SiTS

Your Trusted
Cyber Security Partner

Top 15: So sichern Sie Ihre privilegierten Konten effetiv

1 Was sind die aktuellen Bedrohungen und Vorschriften, die die Cybersicherheit beeinflussen?

Cyberbedrohungen wie Ransomware, Phishing und Insiderangriffe nehmen stetig zu. Gleichzeitig machen strenge Regulierungen wie NIS2, GDPR, HIPAA und DORA robuste Schutzmaßnahmen unverzichtbar. Der Druck auf IT-Sicherheitsstrategien steigt.

2 Wie setzen diese Bedrohungen IT-Sicherheitsprofis unter Druck?

Sicherheitsprofis stehen unter Druck, sensible Daten zu schützen und die Compliance sicherzustellen. Sie müssen eine umfassende Sicherheitsstrategie entwickeln, die auf Bedrohungen reagiert, ohne die betriebliche Effizienz zu gefährden.

3 Was sind die größten Herausforderungen bei der Entwicklung einer Sicherheitsstrategie?

IT-Sicherheitsverantwortliche müssen Identitätssicherheit, Netzwerkschutz, Endpoint-Security und Mitarbeiterschulungen in Einklang bringen. Besonders die Verwaltung privilegierter Konten, die mit hohen Zugriffsrechten verbunden sind, stellt ein erhebliches Risiko dar.

4 Was sind privilegierte Konten und warum sind sie so wichtig?

Privilegierte Konten gewähren weitreichenden Zugriff auf kritische Systeme und Daten – dazu gehören Admin-Konten, Anbieterzugriffe oder Maschinen-Accounts. Sie sind unverzichtbar für das Systemmanagement, aber auch eine potenzielle Schwachstelle, wenn sie nicht korrekt verwaltet werden.

5 Welche Risiken gehen von privilegierten Konten aus?

Compromised privileged accounts can result in unauthorized data access, system disruptions, and compliance violations. Their high level of access makes them attractive targets for cybercriminals and a critical point of vulnerability.

6 Was ist PAM und wie hilft es?

PAM (Privileged Access Management) ist ein Set von Sicherheitspraktiken und Technologien, das den Zugriff auf kritische Systeme kontrolliert und auditiert. Es stellt sicher, dass nur autorisierte Nutzer privilegierte Aktionen durchführen können, und minimiert so das Risiko von Missbrauch.

7 Welche Vorteile bietet die Implementierung von PAM?

PAM setzt das Prinzip der minimalen Privilegien um, bietet detaillierte Audits, reduziert die Angriffsfläche und stellt die Compliance sicher. Es unterstützt die Verwaltung und Überwachung der Aktivitäten privilegierter Konten.

8 Welche Arten von PAM-Implementierungen sind verfügbar?

Do It Yourself On-Premise PAM: Wird innerhalb der Infrastruktur der Organisation installiert, bietet Kontrolle und Sicherheit, erfordert aber laufende interne Wartung und Anpassungen.
Do It Yourself Cloud PAM: Wird in der Cloud gehostet, bietet Skalierbarkeit und reduziert den internen Verwaltungsaufwand, ist jedoch auf die Sicherheit und qualifizierten Ressourcen des Anbieters angewiesen.
PAM as a Service (PAMaaS): Wird von Drittanbietern verwaltet und bietet umfassende PAM-Lösungen, die ideal für KMUs mit begrenzten IT-Ressourcen sind.

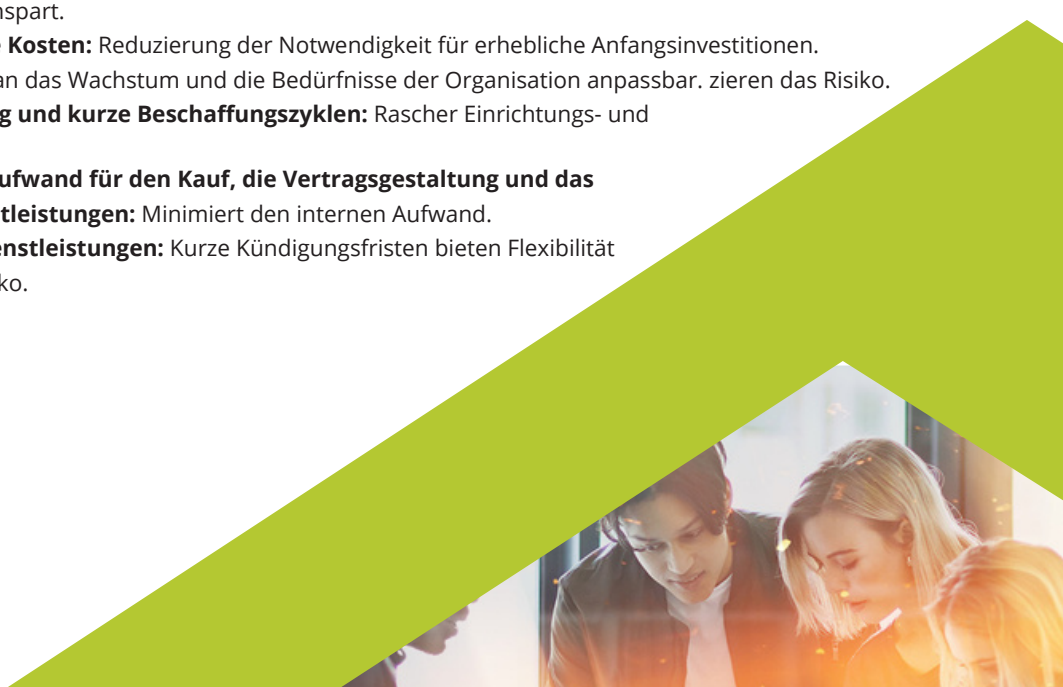
9 Was sind die Unterschiede zwischen Do It Yourself und verwalteten PAM-Diensten?

Do It Yourself: Bietet vollständige Kontrolle und Anpassung, erfordert jedoch umfangreiche interne Expertise und Ressourcen.
Managed Services: Bietet eine schlüsselfertige Lösung mit kontinuierlichem Management und Unterstützung, sodass KMUs sich auf ihre Kerngeschäftsaktivitäten konzentrieren können, während gleichzeitig die Sicherheit gewährleistet ist.

10 Warum sollten KMUs PAM as a Service in Betracht ziehen?

PAMaaS bietet mehrere Vorteile für kleine und mittelständische Unternehmen, darunter:

- **Zugang zu Expertenmanagement:** Keine Notwendigkeit für interne Spezialisten, was Kosten für Schulungen und Zertifizierungen einspart.
- **Geringere anfängliche Kosten:** Reduzierung der Notwendigkeit für erhebliche Anfangsinvestitionen.
- **Skalierbarkeit**: Leicht an das Wachstum und die Bedürfnisse der Organisation anpassbar. zieren das Risiko.
- **Schnelle Bereitstellung und kurze Beschaffungszyklen:** Rascher Einrichtungs- und Beschaffungsprozess.
- **Geringer Ressourcenaufwand für den Kauf, die Vertragsgestaltung und das Onboarding von Dienstleistungen:** Minimiert den internen Aufwand.
- **Flexibilität bei den Dienstleistungen:** Kurze Kündigungsfristen bieten Flexibilität und reduzieren das Risiko.



11 Welche alternativen Lösungen habe ich neben einer PAM-Sicherheitstechnologie oder -dienstleistung?

Alternativen umfassen die manuelle Verwaltung privilegierter Konten, die die Verwendung von Tabellenkalkulationen oder einfachen Zugriffskontrolllisten beinhaltet, sowie die Abhängigkeit von integrierten Betriebssystemfunktionen. Diese Methoden können jedoch fehleranfällig sein und bieten nicht die erweiterten Sicherheitsfunktionen, die dedizierte PAM-Lösungen bereitstellen. Bedenken Sie, dass nicht alle Sicherheitsrisiken eliminiert werden können.

12 Was passiert, wenn ich keine spezialisierte Technologie oder Dienstleistung verwende, die von einem Spezialisten verwaltet wird?

Ohne eine spezialisierte PAM-Lösung kann Ihre Organisation höheren Risiken von Sicherheitsverletzungen ausgesetzt sein, da die Kontrolle und Überwachung privilegierter Konten unzureichend ist. Dies kann zu unbefugtem Zugriff, Datenverlust und Nichteinhaltung von regulatorischen Anforderungen führen, was potenziell schwerwiegende finanzielle und reputationsschädigende Folgen nach sich ziehen kann.

13 Haftete ich persönlich im Falle von Sicherheitsverletzungen, wenn kein angemessenes PAM-Programm und -Lösung vorhanden ist?

Die persönliche Haftung kann je nach Gerichtsbarkeit und Unternehmensrichtlinien variieren. IT-Sicherheitsleiter können jedoch berufliche Konsequenzen, einschließlich Arbeitsplatzverlust oder rechtlicher Schritte, erleiden, wenn sie nachweislich fahrlässig bei der Implementierung erforderlicher Sicherheitsmaßnahmen sind. Die Gewährleistung robuster PAM-Praktiken kann diese Risiken mindern.

14 Gibt es Voraussetzungen, die ich erfüllen sollte, bevor ich mit einem spezialisierten PAM-Technologiedienst beginne?

Vor der Implementierung einer PAM-Lösung sollten Sie eine umfassende Bewertung Ihrer aktuellen Landschaft privilegierter Konten durchführen. Identifizieren und katalogisieren Sie alle privilegierten Konten, bewerten Sie deren Nutzung und verstehen Sie die damit verbundenen Risiken. Stellen Sie außerdem sicher, dass Ihre Organisation über klare Sicherheitsrichtlinien und -verfahren verfügt.

15 Welche Kosten sind mit PAM-Lösungen verbunden, und welche Faktoren bestimmen diese Kosten?

Die Kosten für PAM-Lösungen können je nach mehreren Faktoren erheblich variieren:

- **Einmalige Kosten:** Anfangskosten für Einrichtung und Implementierung, einschließlich Hardware- und Softwarebeschaffung.
- **Wiederkehrende Kosten:** Laufende Wartung, Abonnementgebühren für cloudbasierte Dienste und Supportverträge.
- **Interne Ressourcen Kosten:** Gehälter und Schulungen für Mitarbeiter, die erforderlich sind, um die Lösung intern zu verwalten und zu warten.
- **Vorteile von PAM as a Service:** Für KMUs kann PAMaaS kosteneffektiver sein, da es die Notwendigkeit für erhebliche Anfangsinvestitionen verringert und den Zugang zu Expertenmanagement ohne den Bedarf an dedizierten internen Ressourcen ermöglicht. Darüber hinaus bietet es eine schnelle Bereitstellung, kurze Beschaffungszyklen, minimalen internen Ressourcenaufwand für Vertragsabschlüsse und Onboarding sowie Flexibilität mit kurzen Kündigungsfristen.

Loslegen!

Fordern Sie Ihre Demo oder Ihr Webinar an!

Melden Sie sich jetzt für eine Demo oder ein Webinar an und entdecken Sie, wie Sie Ihre Sicherheitsmaßnahmen verbessern können. Reduzieren Sie das Risiko von Datenverletzungen und gewährleisten Sie die Einhaltung regulatorischer Standards.

Erhalten Sie Ihr Preisangebot innerhalb von 48 Stunden!

- Keine Einrichtungskosten;
- Nur eine feste monatliche Gebühr;
- Skalierbar in Benutzerzahlen;
- Transparent und vorhersehbar.

info.de@sits.com
info.ch@sits.com
info.dk@sits.com
info.nl@sits.com

www.sits.com

SITS