CYBERARK®

PRIVILEGED ACCOUNT SECURITY – EIN LEITFADEN FÜR DIE ERFOLGREICHE IMPLEMENTIERUNG

Inhalt

Privilegierte Benutzerkonten im Überblick

Täglich werden bei Angriffen auf privilegierte Benutzerkonten vertrauliche Daten im Wert von mehreren Milliarden Euro entwendet. Unter IT-Fachleuten herrscht weitgehend Einigkeit darüber, dass diese Benutzerkonten der entscheidende Schlüssel zu den wichtigsten Daten im Unternehmen sind. Um welche Konten geht es also, und wie schützen sich Unternehmen am erfolgreichsten vor potenziellen Angriffen?

Privilegierte Benutzerkonten erfordern wie normale Benutzerkonten gültige Zugangsdaten für den Zugriff auf Systeme in einem Netzwerk. Im Unterschied zu normalen Benutzerkonten verschaffen privilegierte Benutzerkonten allerdings den Anwendern einen uneingeschränkten Zugang zu unternehmenskritischen Systemen und Daten. Gelangen Eindringlinge in den Besitz von Zugangsdaten, können sie erheblichen Schaden im Netzwerk und damit im Unternehmen anrichten.

Arten von privilegierten Konten

Privilegierte Benutzerkonten existieren in Unternehmen in den unterschiedlichsten Formen und ihre Anzahl übersteigt diejenige der Mitarbeiter oft um das Doppelte oder Dreifache. Alle diese Benutzerkonten bergen erhebliche Sicherheitsrisiken, wenn sie nicht gesichert, kontrolliert und überwacht werden. In Unternehmen finden sich in der Regel folgende Arten von privilegierten Benutzerkonten:

Lokale Administrator-Konten ermöglichen einen administrativen Zugriff zum Beispiel auf Windows-Arbeitsplatzrechner. Oft wird dabei dasselbe Passwort für alle Geräte der jeweiligen Plattform verwendet. Ein derart weit verbreitetes Passwort bietet ein einfaches Ziel für fortschrittliche Angriffe.

Privilegierte administrative Benutzerkonten sind die in Unternehmensnetzwerken am häufigsten vorkommenden Typen von privilegierten Accounts. Über sie erfolgt die Verwaltung und Steuerung der gesamten IT-Infrastruktur, von Servern über Datenbanken bis hin zu den Netzwerkgeräten. Besonders problematisch sind dabei die so genannten Shared Accounts, das heißt die Nutzung desselben Passworts durch mehrere Administratoren. Dadurch kann nicht kontrolliert werden, welche Person ein solches Passwort wann und wozu verwendet hat. Eine revisionssichere Überprüfung der Verwendung eines generischen Accounts bis auf die Personenebene ist also nicht möglich.

Über Domain-Administrator-Accounts ist ein privilegierter administrativer Zugriff auf sämtliche Arbeitsplatzrechner und Server einer Domäne möglich. In der Regel gibt es zwar nur wenige dieser Konten, aber auch sie eröffnen weitreichende Zugriffsmöglichkeiten im Netzwerk und stellen deshalb ein erhebliches Sicherheitsrisiko dar.

Notfall-Benutzerkonten verschaffen Anwendern ohne besondere Berechtigungen bei Bedarf einen administrativen Zugriff auf Unternehmenssysteme. Die Nutzung derartiger Konten erfordert aus Sicherheitsgründen meistens eine Genehmigung eines Vorgesetzten. Es handelt sich dabei um ein wenig effizientes manuelles Verfahren, das zudem nicht auditierbar ist.

Auch Service Accounts für Systemdienste sind zu berücksichtigen. Sie können als privilegierte lokale oder Domain Accounts vorhanden sein. In der Regel werden bei ihnen die Zugangsdaten nur selten geändert, da Passwortänderungen bei Active-Directory- oder Domain-Service-Accounts zusätzlich eine systemübergreifende Koordination erfordern. Damit steigt aber auch das Sicherheitsrisiko für Unternehmen.

Application Accounts werden von Anwendungen für die Ausführung von Batch-Jobs und Scripts oder den Zugriff auf Datenbanken und andere Anwendungen verwendet. Über diese privilegierten Benutzerkonten ist in der Regel ein umfassender Zugriff auf Unternehmensdaten, -anwendungen und -datenbanken möglich. Da die Passwörter häufig in Applikationen, Scripts, Windows Services oder Batch-Jobs unverschlüsselt in Klartext eingebettet sind, bilden diese Accounts ebenfalls eine gravierende Lücke der Unternehmens-IT.

Schutz von privilegierten Accounts

Die fehlende Sicherung privilegierter Benutzerkonten in Unternehmensnetzen ist genau die Schwachstelle, die bei fortschrittlichen Cyber-Attacken oder Insider-Angriffen bevorzugt ausgenutzt wird. Deshalb ist eine Einführung von Sicherheitsmaßnahmen für solche Accounts unverzichtbar. Unabhängig von den verfügbaren Ressourcen gibt es praktische Lösungen für jedes Unternehmen und jedes Budget. Lösungsansätze reichen von der Einführung manueller Prozesse zur schrittweisen Verbesserung der Sicherheit bis zur Implementierung von Enterprise-Lösungen, die eine automatische Verwaltung und Überwachung privilegierter Benutzerkonten und Aktivitäten bieten.

Manueller Schutz

Es ist zwar besser, privilegierte Benutzerkonten manuell zu verwalten und zu überwachen, als überhaupt keine Sicherheitsmaßnahmen zu ergreifen. Allerdings ist es auch ein extrem zeitaufwändiger und vor allem fehlerbehafteter Prozess. Und in mittleren und großen Unternehmen und Organisationen ist es praktisch unmöglich, Tausende von privilegierten Benutzerkonten manuell zu verwalten.

Sicherheitslösungen für privilegierte Benutzerkonten

Wesentlich effizienter als die manuelle und teilweise kaum praktikable Verwaltung privilegierter Benutzerkonten ist die Implementierung einer eigenen Sicherheitslösung oder die Nutzung eines Managed Service. Enterprise-Lösungen, mit denen privilegierte Benutzerkonten und Aktivitäten verwaltet, gesichert und überwacht werden können, machen sich in Unternehmen sehr schnell bezahlt.

Bei der Implementierung einer Sicherheitslösung empfiehlt sich eine schrittweise Vorgehensweise. Es gibt Lösungen auf dem Markt, die eine mehrstufige strukturierte Umsetzung von Sicherheitskonzepten ermöglichen.

Best Practices

Privilegierte Benutzerkonten lassen sich durch verschiedene Maßnahmen verwalten und überwachen. Viele dieser Maßnahmen erfordern lediglich Prozessveränderungen, für andere hingegen werden spezielle Lösungen oder Tools benötigt. Ein 3-Phasen-Modell beschreibt den Weg zu einer zuverlässigen Identifizierung, Sicherung, Verwaltung und Überwachung privilegierter Accounts.

Einstiegslösung

Bestandsaufnahme und Reduzierung der Anzahl privilegierter Accounts im Unternehmen

Ein wesentlicher erster Schritt zur Verwaltung, Sicherung und Überwachung der privilegierten Accounts ist ihre Lokalisierung im Unternehmensnetz. Nach der Bestandsaufnahme und Ermittlung der exakten Anzahl sollten die privilegierten Benutzerkonten im Hinblick auf ihre Bedeutung und Funktion überprüft werden, wobei überflüssige Konten zur Verringerung des Verwaltungsaufwandes zu löschen sind.

Normale Benutzerkonten sollten keine privilegierten Zugriffsrechte haben

Durch eine Trennung von Konten für allgemeine und administrative Zwecke wird auch eine Erkennung des Missbrauchs privilegierter Benutzerkonten erleichtert. Zudem ist die Vergabe minimaler Zugriffsrechte ein wichtiges Element bei der Verbesserung der Netzwerksicherheit.

Einführung eines Prozesses zum Hinzufügen und Entfernen von Mitarbeitern mit privilegierten Zugriffsrechten

Bevor Mitarbeiter administrative Zugriffsrechte erhalten, sollten sie über die damit verbundenen Verpflichtungen informiert und zu den Unternehmensrichtlinien geschult werden. Regelmäßig sollte überprüft werden, ob Mitarbeiter diese privilegierten Zugriffsrechte benötigen. Beendet ein Mitarbeiter seine Tätigkeit im Unternehmen, sollten seine sämtlichen privilegierten Benutzerkonten deaktiviert werden. Außerdem sind die Passwörter für generische Accounts zu ändern, auf die der Mitarbeiter Zugriff hatte.

Keine zeitlich unbefristeten Passwörter vergeben

Passwörter sollten regelmäßig geändert werden, um die mit Passwort-Entschlüsselungstools oder der Weitergabe von Passwörtern an andere Mitarbeiter verbundenen Gefahren zu verringern.

Passwörter sicher speichern

Zur Speicherung privilegierter Passwörter sollte ein sicheres System mit Verschlüsselung eingesetzt werden. Privilegierte Zugangsdaten sollten nicht in Briefumschlägen, Excel-Tabellen oder Textdateien abgelegt werden.

Sorgen Sie nach Möglichkeit dafür, dass alle Maßnahmen im Zusammenhang mit gemeinsam genutzten administrativen Accounts einer bestimmten Person zugeordnet werden können.

Zugangsdaten sollten nicht von mehreren Personen gemeinsam genutzt werden.

Erweiterte Lösung

Passwörter für privilegierte Benutzerkonten werden alle 30 oder 60 Tage automatisch geändert.

Privilegierte Passwörter sollten regelmäßig geändert werden. Sie sollten komplex sein und nur einmal vergeben werden. Die Passwörter dürfen allerdings auch keine extreme Komplexität aufweisen, damit die Benutzer nicht in Versuchung kommen, sie aufzuschreiben.

Verwenden Sie Einmal-Passwörter, die nur für eine Session oder Transaktion gültig sind.

Das häufige Ändern von Passwörtern – gegebenenfalls sogar nach jeder Nutzung – erhöht den Aufwand und die Kosten für den Angreifer bei einer versuchten Ermittlung der Zugangsdaten und senkt daher das Sicherheitsrisiko.

Zeichnen Sie Sessions bei wichtigen Systemen und Servern sowie beim Zugriff durch Dritte auf.

Aktivitäten privilegierter Benutzerkonten auf wichtigen Systemen und Servern sowie Zugriffe durch Dritte sollten überwacht und erfasst werden.

Eliminieren Sie bei Service Accounts die Möglichkeit interaktiver Anmeldungen durch Mitarbeiter.

Die interaktive Nutzung von Service Accounts stellt eine erhebliche Schwachstelle dar, die sich relativ einfach beseitigen lässt, sobald alle vorhandenen Benutzerkonten erfasst sind.

Einführung eines Prozesses zur Änderung hart kodierter oder eingebetteter Passwörter für Scripts und Service Accounts

Ohne Nutzung adäquater Prozesse kann eine Änderung hart kodierter Passwörter negative Auswirkungen auf die gesamte Infrastruktur haben. Eine Lösung, die eine automatisierte Änderung eingebetteter Passwörter in Scripts und Service Accounts ermöglicht, kann die Sicherheit erhöhen, ohne zusätzliche Risiken zu verursachen.

Führen Sie gezielte Kontrollen zur Verwendung administrativer privilegierter Accounts ein und überwachen sie auch Anomalien

Durch die Protokollierung aller Benutzeraktivitäten und die Generierung von Alarmen bei ungewöhnlichem Verhalten erhalten Sie zusätzliche Informationen über den Zugriff auf privilegierte Benutzerkonten und deren Nutzung. Damit lässt sich der Zeitaufwand für die Prüfung potenzieller Sicherheitsvorfälle und/oder -verletzungen erheblich reduzieren.

.

Umfassende Lösung

Einsatz automatisierter Tools zur Verwaltung privilegierter Accounts

Eine manuelle Verwaltung und Sicherung privilegierter Benutzerkonten im gesamten Unternehmen ist schwer zu realisieren und außerdem extrem fehlerbehaftet. Wesentlich effizienter sind Lösungen mit einem hohen Automatisierungsgrad.

Nutzung einer Multifaktor-Authentifizierung für sämtliche administrativen Zugriffe

Eine Multifaktor-Authentifizierung bietet für privilegierte Identitäten einen zusätzlichen Schutz vor fortschrittlichen Angriffen. Viele Systeme unterstützen allerdings keine mehrstufigen Authentifizierungskonzepte, beispielsweise ältere Netzwerkgeräte oder Legacy-Applikationen. Durch den Einsatz einer Privileged-Account-Security-Lösung, die eine mehrstufige Authentifizierung bietet, entfällt die Notwendigkeit der Unterstützung durch diese Zielgeräte oder -applikationen.

Implementierung einer Lösung zur automatischen Verifizierung von Passwörtern

Beim Management privilegierter Benutzerkonten ist eine Automatisierung unverzichtbar. Da kontinuierlich neue Benutzerkonten angelegt und andere gelöscht werden, müssen die Passwörter automatisch verwaltet und überprüft sowie gegebenenfalls kontrolliert zurückgesetzt werden.

Regelmäßiges Ändern und Überprüfen hart kodierter Passwörter in Anwendungen

Durch eine Überwachung aller Accounts und die Einführung einer automatischen Verwaltung von Zugangsdaten wird eine regelmäßige Passwortänderung ohne zusätzliche Risiken möglich. Nur unter Einbeziehung der Application Accounts werden die mit privilegierten Benutzerkonten in der Unternehmensinfrastruktur verbundenen Risiken beseitigt.

Einführung einer Lösung zur direkten Verbindung mit einem Zielsystem ohne Passwortanzeige

Wenn der Benutzer privilegierte Passwörter nicht einsehen kann, wird ein weiterer Risikofaktor eliminiert. Gleichzeitig sinkt damit der Administrationsaufwand für gemeinsam genutzte Accounts und die Benutzerfreundlichkeit wird erhöht.

Implementierung eines Gateways zur Unterbindung des direkten Zugriffs privilegierter Benutzer auf vertrauliche Systeme und Daten der IT-Infrastruktur

Ein Gateway zwischen Benutzer und unternehmenskritischen IT-Systemen reduziert die Bedrohung durch Malware. Außerdem müssen privilegierte Zugangsdaten dabei nicht auf Endgeräten wie Desktops hinterlegt werden.

Einführung eines Prozesses für die Genehmigung von privilegierten Zugriffen nach dem Vier-Augen-Prinzip und Integration von Helpdesk-Ticketing-Systemen

Der Einsatz des Vier-Augen-Prinzips verhindert, dass böswillige Insider ihre privilegierten Benutzerkonten missbräuchlich nutzen, und ermöglicht eine klare Nachvollziehbarkeit der Benutzerzugriffe.

Aufzeichnung aller Sessions mit privilegierten Zugriffsrechten

Alle Aktionen von privilegierten Benutzerkonten sollten grundsätzlich aufgezeichnet werden. Session-Protokolle und Video-Aufzeichnungen ermöglichen auch forensische Analysen.

Frühzeitiges Erkennen von böswilligem Verhalten

Eine wichtige Komponente einer innovativen Privileged-Account-Security-Strategie ist die Möglichkeit, bereits ein verdächtiges Verhalten bei der Nutzung privilegierter Benutzerkonten erkennen zu können.

Fazit

Angreifer nutzen Zugangsdaten und/oder privilegierte Benutzerkonten kompromisslos aus. Angesichts der jüngsten Vorfälle können Unternehmen es sich nicht leisten, dies zu ignorieren. Die regelmäßigen Berichte über Sicherheitslücken in großen wie kleinen Unternehmen weltweit sprechen für sich. Es gibt keine Branche, in der nicht das Risiko besteht, dass privilegierte Benutzerkonten missbräuchlich genutzt werden.

Bei der Suche nach einer Lösung, mit der privilegierte Benutzerkonten aktiv geschützt und überwacht werden können, kommt es darauf an, die Anforderungen des Unternehmens mit den verfügbaren Alternativen abzugleichen und die optimale Lösung nach Best-Practices-Gesichtspunkten auszuwählen. Entscheidend für eine zuverlässige Sicherung privilegierter Benutzerkonten ist zudem eine kontinuierliche Anpassung der Sicherheitsmaßnahmen an geänderte Unternehmensanforderungen oder Sicherheitsbedrohungen.