diese Weise eine zusätzliche Sicherheitsebene für privilegierte Zugriffe eingezogen, während gleichzeitig alle Voraussetzungen dafür geschaffen werden, dass die Systemadministratoren ihre Aufgaben effizient und richtlinienkonform erfüllen können.

Produktmerkmale & Features

- Individuelle Sicherheitskonzepte für privilegierte Passwörter und Sitzungen
- Richtlinienbasierte Freigabekontrolle
- Ermittlung von risikobehafteten Benutzern
- Biometrische Analyse des Benutzerverhaltens
- Warnen und Blockieren in Echtzeit
- Systematische Befehls- und Anwendungskontrolle via weißer/schwarzer Liste
- Unterstützung zahlreicher Protokolle (SSH, Telnet, RDP, HTTP(s), ICA und VNC)
- Drop-in-Bereitstellung
- REST-basierte API für eine vereinfachte Integration von Anwendungen und Systemen

Ihr Nutzen auf einen Blick

- Vereinfachung der Verwaltung privilegierter Konten und Sessions
- Verbesserter Schutz für sensible Daten und Unternehmensinformationen
- Identifizierung von privilegierten Benutzern mit hohem Risiko, riskantem Verhalten und ungewöhnlichen Ereignissen
- Abmilderung des potenziellen Schadens von Sicherheitsverstößen
- Effiziente Erstellung von Überwachungsberichten
- Erfüllung von Compliance-Anforderungen
- Schnelle Amortisierung durch vereinfachte Bereitstellung und Verwaltung

„Da vor allem privilegierte Konten ein bevorzugtes Ziel von Hackern darstellen, kommt der Verwaltung und Administration dieser Konten für die Gesamtsicherheit der IT in einem Unternehmen eine besondere Bedeutung zu. Der Safeguard wird deshalb auf einer gehärteten Instanz betrieben, auf die nicht jeder Zugriff hat. Die Anwendung bietet bestmöglichen Schutz für sämtliche privilegierte Konten, in dem er eine Sitzungsverwaltung und -überwachung mit umfassenden Analysemöglichkeiten kombiniert. So können auffällige Aktivitäten und Bedrohungen frühzeitig erkannt und entsprechende Schutzmaßnahmen initiiert werden.“

Gerald Appel (Team Lead One Identity)