AUSZUG AUS... IT DIRECTOR AUSGABE 10|2016

Privilegierte Nutzer-Accounts überwachen

Privilegierte Benutzerkonten werden zunehmend von Hackern als Einfallstor für Datendiebstahl missbraucht. Die Verwaltung dieser Accounts bedarf einer sicheren und überschaubaren Verwaltung – zum Einsatz kommen Privileged-Management-Lösungen.

von Kathrin Zieblo,
Redakteurin IT-DIRECTOR

> Nicht selten herrscht in Großunternehmen eine ziemliche Heterogenität in Bezug auf die unterschiedlichen Zugriffsbefugnisse – unabhängig von Hierarchieebene oder Gruppenzugehörigkeit – der einzelnen Mitarbeiter. Ob es um das Anlegen eines neuen Mitarbeiterkontos, den automatisierten Löschvorgang eines ausscheidenden Kollegen oder gar ein neues IT-System geht, die Benutzer- und Zugriffsverwaltung ist ein umfangreicher Prozess. Unübersichtlich wird es vor allem dann, wenn Nutzer hausintern rotieren und dabei neue Aufgaben und Kompetenzen übernehmen oder temporär in Projekten mitarbeiten. So ist es nicht erstaunlich, dass ein Vielzahl der Mitarbeiter zu umfangreiche Zugriffsrechte besitzen, die sie gar nicht oder nur selten benötigen. Eine Studie des US-amerikanischen Ponemon Institutes hat im letzten Jahr gezeigt, dass 71 Prozent der Beschäftigten aufgrund zu großzügig erteilter Zugriffsrechte Einblick in Unternehmensdaten haben, die gar nicht für ihre Augen bestimmt sind.

Doch nicht allein die zu großzügige Nutzerrechteverteilung stellt ein Risiko dar. Auch die Vielzahl sogenannter privilegierter Benutzerkonten, die häufig uneingeschränkten Zugriff auf Unternehmenssysteme haben, bedeutet eine zentrale Schwachstelle in der IT. Denn mit nur wenigen Kommandos lassen sich Infrastrukturen korrumpieren, Daten auslesen und Systeme abschalten oder irreparabel zerstören.

„In vielen Unternehmen werden privilegierte Konten immer noch mit Administratoren- oder Superuser-Ac-

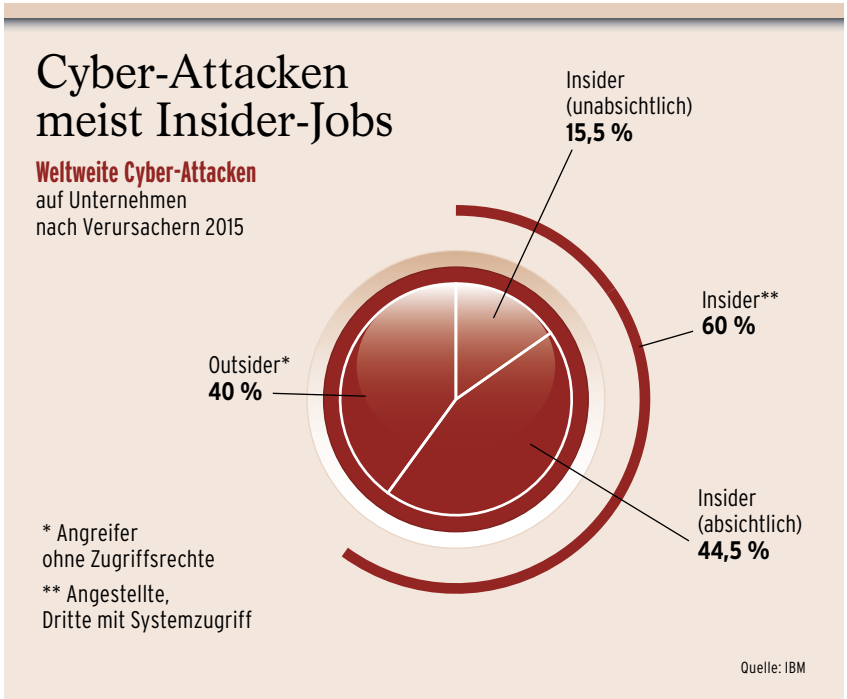
Auswahlkriterien für das Privileged Management

Eine Sicherheitslösung im Bereich des Privileged Management sollte nach Ansicht von **Ralf Nitzgen** von Allgeier IT Solutions GmbH die folgenden Parameter erfüllen:

- Über eine Inventarisierung privilegierter Accounts behält man den Überblick der sich im Einsatz befindlichen Accounts.
- Automatische Protokollierung, Auswertung sowie Alarmierung bei der Verwendung privilegierter Accounts - Transparenz ist hier wichtig. Die unbemerkte Verwendung dieser Accounts muss unbedingt vermieden werden.
- Unterstützung der Prozesse im Unternehmen: Eine Policy sollte definiert werden, die die Art des Zugriffs einzelner privilegierter Accounts festlegt. Was sogenannten Super-Usern im Unternehmen gestattet werden soll, muss in einem System abgebildet werden können. So kann auch die Einhaltung der definierten Policy systematisch geprüft werden.

couts gleichgestellt – also administrative Benutzerkonten für die Verwaltung und Steuerung der gesamten IT-Infrastruktur. Aber auch Accounts, die Zugriff auf bestimmte Applikationen oder Services haben, gehören dazu. Und das erhöht die Anzahl an privilegierten Accounts beträchtlich – sie sind vielfältiger als oft gedacht“, warnt Sandro Linder, Geschäftsführer Unisys Deutschland.

Immer häufiger werden diese Konten von Hackern als Ziel auserkoren. „Privilegierte Konten sind für Angreifer deshalb ein primäres Angriffsziel, da nach der Übernahme deren erweiterte Rechte dazu führen, einen vollen und ungehinderten Zugriff auf das System und die dort gespeicherten Daten zu erhalten“, berichtet Ralf Nitzgen, Allgeier IT Soutions GmbH. Dabei →



wird deutlich, dass die klassischen Sicherheitsmaßnahmen wie Firewall oder Anti-Virus-Scanner keinen ausreichenden Schutz bieten.

Die Bedrohung wächst allerdings nicht nur von außen. 60 Prozent aller Cyber-Attacken weltweit werden von Personen ausgeführt, die eine Zugriffsberechtigung zum IT-System besitzen. Damit weist die Nationale Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS) auf eine große Sicherheitslücke hin: die Zugangsverwaltung. Es genügt also nicht, sich um die technische Sicherheit zu kümmern. Denn wenn ein quasi berechtigter Zugriff einen Angriff darstellt, bleibt dies häufig lange unentdeckt. In 16 Prozent aller Fälle erfolgt ein Angriff „aus Versehen", weil derjenige seine Berechtigungen missversteht oder schlichtweg zu Zugriffen berechtigt ist, die eigentlich für ihn gar nicht vorgesehen sind.

Ohne eine strikte Vorgabe und Überwachung von Zugriffsberechtigungen sind Unternehmen potentiellen Attacken schutzlos ausgeliefert. Weil sich das ganze (IT-)Unternehmenssystem aber oft auf unzählige Server, Datenbanken oder Netzwerkgeräten erstreckt, die mitunter jeweils von einem anderen Administrator verwaltet werden, ist die Herausforderung entsprechend groß. Besonders problematisch sind die von mehreren Personen genutzten „Shared Accounts", weil sich nicht nachverfolgen lässt, welcher Mitarbeiter diesen wann und wozu genutzt hat. Sämtliche durchgeführten Änderungen müssen jedoch bis auf die Personenebene kontrollierbar sein.

Ursprünglich wurde das Berechtigungsmanagement in vielen Unternehmen in Identity-Access-Management (IAM)-Projekten überwacht. Inzwischen hat sich daraus eine eigene Disziplin entwickelt. Mit Privileged-Management-Lösungen (PxM) wird der Umgang mit privilegierten Benutzern, Konten, Identitäten und Zugriffen bewerkstelligt. Wie so oft widmen sich die diversen Lösungsanbieter verschiedenen Teilaspekten, sodass unterschiedliche Bezeichnungen kursieren.

Zu den gängigsten zählen das Privileged Identity Management (PIM) und das Privileged Account Management (PAM). Manchmal ist aber auch von PUM – dem Privileged User Management – die Rede.

Eines haben sie alle gemeinsam: Im Fokus steht die umfassende Administrierung und Überwachung privi-

„Unsere Stealth-Lösung sorgt zum Beispiel dafür, dass das Unternehmensnetzwerk in Mikrosegmente aufgeteilt wird, auf die nur gewisse Mitarbeiter Zugriff haben. Sie werden durch Endpunktverschlüsselung geschützt – und sind für unberechtigte Nutzer noch nicht einmal sichtbar."

Sandro Lindner von der Unisys Deutschland GmbH

Einsatzfelder für privilegierte Accounts

Sebastian Rohr von Accessec unterscheidet zwischen drei Typen von privilegierten Accounts:

- Administrative Accounts (Local oder Domain Level)
- Application Accounts für die Verbindung, Identifizierung und Authentifizierung einer Applikation
- Service Accounts (Local oder Domain Level) für die Ausführung von geplanten Aufgaben oder Services innerhalb eines definierten Sicherheitskontextes

Sebastian Rohr

Markus J. Krauss

Für den Einsatz einer PxM-Lösung gibt **Markus J. Krauss** von CA Technologies drei Tipps:

- Anmeldeinformationen schützen, Anwender mit entsprechender Sicherheit authentifizieren und proaktiv Kontrolle über ihre Verhaltensweisen und Maßnahmen ausüben, um Richtlinienverstöße, Risiken und Ausfallzeiten zu verhindern.
- Effektive Kontrollmechanismen einsetzen, um privilegierte Accounts und ihre Zugriffe zu verwalten und zu überwachen und so die Vertraulichkeit, Integrität und Verfügbarkeit von Systemen und Daten des Unternehmens zu garantieren. Notwendige Dokumentationen und Berichte zur Verfügung stellen, um gegenüber Regulierungsbehörden und Auditoren nachzuweisen, dass Vorschriften eingehalten werden.
- Den gesamten Lebenszyklus für das Privileged Access Management beschleunigen, automatisieren und vereinfachen. Privilegierten Anwendern den Zugriff über ein schnelles Single Sign-on ermöglichen und über Federated Identity in der gesamten hybriden Unternehmensinfrastruktur vom Rechenzentrum bis hin zur virtuellen Infrastruktur und zu öffentlichen und privaten Cloud-Umgebungen.

legierter Konten. Dazu gehören etwa Funktionen wie die zentrale Verwaltung von Zugangsdaten wie Passwörter sowie die Beantragung, Genehmigung und Protokollierung von administrativen Sitzungen. Ziel ist die minimale Rechtevergabe nach dem Motto „So viel wie nötig, so wenig wie möglich“. „Es bietet sich an, die Zugangskontrolle für Mitarbeiter flexibel und policybasiert nach dem Muster ‚geringste Privilegien‘ aufzusetzen, denn so kann man ohne Aufwand auf dynamische Anforderungen reagieren“, regt Markus J. Krauss, Senior Director Security Sales EMEA bei CA Technologies an.

Risiken eliminieren

In vier Schritten lassen sich die Bedrohungen, die von privilegierten Accounts ausgehen, minimieren. Zunächst gilt es für die Verantwortlichen, in Erfahrung zu bringen, welche und wie viele dieser Konten im Unternehmen überhaupt existieren. Dabei geht es um die zuverlässige Identifizierung aller Kontoarten mit erweiterten Rechten sowie um die Prüfung auf Aktualität und Relevanz. Überflüssige werden gelöscht bzw. eingeschränkt. „Dies ist nur durch regelmäßige Revisionen möglich, in deren Rahmen die Rechtmäßigkeit des Vorhandenseins eines privilegierten Accounts geprüft wird. Ein System kann hier unterstützen, indem es Auswertungen bezüglich der durchgeführten Zugriffe mithilfe privilegierter Accounts zur Verfügung stellt. Eine abnehmende Häufigkeit der Zugriffe könnte ein Indiz dafür sein, dass dieser Benutzer nicht mehr benötigt wird“, schlägt Ralf Nitzgen vor.

Im Anschluss müssen die Passwörter entsprechend verwaltet und geschützt werden. „Dies beinhaltet die Verwendung von starken kryptografischen Passwörtern, die regelmäßige Änderung dieser Passwörter sowie Aufzeichnungsmethoden“, betont Sebsatian Rohr, Technischer Geschäftsführer bei der Accessec GmbH. Darüber hinaus sollten sämtliche Zugriffe privilegierter Acounts auf die Infrastruktur überwacht, kontrolliert und protokolliert werden. Zu guter Letzt gilt es, Unregelmäßigkeiten bei der Verwendung jener Zugänge zu erkennen und entsprechend zu reagieren. „Erst wenn man weiß, wie ein Anwender seinen privilegierten Zugang nutzt, kann man unerlaubten Systemzugriff oder die Ausführung von Systemkommandos proaktiv verhindern“, kommentiert Markus J. Krauss.

Weil alle diese Aufgaben Privileged-Management-Lösungen automatisiert übernehmen, sind diese unverzichtbar geworden, um die missbräuchliche Nutzung und vor allem die zu großzügig vergebenen Zugriffsrechte als Sicherheitsrisiko zu minimieren. Bei einem akuten Sicherheitsvorfall ermöglichen sie ein sofortiges Reagieren, indem etwa aktive Verbindungen unterbrochen oder entsprechende Zugriffsberechtigungen entzogen werden. <