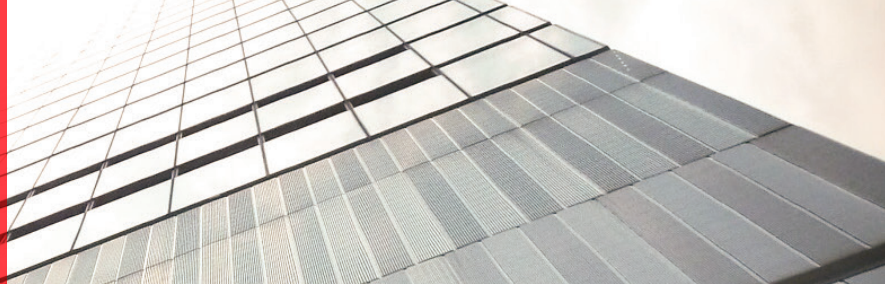

Centrify Privilege Elevation Service

Zugriff mit geringstmöglichen Rechten zur Verkleinerung der Angriffsfläche

In den letzten Jahren wurde deutlich, dass Angreifer sich nicht mehr nur „einhacken", um an geheime Daten zu gelangen: Sie melden sich einfach mithilfe von schwachen, gestohlenen oder anderweitig kompromittierten privilegierten Zugriffsdaten an. Sobald sie eingedrungen sind, machen sie sich die Tatsache zunutze, dass viele Organisationen ihren Administratoren zu viele Rechte einräumen. So können Hacker sich im gesamten Netzwerk ausbreiten, wo sie nach weiteren privilegierten Benutzerkonten und Zugriffsdaten suchen, die ihnen Zugriff auf den kritischsten Teil der Infrastruktur einer Organisation und auf deren sensibelste Daten ermöglichen. Zero Trust Privilege verlangt, dass nur gerade ausreichende Just-in-time-Privilegien erteilt werden, um die Möglichkeit, sich entlang des gesamten Netzwerks zu bewegen, möglichst gering zu halten.

Achtung: Zu viele Privilegien

Das Konzept der geringstmöglichen Privilegien ist verbreiteter, als Sie denken. Denken Sie an die physischen Zugangskontrollen in Ihrem Büro: Verschiedene Benutzergruppen verfügen über unterschiedliche Zugangsrechte. Um Zugang zu bestimmten Bereichen zu erhalten, müssen Sie einen Antrag stellen, der genehmigt werden muss. Im Bereich der physischen Sicherheit ist dieses Konzept allgemein anerkannt, und dasselbe Prinzip gilt für logische Sicherheit. Es gilt bei der Gewährung von granularem rollenbasiertem Zugriff auf privilegierte Ressourcen.

Ein weiterer Grund dafür, nur geringstmögliche Privilegien zu vergeben, ist es, die Möglichkeit der Seitwärtsbewegung im Netzwerk einzuschränken. Dies ist die häufigste Art, auf die Angreifer Zugriff auf sensible Daten erhalten: Sie beginnen an einem Ort und bewegen sich dann seitwärts, bis sie das finden, wonach sie suchen. Wenn wir die Bereiche eingrenzen, auf die sie zugreifen können, können wir Seitwärtsbewegungen aufhalten. Genauso, wie niemand einen einzigen Schlüssel/Ausweis haben sollte, mit dem er überall Zugang erhält, sollten Sie auf keinen Fall das Root-Konto auf einem Server nutzen, da es zu viele Zugriffsrechte gewährt und dem jeweiligen Benutzer – nennen wir ihn „Bob" – nicht zugeordnet werden kann. Stattdessen sollte sich Bob direkt beim Zielsystem mit seinen eigenen Administratorenrechten anmelden, die ihm lediglich ermöglichen, eine bestimmte Reihe von Servern neu zu starten. Wenn er die Konfiguration ändern oder auf ein anderes Zielsystem zugreifen möchte, muss er die zugehörigen Zugriffsrechte für einen festgelegten Zeitraum beantragen. Der Zugriff kann automatisch oder über Dienste wie ServiceNow® oder SailPoint Technologies® bereitgestellt werden. Zudem kann eine Multi-Faktor-Authentifizierung (MFA) eingerichtet werden. Nach Abschluss werden Bobs Rechte wieder auf das Nötigste beschränkt.

Zugriff mit geringstmöglichen Rechten zur Verkleinerung der Angriffsfläche

Der Centrify Privilege Elevation Service verringert das Risiko für Cyberangriffe, das durch Personen mit zu vielen Berechtigungen entsteht. Der Dienst bietet Kunden die Möglichkeit, die optimale Vorgehensweise in Bezug auf geringstmögliche Just-in-time-Privilegien umzusetzen und dadurch mögliche Schäden durch Sicherheitsverletzungen zu verringern.

ERWEITERUNG VON BERECHTIGUNGEN

Schützen und verwalten Sie hochgradig granulare Privilegien auf Windows-, Linux- und UNIX-Systemen und verringern Sie so mögliche Schäden durch Sicherheitsverletzungen. Lassen Sie Benutzer sich mit ihren eigenen Konten anmelden, um diese später zuordnen zu können, und erweitern Sie Privilegien auf Grundlage ihrer Rolle innerhalb der Organisation.

ZEITBASIERTE ROLLENZUWEISUNG

Verringern Sie das Sicherheitsrisiko, indem Sie Administratoren ermöglichen, systematisch neue Rollen anzufordern, deren Rechte sie für die Durchführung ihrer Aufgaben benötigen. Durch die Einrichtung von Zugriffsanfragen für privilegierte Rollen können Unternehmen langfristige oder temporäre Berechtigungen und Rollen mit einem flexiblen Just-in-time-Modells vergeben, das sich an die sich stetig verändernden Geschäftsbedürfnisse anpasst.

VERWALTUNG ZUGEWIESENER ROLLEN UND RICHTLINIEN

Durch zentrale Rollen, Rechte und Privilegienrichtlinien wird die Verwaltung in heterogenen Umgebungen (UNIX, Linux und Windows) vereinfacht. Richtlinien werden in der Active Directory getrennt von anderen gemeinsamen Objekten gespeichert, um das Delegieren an Serveradministratoren und die Trennung von Aufgaben von Active-Directory-Administratoren zu unterstützen und so zu verhindern, dass Serveradministratoren für sie nicht vorgesehene Active-Directory-Objekte verwalten. All dies wird ohne Modifikationen am Active-Directory-Schema erreicht.

MFA BEI BERECHTIGUNGSERWEITERUNG

MFA bei Anmeldung ist eine hervorragende Best Practice – besonders für Administratoren. Zum Schutz vor böswilligen Akteuren sollte dies jedoch durch eine MFA bei der Erweiterung von Privilegien ergänzt werden, um sicherzustellen, dass lediglich autorisierte Personen privilegierte Anweisungen ausführen, indem vor der Durchführung privilegierter Anweisungen eine MFA erforderlich ist.

Geringstmögliche Privilegien auf Windows-, Linux- und UNIX-Systemen

Verringern Sie das Risiko eines Angriffs durch Personen mit zu vielen Berechtigungen und die routinemäßige Verwendung von gemeinsam genutzten privilegierten Benutzerkonten. Die Implementierung von Zugriffen mit geringstmöglichen Berechtigungen schränkt den möglichen Schaden von Sicherheitsverletzungen ein. Der flexible, hochgradig granulare Centrify Privilege Elevation Service bietet daher Ihren Benutzern die Möglichkeit, ihre Aufgaben zu erledigen, verringert das Risiko und vereinfacht die Implementierung eines Just-in-time-Modells mit geringstmöglichen Berechtigungen dank rollenbasierter Zugriffskontrollen.

- Mithilfe rollenbasierter Zugriffskontrollen wird die Einführung von Zugriffsrechten mit geringstmöglichen Berechtigungen zum Kinderspiel. Die patentierte Zonen-Technologie von Centrify bietet äußerst granulare, rollenbasierte Zugriffskontrollen, die die Implementierung eines Modells geringstmöglicher Berechtigungen auf Windows-, Linux- und UNIX-Systemen vereinfachen.
- Sichern Sie Ihre Windows-, Linux- und UNIX-Systeme, indem Sie genau kontrollieren, wer auf was wann zugreifen kann. Im Gegensatz zu dezentralen Ein-Zweck-Tools wie sudo bietet Centrify die Möglichkeit, dynamische Privilegien zu konfigurieren, sodass Benutzer Berechtigungen nur in bestimmten Momenten, für eine gewisse Dauer und auf bestimmten Servern erweitern können. Darüber hinaus können Sie zum weiteren Schutz Ihrer sensiblen Daten Server auf Grundlage von Zeit und Vertrauensbeziehungen isolieren. Dies hilft dabei, die Möglichkeit von Seitwärtsbewegungen weiter einzuschränken.
- Centrify stellt eine Reihe von leistungsfähigen Tools zur Verfügung, die die Einführung und Verwaltung eines Modells geringstmöglicher Zugriffsrechte vereinfachen.

Vereinfachte Verwaltung heterogener Umgebungen

Durch zentrale Rollen, Rechte und Privilegienrichtlinien wird die Verwaltung in heterogenen Umgebungen (UNIX, Linux und Windows) vereinfacht. Die Richtlinien der Centrify Zero Trust Privilege Services werden in der Active Directory getrennt von anderen gemeinsamen Objekten gespeichert, um das Delegieren an Serveradministratoren und die Trennung von Aufgaben von Active-Directory-Administratoren zu unterstützen und so zu verhindern, dass Serveradministratoren für sie nicht vorgesehene AD-Objekte verwalten. Zusätzlich bietet Centrify ein hierarchisches Richtlinienmodell, um gängige Unternehmens-Managementmodelle für zentralisierte Top-down-Kontrollen mit zentral verwalteten gemeinsamen Rollen und Rechten zu unterstützen, während es gleichzeitig ein abteilungs-, rollen- und computerbasiertes Delegieren an untergeordnete Administratorenteams ermöglicht, denen entsprechende Zugriffsrechte auf bestimmte Systeme gewährt werden.

- Das konsistente und strukturierte Richtlinienmodell sowohl für Windows, als auch für Linux und UNIX sorgt für Konformität und geringere Wartungskosten.
- Die Verwaltung von Windows-, Linux- und UNIX-Richtlinien in der Active Directory sorgt für einen konsistenten Sicherheitsansatz privilegierter Zugriffsrechte und führt darüber hinaus zur angemessenen Trennung der Aufgaben zwischen Richtlinieninhabern und Systemadministratoren. Dieser homogene Ansatz für heterogene Umgebungen ermöglicht kürzere Audits und vereinfacht die Einhaltung der Konformität.

Self-Service-Rollenanfragen für Just-in-time-Berechtigung

Verringern Sie das Sicherheitsrisiko, indem Sie Administratoren ermöglichen, systematisch neue Rollen anzufordern, deren Rechte sie für die Durchführung ihrer Aufgaben benötigen. Durch die Einrichtung von Zugriffsanfragen für privilegierte Rollen können Unternehmen temporäre Berechtigungen und Rollen mit einem flexiblen Just-in-time-Modells vergeben, das sich an die sich stetig verändernden Geschäftsbedürfnisse anpasst.

- Geben Sie Administratoren die Möglichkeit, sich mit ihrem eigenen Benutzerkonto anzumelden und ihre Berechtigungen durch das systematische Anfordern einer neuen Rolle zu erweitern, um ihre Aufgaben zu erledigen. Ein Self-Service-Anfragesystem vereinfacht das Anfordern einer bestimmten Rolle für einen bestimmten Zeitraum. Wenn die Anfrage genehmigt wird, werden die Berechtigungen nach Ablauf der zuvor festgelegten Zeitspanne automatisch wieder entzogen.
- Verkleinern Sie die Angriffsfläche, indem Sie temporären, an gewisse Zeiten gebundenen Zugriff auf privilegierte Benutzerkonten gewähren und Rollen für Just-in-time-Berechtigungen vergeben. Gewähren Sie IT-Administratoren Zugriff auf die Zugangsdaten für privilegierte Benutzerkonten, Remote-Management-Sitzungen oder wenn diese ihre Rolle vorübergehend ändern müssen, um zusätzliche Administratorenaufgaben durchzuführen.
- Verringern Sie das Risiko von Datensicherheitsverletzungen, indem Sie Genehmigungen für IT-Benutzer einführen, die Zugriff auf Systeme mit privilegierten Rollen benötigen. IT-Benutzer der ServiceNow® Asset Management and Configuration Management Database (CMDB) oder von Identitätssteuerungs- und -verwaltungslösungen von SailPoint Technologies® können eine Anfrage bezüglich der Nutzung einer Rolle mit Privilegien für den Zugriff auf bestimmte Server für eine festgelegte Zeitspanne stellen. Die Anfragen werden über einen Workflow-basierten Managementprozess genehmigt oder abgelehnt.

Überprüfen, dass der richtige privilegierte Benutzer die privilegierten Anweisungen ausgibt

Die Ausführung einer privilegierten Anweisung sollte stets vor böswilligen Akteuren geschützt werden, indem sichergestellt wird, dass nur autorisierte Personen sowie Anwendungen und Dienste mit entsprechenden Rechten privilegierte Aktivitäten durchführen können. Centrify bietet eine hostbasierte Technologie, die nicht umgangen werden kann, um eine MFA bei der Durchführung privilegierter Aktionen auf Linux-, UNIX- und Windows-Servern durchzusetzen.

- Egal, ob Sie die MFA bei System- oder Tresoranmeldung oder im Rahmen der Erweiterung von Privilegien anwenden: Die Integration des Centrify Privileged Access Service bietet einen konsistenten und leicht zu wartenden MFA-Dienst für sämtliche privilegierten Zugriffe. Mit der umfangreichsten Bandbreite an Authentifikatoren und einem vorkonfigurierten Support für NIST Assurance Level 2 und 3.
- Ein „Zero Trust Privilege"-Ansatz setzt voraus, dass stets geprüft wird, wer privilegierten Zugriff anfordert. UNIX-/Linux-Administratoren, die sich zur Kontrolle des Systems anmelden, gelten nicht als Risiko und sollten nicht zu einer MFA gezwungen werden. Die Ausführung sämtlicher privilegierter Anweisungen sollte jedoch so konfiguriert werden, dass zuvor eine MFA unter Verwendung der zentralen MFA-Dienste von Centrify erforderlich ist.
- Ein „Zero Trust Privilege"-Ansatz setzt voraus, dass stets geprüft wird, wer privilegierten Zugriff anfordert. Von Windows-Administratoren, die privilegierte Anweisungen ausführen müssen, kann eine MFA verlangt werden, bei der sie ihr AD-Passwort erneut authentifizieren oder ihre Identität mit einer Smartcard bestätigen müssen.

Unsere Mission besteht darin, die Hauptursache für Sicherheitsverletzungen – den Missbrauch privilegierter Zugriffsrechte – zu stoppen. Centrify ermöglicht es seinen Kunden mit einem Cloud-fähigen „Zero Trust Privilege"-Ansatz, den Zugang zu Infrastruktur, DevOps, Cloud, Containern, Big Data und anderen Angriffsflächen in modernen Unternehmen zu sichern. Weitere Informationen erhalten Sie unter www.centrify.com.

Hauptsitz (USA) +1 (669) 444 5200
Europa, Naher Osten und Afrika (EMEA)
+44 (0) 1344 317950
Asien/Pazifik +61 1300 795 789
Brasilien +55 11 3958 4876
Lateinamerika +1 305 900 5354
sales@centrify.com

www.centrify.com