Top-Risiken bei Privilegierten Zugriffen und wie PAM diese minimiert?

	RISIKO	LÖSUNG
Anmeldedatendiebstahl	Gestohlene privilegierte Zugangsdaten ermöglichen es Angreifern, sich als Administratoren auszugeben und Sicherheitsbarrieren zu umgehen. Der Diebstahl von Zugangsdaten gehört zu den häufigsten Einstiegspunkten bei Cyberangriffen.	✓ Strenge Authentifizierung durchsetzen. ✓ Zugriffsrechte einschränken: Gewähren Sie Mitarbeitern nur Zugriff auf die Daten und Tools, die für ihre Rolle erforderlich sind. ✓ Starke Passwort-Richtlinien einführen: Kritische Konten sollten mit starken Passwörtern von mindestens 16+ Zeichen geschützt werden.
Interne Bedrohungen	Mitarbeiter, Dienstleister oder Administratoren mit erweiterten Rechten können ihre Privilegien missbrauchen - entweder böswillig oder versehentlich. Dies kann zu Datenlecks oder Systemausfällen führen.	✓ Das Prinzip der geringsten Privilegien anwenden. ✓ Privilegierte Sitzungen in Echtzeit überwachen. ✓ Genehmigungs-Workflows für sensible Aktionen anwenden.
Generische und unverwaltete Konten	Gemeinsam genutzte „Admin“-Konten oder vergessene Systemkonten schaffen blinde Flecken, in denen die Verantwortlichkeit verloren geht. Angreifer können diese nicht verwalteten Konten unbemerkt ausnutzen.	✓ Alle privilegierten Konten identifizieren. ✓ Generische Logins eliminieren. ✓ Eindeutige Zugangsdaten einzelnen Benutzern zuordnen.
Verbindung mit kompromittiertem Gerät	Wenn sich ein privilegierter Benutzer von einem infizierten Endpunkt aus verbindet, können Angreifer Sitzungen übernehmen und Malware in kritische Systeme einschleusen.	✓ Sichere Zugangsgateways durchsetzen. ✓ Gerätezustand prüfen, bevor Zugriff gewährt wird. ✓ Riskante Verbindungen isolieren.
Übertragung infizierter Dateien	Privilegierte Benutzer teilen häufig sensible Dateien zwischen verschiedenen Systemen aus. Wenn eine Datei kompromittiert wird, kann sich Malware mit erhöhten Berechtigungen schnell verbreiten.	✓ Optionen für die Dateiübertragung einschränken. ✓ Dateien vor dem Hochladen auf Bedrohungen scannen. ✓ Alle privilegierten Datenbewegungen protokollieren.
Operative Ineffizienz	Ohne Automatisierung verlangsamt die manuelle Verwaltung privilegierter Konten die IT-Teams, erhöht die Fehlerquote und stört die Arbeitsabläufe.	✓ Bereitstellung automatisieren. ✓ Genehmigungsprozesse optimieren. ✓ Zugriffsprozesse standardisieren, Effizienz erhöhen, Kosten senken.
Compliance-Verstöße	Vorschriften wie die DSGVO, NIS2 und der ISO-27001-Standard erfordern strenge Kontrollen für privilegierten Zugriff. Schwache Überwachung oder fehlende Audit-Trails können zu hohen Bußgeldern führen.	✓ Bereitstellung automatisieren und Genehmigungen vereinfachen. ✓ Zugriffsprozesse standardisieren, um Effizienz zu steigern und Kosten zu senken.

www.patecco.com

Tel.: +49 (0) 23 23 - 9 87 97 96

Ringstrasse 72 - 44627 Herne

E-Mail: info@patecco.com