LÖSUNG IM ÜBERBLICK

Wie schützen Sie privilegierte Anmeldeinformationen in herkömmlichen und virtuellen Rechenzentren, privaten und öffentlichen Clouds und hybriden Umgebungen?

ca technologies

Anmeldeinformationen für privilegierte Accounts zu verwalten und zu schützen, ist eine wesentliche Voraussetzung zur Minimierung von Risiken und zur Erfüllung von Compliance-Anforderungen. Die Unternehmen sollten Lösungen für das Passwortmanagement privilegierter Accounts im Hinblick auf Kontrolltiefe, Leistungsumfang und den Grad ihrer Cloud-Unterstützung evaluieren. CA Privileged Access Manager erfüllt alle drei dieser Anforderungen und stellt eine Lösung der nächsten Generation für das Management privilegierter Anmeldeinformationen bereit, die die IT-Risiken reduziert, die Unternehmenseffizienz erhöht und bereits getätigte Investitionen schützt, da sie herkömmliche und virtualisierte Infrastrukturen wie auch hybride Cloud-Infrastrukturen unterstützt.

Kurzfassung

Ausgangssituation

Durch den vermehrten Einsatz von Virtualisierung und Cloud-Computing rückt ein uraltes Problem wieder in den Vordergrund, das allerdings mit ganz neuer Komplexität daherkommt: die effektive Verwaltung und der wirksame Schutz von Passwörtern privilegierter Accounts. Die Verwaltung privilegierter Passwörter in herkömmlichen Infrastrukturen (Netzwerkausrüstung, Server, Mainframe usw.) stellt bereits seit längerer Zeit ein großes Security- und Complianceproblem dar. Noch komplizierter wird die Sache durch die unzähligen privilegierten Anmeldeinformationen, die fest in Anwendungen einprogrammiert sind. Zu solchen Anmeldeinformationen zählen beispielsweise SSH-Schlüsselpaare und die PEM-codierten Schlüssel für den Zugriff auf die Ressourcen von Amazon Web Services (AWS).

Chance

Wem es gelingt, privilegierte Anmeldeinformationen im gesamten hybriden Unternehmen zu schützen, kann die Risiken durch externe Angreifer und böswillige Insider in den Griff bekommen. Die Unternehmen haben nun die Möglichkeit, Ansätze für das Privileged Access Management in die Praxis umzusetzen, die die wichtigsten zwölf Anforderungen erfüllen, die in diesem Dokument dargelegt sind. So werden sie in der Lage sein, Risiken wie nicht bestandene Audits, Verstöße gegen Vorschriften, den Verlust erfolgskritischer Daten und teure Betriebsunterbrechungen zu minimieren – die allesamt auf ungeschützte privilegierte Accounts zurückzuführen sind.

Nutzen

CA Privileged Access Manager enthält umfassende Kontrollmechanismen für den Schutz und das Management aller möglichen Arten von Anmeldeinformationen für beliebige Ressourcentypen, wo auch immer diese sich befinden. Unterstützt werden natürlich auch die hybriden Cloud-Umgebungen von heute. So können die Unternehmen ihre Risiken noch besser eindämmen, die Betriebskosten senken und die betriebliche Auslastung weiter optimieren als mit alternativen Ansätzen, die keine vergleichbare Detailtiefe der Kontrollen, kein so umfassendes Funktionsspektrum und nicht dieselbe Unterstützung für Cloud-Computing bieten.

Abschnitt 1:

Passwortmanagement für privilegierte Accounts: ein paar Grundlagen

Passwörter privilegierter Anwender (nachfolgend als „privilegierte Passwörter“ bezeichnet) unterscheiden sich von den „normalen“ Anwenderpasswörtern darin, dass sie uniform Zugriff auf die sensibelsten Ressourcen des Unternehmens gewähren. Gemeint sind damit die Administratoraccounts (z. B. „admin“, „root“, „SYS“ und „sa“) und die damit verknüpften Fähigkeiten zur Konfiguration und Steuerung der IT-Infrastruktur eines Unternehmens. Macht man sich die damit verbundenen Risiken bewusst, wird klar, warum die Verwaltung und der Schutz dieser Anmeldeinformationen so wichtig sind. Dies äußert sich auch in den zahlreichen Anforderungen, die in häufig zitierten Securitystandards wie NIST Special Publication 800-53 und Payment Card Industry Data Security Standard (PCI-DSS) enthalten sind.

Abgesehen von den gesetzlichen Anforderungen ist das Management privilegierter Passwörter nicht nur eine gute Sache aus Sicht des Risikomanagements, sondern auch ein unverzichtbares Instrument, um die vielen unsicheren Praktiken, die in den Unternehmen von heute üblich sind, abzuschaffen. Schwache, veraltete oder offengelegte Passwörter (z. B. weil sie auf einer Haftnotiz notiert werden oder in einer Excel-Tabelle erfasst sind), zu viele Passwörter, gemeinsam genutzte Passwörter, keine klare Zurechenbarkeit für gemeinsam genutzte Accounts, keine Option für eine strenge Authentifizierung oder für einen zentralisierten Widerruf von Passwörtern – all dies sind Probleme, mit denen man sich im heutigen Unternehmensalltag immer wieder konfrontiert sieht.

Laut dem Bericht von Verizon zu Datenschutzverletzungen 2015 waren 95 Prozent der Verstöße auf gestohlene Anmeldeinformationen zurückzuführen, während 10 Prozent das Ergebnis des Missbrauchs von Anmeldeinformationen durch vertrauenswürdige Insider waren.[1]

Das wahre Problem ist jedoch, dass jeder dieser Missstände zu erfolgreichen Phishing-Angriffen und zielgerichteten Attacken und somit auch zu Datendiebstahl führen kann, ganz zu schweigen von möglichen Complianceverstößen. Dies wird auch durch folgende Untersuchung belegt: Laut dem Bericht von Verizon zu Datenschutzverletzungen in 2015 waren 95 Prozent der Verstöße auf gestohlene Anmeldeinformationen zurückzuführen, während 10 Prozent das Ergebnis des Missbrauchs von Anmeldeinformationen durch vertrauenswürdige Insider waren.[1] Erkenntnisse wie diese machen mehr als deutlich, warum die Unternehmen von heute eine Lösung der Enterprise-Klasse wie z. B. CA Privileged Access Manager für das Management und den Schutz privilegierter Anmeldeinformationen sowie für die Access Control benötigen.

Die Folgen der hybriden Cloud

Die oben dargelegten herkömmlichen Probleme sind jedoch nur die Spitze des Eisbergs. Da hybride Cloud-Konfigurationen so große Vorteile bieten, im Hinblick auf die Kosten, Anpassbarkeit und Reaktionsfähigkeit, aber auch weil die IT-Services und Anwendungen hier sowohl die herkömmliche als auch die virtualisierte Infrastruktur im Unternehmens- und Cloud-Rechenzentrum nutzen, ist eine weitläufige Verbreitung dieses Modells unumgänglich. Neben all diesen Vorteilen bringen hybride Clouds aber auch einige neue Herausforderungen für das Management privilegierter Passwörter mit sich, darunter z. B.:

- Größeres Volumen: Da die betrieblichen Anforderungen steigen und sich virtuelle Maschinen immer einfacher bereitstellen lassen, fordern auch mehr Entitäten einen privilegierten Zugriff (und damit privilegierte Passwörter).
- Größerer Umfang: Durch die geballte Kraft der Virtualisierungs- und Cloud-Management-Konsolen kommt eine neue Art von privilegierter Ressource bzw. privilegiertem Account hinzu.
- Größere Dynamik: Neue Server/Systeme können bei Bedarf hinzugefügt werden, abgesehen von den Massenvorgängen (z. B. 10, 20 oder mehr gleichzeitig).
- Es besteht die Möglichkeit von Identitätsinseln, da jeder Cloud-Service über einen eigenen Identitätsspeicher und eine eigene Infrastruktur für die Identitäten verfügt.[2]

Abgesehen von den Herausforderungen der hybriden Cloud müssen IT-Security-Manager beim Management privilegierter Passwörter noch zwei weitere Aspekte berücksichtigen, wenn sie infrage kommende Lösungen evaluieren. Erstens müssen sie berücksichtigen, dass Passwörter auch zwischen Rechnern (Machine-to-Machine) bzw. Anwendungen (Application-to-Application, A2A) verwendet werden. In diesem Fall sind die Passwörter, die von einem System oder einer Anwendung genutzt werden, um Zugriff auf ein anderes System oder eine andere Anwendung zu erhalten, in die zugreifende Anwendung fest codiert, oder sie werden in einer Konfigurationstextdatei zur Verfügung gestellt. Der zweite Aspekt betrifft ein Problem, das häufig übersehen wird, nämlich die Tatsache, dass die meisten Unternehmen auch über Tausende von Schlüsseln (z. B. für die SSH-Implementierung) verfügen, die nach wie vor als Authentifizierungsinformationen für privilegierte Accounts verwendet werden, auch wenn es sich dabei nicht um herkömmliche, phrasenbasierte Passwörter handelt. Aber auch diese müssen verwaltet und geschützt werden, um die entsprechenden Risiken zu minimieren.

Aus all dem können wir nun schlussfolgern, dass das Management privilegierter Passwörter im Zeitalter hybrider Clouds heute wichtiger und komplexer ist als je zuvor.

Abschnitt 2:

Die Privileged Access Management-Lösung von CA Technologies

CA Privileged Identity Manager ist eine umfassende Lösung für das Privileged Access Management. Als solche ist die Lösung nicht nur in der Lage, in hybriden Cloud-Umgebungen den Zugriff zu steuern und die Aktivitäten privilegierter Anwender zu überwachen und aufzuzeichnen, sondern sie umfasst auch Funktionen, die in einer Lösung der nächsten Generation für das Management privilegierter Passwörter unverzichtbar sind. Die IT-Security-Teams sollten anerkennen, dass das Management und der Schutz von Passwörtern nicht nur an sich eine nützliche Sache ist, sondern dies auch einem höheren Zweck dient. So ist dies vor allem der erste (oder ergänzende) Schritt im umfassenderen, aber nicht minder wichtigen Prozess der tatsächlichen Kontrolle und Verwaltung des Zugriffs auf risikolastige Ressourcen. Der Unterschied mag nur minimal erscheinen, tatsächlich jedoch ist er recht groß. Da in der Praxis funktionale Implementierungen von Authentifizierungsmechanismen (also Passwörtern) und Access Controls jedoch fast immer miteinander auftreten, werden sie von uns häufig in einen Topf geworfen.

Auf jeden Fall folgt das Design der Funktionen für das Management privilegierter Passwörter, die in CA Privileged Access Manager integriert sind, denselben Prinzipien wie diejenigen in der restlichen Lösung. Wir möchten vor allem eine Lösung anbieten, die nicht nur umfassende Kontrollen und Funktionen für zahlreiche Zielressourcen und Anwendungsszenarien bereithält, sondern die dies auch auf vereinbare Weise mit den Bereitstellungsoptionen, Methoden und Architekturen der Cloud-Ära tut.

Umfassende Kontrollen

Wenn es darum geht, Lösungen für das Management privilegierter Passwörter zu evaluieren, empfehlen wir, zuerst festzustellen, ob die Lösung umfassende Kontrollen bietet, die dem Security-Team die Risiken herkömmlicher Ansätze zum Erstellen, Verwalten und Verwenden sensibler Administratoranmeldeinformationen überwinden helfen. Besonderes Augenmerk sollte auf folgende Bereiche gelegt werden: Erkennung, Vaulting, Richtlinienerzwingung, Abruf und die Möglichkeit der Unterstützung eines nahtlosen Übergangs zu einer mit allen Funktionen ausgestatteten Privileged Access Management-Implementierung.

Abschnitt 3:

Die zwölf wichtigsten Funktionen beim Privileged Access Management

1. Automatisierte/unterstützte Erkennung

Ohne eine Möglichkeit der automatischen oder unterstützten Erkennung kann sich das Management privilegierter Passwörter als äußerst beschwerlich erweisen – ganz zu schweigen von eventuellen Fehlern oder sonstigen Versäumnissen, die die Rechenumgebung eines Unternehmens anfällig für die ausgefeilten Angriffe von heute machen. Deshalb bietet CA Privileged Access Manager eine Reihe von Methoden für die Erkennung von Geräten, Systemen, Anwendungen, Services und Accounts. Dazu nutzt die Lösung bekannte Portverknüpfungen, Verzeichnisinformationen, Managementkonsolen und APIs. So verwendet CA Privileged Access Manager beispielsweise verfügbare APIs für unterstützte Virtualisierungs- und Cloud-Management-Lösungen, um Administratoren zu benachrichtigen, sobald neue virtuelle Maschinen erstellt werden. Darüber hinaus vereinfacht die Lösung den Massenimport von Systemlisten aus Textdateien sowie die Ad-hoc-Erfassung über die Managementkonsole. Wichtig ist auch zu wissen, dass wir absichtlich keine disruptiveren (und ggf. auch risikoreicheren) Erkennungstechniken verwendet haben, die zielbasierte Agenten erfordern, welche den lokalen TCP-Stack mit Hook oder Shim verändern.

2. Sicheres Speichern/Vaulting

Ein verschlüsselter Vault bietet einen zentralen Kontrollpunkt und ersetzt jegliche unsicheren Speichermethoden (wie Kalkulationstabellen), die eine Offenlegung und Kompromittierung von Anmeldeinformationen einfacher machen. Der Vault von CA Privileged Access Manager schützt die Anmeldeinformationen und ist mit FIPS 140-2 Level 1 kompatibel. Die Lösung nutzt AES-256-Bit-Verschlüsselung für die sichere Speicherung sämtlicher Arten von Anmeldeinformationen, nicht nur von Passwörtern. Weitere überzeugende Leistungsmerkmale der Lösung:

- Es ist eine Option zur Verwendung integrierter Hardware-Security-Module (HSM), z. B. von SafeNet und Thales, zur Unterstützung einer FIPS 140-2 Level 2- oder Level 3-Implementierung enthalten. Dies ist vor allem wichtig für anspruchsvolle, risikoaverse Clients und Anwendungsszenarien, beispielsweise bei Finanz- und Bankensystemen, für die es wünschenswert ist, dass die zur Verschlüsselung der Anmeldeinformationen verwendeten Schlüssel von den verschlüsselten Anmeldeinformationen getrennt gespeichert werden. Es werden mehrere Bereitstellungsoptionen unterstützt, z. B. CA Privileged Access Manager-Hardwaregeräte mit integrierten PCI-Karten, virtuelle CA Privileged Access Manager-Geräte, die mit dem Netzwerk verbundene HSM-Geräte aufrufen, sowie CA Privileged Access Manager-Geräte, die einen „HSM-as-a-Service“ von AWS aufrufen.
- Bewährte kryptografische Whitebox-Routinen schützen die Verschlüsselungsschlüssel während ihrer Verwendung im System (d. h. im Arbeitsspeicher). Mit diesem Ansatz sollen Hacker daran gehindert werden, Schlüssel abzufangen und zusammenzufügen. Dazu werden kryptografische Standard-APIs und der Arbeitsspeicher überwacht. So soll die Abkehr von schlechteren alternativen Lösungen basierend auf Schlüsselblockerstellung oder einfacher Maskierung realisiert werden. Diese Technologie ist besonders wichtig für die A2A-Szenarien, bei denen das zugreifende System ebenfalls Anmeldeinformationen im Vault speichern muss und ein größeres Risiko für eine Kompromittierung des Systems besteht (z. B. wenn es sich an einem recht exponierten Ort befindet).

3. Automatisierte Richtlinienerzwingung

CA Privileged Access Manager automatisiert die Erstellung, Verwendung und Änderung von Passwörtern. Dadurch ist man weniger geneigt, Passwörter wiederzuverwenden oder sich auf schwache (und leicht zu merkende) Passwörter zu verlassen. Mit CA Privileged Access Manager können flexible Richtlinien so eingerichtet werden, dass komplexe Passwörter erzwungen und Änderungsanforderungen implementiert werden – etwa zeitbasierte rotierende Passwörter (z. B. täglich oder wöchentlich) oder als Reaktion auf ein bestimmtes Ereignis (z. B. nach jeder Verwendung) – und die Verwendung gesteuert wird (z. B. Zugriff nur innerhalb bestimmter Zeitfenster erlauben oder bei Anforderung von zwei/mehreren Autorisierungen für den Passwortzugriff). Da diese Richtlinien hierarchisch und auf Gruppierungen von Zielressourcen angewandt werden können, ist es nicht nur möglich, unterschiedliche Anforderungen und Fähigkeiten für verschiedene Ziele zu konfigurieren, sondern auch die Erzwingung zu dynamisieren: Wenn beispielsweise eine Ressource zur Gruppe hinzugefügt wird, übernimmt sie automatisch die Richtlinien für diese Gruppe. Im Hintergrund interagiert CA Privileged Access Manager direkt mit den betroffenen Zielressourcen, um dafür zu sorgen, dass alle Anmeldeinformationen synchron bleiben (das heißt, wenn sie an einer Stelle geändert werden, werden diese Änderungen auch an anderer Stelle übernommen).

4. Sicheres Abrufen und Präsentieren/Verwenden

Es macht keinen Sinn, privilegierte Anmeldeinformationen in einem Vault zu speichern, wenn sie nicht ebenso sicher abgerufen und verwendet werden können. Der erste Schritt in diesem Prozess besteht in der korrekten Authentifizierung jeglicher Personen (bzw. jeglicher Objekte im Falle von Anwendungen und Scripts), die sich Zugriff verschaffen möchten bzw. eine Anmeldeinformation verwenden. Hier setzt CA Privileged Access Manager voll und ganz auf Ihrer vorhandenen Identitätsinfrastruktur auf und bietet eine Integration in Active Directory und LDAP-kompatible Verzeichnisse sowie in Authentifizierungssysteme wie RADIUS. Darüber hinaus ist noch folgende Unterstützung enthalten:

- Zwei-Faktor-Tokens (z. B. via CA Advanced Authentication oder andere wie etwa von RSA und SafeNet)
- X.509/PKI-Zertifikate
- Personal Identity Verification and Common Access Cards (PIV/CAC), erforderlich für die US-amerikanischen Sicherheitsrichtlinien HSPD-12 und OMB-11-11
- SAML
- Zusammengesetzte Mehrfaktor-Techniken (z. B. die Kombination von Passwörtern mit RSA-Tokens)

Im bevorzugten Betriebsmodus präsentiert CA Privileged Access Manager dann die angeforderten Anmeldeinformationen dem Zielsystem im Namen der zugreifenden Entität (Anwender oder Anwendung). Dieser Ansatz beschert noch einige weitere Vorteile in puncto Security. Anders als bei einfachen Ein-/Auschecklösungen werden die Anmeldeinformationen von der zugreifenden Entität niemals gesehen oder an sie verteilt. Dies reduziert die möglichen Risiken. Da die Authentifizierung zum Zielsystem vollständig automatisiert ist und sich die Anwender ihre Passwörter niemals merken müssen, können Richtlinien implementiert werden, um die Passwortkomplexität drastisch zu erhöhen. Der gesamte Zugriff auf die Zielressourcen erfolgt über CA Privileged Access Manager, folglich kann die Lösung die Aktivitäten privilegierter Anwender lückenlos zuordnen, auch bei gemeinsam genutzten Administratoraccounts.

Der Vollständigkeit halber sollte auch darauf hingewiesen werden, dass die gesamte Netzwerkkommunikation zwischen den zugreifenden Entitäten, CA Privileged Access Manager und den verwalteten Zielen via SSL verschlüsselt ist. CA Privileged Access Manager unterstützt noch einen weiteren Betriebsmodus, bei dem die zugreifenden Entitäten die benötigten Anmeldeinformationen für die Zielsysteme selbst abrufen und übermitteln können.

5. Nahtloser Übergang zu einem vollständigen Privileged Access Management

CA Privileged Access Manager bietet Unternehmen, die sich zuvor allein auf das Passwortmanagement verließen, all das, was sie brauchen, um auf ein mit vollem Funktionsumfang ausgestatteten Access Management privilegierter Accounts

umzustellen, ob und wann immer sie dies wünschen. Dies sind einige der wichtigsten Fähigkeiten, von denen die IT-Security-Abteilung immens profitieren wird:

- Differenzierte rollenbasierte Access Control mit zugehörigen Workflows (z. B. für die Anforderung/Autorisierung zusätzlicher Berechtigungen)
- Automatische Herstellung von Verbindungen/Sessions mit den Zielressourcen (inklusive Unterstützung für RDP, SSH, Web und zahlreiche weitere Zugriffsmodi/-optionen)
- Echtzeitüberwachung der Sessions privilegierter Anwender, einschließlich der richtlinienbasierten Erzwingung erlaubter/verweigerter Aktivitäten (z. B. welche Befehle ein bestimmter Anwender ausführen kann)
- Protokollierung, einschließlich systemprotokollbasierter SIEM-Integration
- Vollständige Session-Aufzeichnung mit DVR-ähnlicher Wiedergabe, um direkt zu relevanten Ereignissen zu springen
- Verhindert, dass Anwender ihre Berechtigungen umgehen, indem sie zugängliche Ziele nutzen, um sich Zugang zu anderen, nicht autorisierten Zielen zu verschaffen

Die Implementierung dieser zusätzlichen Funktionen ist mehr als einfach. CA Privileged Access Manager stellt das gesamte Passwortmanagement privilegierter Accounts sowie die Access Control-Funktionalität in einer nahtlos integrierten Lösung bereit. Darüber hinaus ermöglicht CA Privileged Access Manager ein einheitliches Richtlinienmanagement für die gesamte Lösung, was die Implementierung und Verwaltung weiter vereinfacht.

Umfassende Abdeckung

Der zweite wichtige Bereich, den es bei der Auswahl einer Lösung für das Management privilegierter Passwörter zu untersuchen gilt, ist der Leistungsumfang. Man sollte also prüfen, welche Arten zugreifender Entitäten, Anmeldeinformationen und Zielsysteme unter Berücksichtigung der oben genannten Kontrollmechanismen von der Lösung wirklich unterstützt werden.

6. Umfassende Unterstützung herkömmlicher Ziele

CA Privileged Access Manager umfasst eine Vielzahl verschiedener Konnektoren für die Zielsysteme. So besteht eine sofort einsatzfähige Integration für alle Arten von IT-Infrastrukturen, Netzwerkgeräten, Systemen und Anwendungen. Darunter z. B.:

- Windows®-Domäne, lokaler Administrator und Service-Accounts
- Gängige Linux®- und UNIX®-Distributionen
- AS/400
- Cisco- und Juniper-Netzwerkgeräte
- Telnet/SSH-basierte Systeme
- SAP
- Remedy
- ODBC/JDBC-Datenbanken
- System- und Anwendungsserver

Als erweiterbare Lösung bietet CA Privileged Access Manager auch flexible Anpassungsoptionen an, sodass es für die Unternehmen vereinfacht wird, die Unterstützung auf eigene und intern entwickelte Systeme auszuweiten.

7. Unterstützung für Virtualisierungs- und Cloud-Management-Konsolen

Die sofort einsatzfähigen Funktionen von CA Privileged Access Manager für das Management und den Schutz von Anmeldeinformationen beschränken sich nicht nur auf herkömmliche Zielressourcen. Sie erstrecken sich auch auf gängige Virtualisierungslösungen und Cloud Solutions, z. B. VMware vSphere, VMware NSX, Amazon Web Services und Microsoft® Online Services. Die für diese Lösungen verfügbaren Funktionen sind im Übrigen nicht auf einzelne Instanzen zugehöriger virtueller Maschinen, Anwendungen oder Services beschränkt. Zum Leistungsumfang gehören auch die entsprechenden Managementkonsolen, die aufgrund der wichtigen Befehle, die über sie ausgeführt werden, ebenso als privilegierte Ressourcen anzusehen sind.

8. Unterstützung für die Authentifizierung zwischen Maschinen

Wie bereits erwähnt, werden privilegierte Anmeldeinformationen nicht nur von Menschen genutzt. In den meisten Unternehmen sind auch zahlreiche Anwendungen und Systeme in der Lage, auf sensible Ressourcen zuzugreifen, z. B. andere Anwendungen oder Datenbanken. Zu diesem Zweck werden die Anmeldeinformationen für gewöhnlich in den Code der zugreifenden Anwendung eingebettet, oder sie werden zur Laufzeit über eine Konfigurationsdatei verfügbar gemacht. Keines dieser Vorgehen ist jedoch besonders praktisch oder sicher. CA Privileged Access Manager unterstützt diese beiden A2A-Anwendungsfälle, indem Entwickler in die Lage versetzt werden, einen kompakten CA Privileged Access Manager-Client in die Anwendungen zu integrieren. So steht den „privilegierten Anwendungen“ alles zur Verfügung, was sie brauchen, um sich bei CA Privileged Access Manager zu registrieren, die erforderlichen Passwörter dynamisch abzurufen und sie dann im Arbeitsspeicher im lokalen System zu schützen. Darüber hinaus gibt es mehrere Mechanismen für die Authentifizierung der privilegierten Anwendungen und für die Überprüfung ihrer Identität, bevor die angeforderten Anmeldeinformationen von CA Privileged Access Manager freigegeben werden.

Wenn Unternehmen CA Privileged Access Manager in A2A-Szenarien einsetzen, können sie anfällige/unsichere A2A-Anmeldeinformationen durch deren zentrale Speicherung in einem Vault effektiver entfernen, das Management der A2A-Anmeldeinformationen und die Erzwingung der zugehörigen Richtlinien automatisieren und die entsprechenden Auditing- und Compliance-Aktivitäten vereinfachen.

9. Unterstützung für das Schlüsselmanagement

Neben der Unterstützung kryptografischer Operationen dienen viele Arten von Schlüssel auch als Token zur Bestätigung von Identitäten. Diese Schlüssel sind zwar keine Passwörter im eigentlichen Sinne, sie funktionieren aber wie Passwörter und sind auch ähnlichen Bedrohungen und Risiken ausgesetzt, z. B. beim Kopieren, bei der gemeinsamen Nutzung, bei der versehentlichen Offenlegung und im Falle ungeprüfter Schlupflöcher. Da derartige Schlüssel in der Regel in die Lösungen eingebettet sind oder dort auf transparente Weise genutzt werden, um ihre relative Komplexität vor den Anwendern zu verbergen, ist es bei ihnen auch wahrscheinlicher, dass sie verwaisen und/oder im Laufe der Zeit einfach zu viele werden. Deshalb ist es sinnvoll, einige der Kontrollen, die für die Verwaltung und den Schutz von Passwörtern herangezogen werden, auch auf diese anderen Anmeldeinformationen anzuwenden. Hier ein paar empfohlene Best Practices zur Abwehr der damit zusammenhängenden Bedrohungen:

- Verschieben der autorisierten Schlüssel zu geschützten Speicherorten
- Regelmäßiges Rotieren aller Schlüssel (um bei Offenlegung eine rechtzeitige Beendigung des Zugriffs zu gewährleisten)
- Erzwingen von Quellbeschränkungen für autorisierte Schlüssel[3]
- Erzwingen von Befehlsbeschränkungen für autorisierte Schlüssel

Um dem Rechnung zu tragen, verfügt CA Privileged Access Manager über entsprechende Kontrollmechanismen und Funktionen für andere Arten von Anmeldeinformationen, z. B. SSH-Schlüssel und die PEM-codierten Schlüssel, die verwendet werden, um auf AWS-Ressourcen und Verwaltungskonsolen zuzugreifen. Anders ausgedrückt: Mit CA Privileged Access Manager können solche Anmeldeinformationen: (1) in einem Vault gespeichert, (2) von konfigurierten Richtlinien rotiert und kontrolliert und (3) auf eine Weise abgerufen und verwendet werden, die die Wahrscheinlichkeit, dass sie gestohlen oder offengelegt werden, minimiert.

Cloud-basierte Bereitstellung

Im Zeitalter der hybriden Cloud ist ein weiterer erfolgsentscheidender Faktor für den Erfolg einer Lösung zum Management privilegierter Passwörter, wie gut sie sich nicht nur physisch „einpasst", sondern auch inwieweit sie an den Networking-Anforderungen und -Fähigkeiten der Cloud ausgerichtet ist.

10. Bereitstellungsoptionen: On-Premise, auf Basis virtueller Maschinen und Cloud-basiert

CA Privileged Access Manager unterstützt drei komfortable Bereitstellungsoptionen, die den Unternehmen dabei helfen, mit komplexen hybriden Cloud-Architekturen Schritt zu halten:

- Ein geschütztes physisches Gerät – verfügbar in mehreren Modellen für die herkömmliche Rackmontage im Unternehmensrechenzentrum
- Eine Amazon Machine Instance (AMI) – vorkonfiguriert für die Bereitstellung mit der Amazon EC2-Infrastruktur
- Ein virtuelles OVF-kompatibles Gerät – sofort einsatzfähig und vorkonfiguriert für die Bereitstellung in VMware-Umgebungen

Unabhängig von der verwendeten Bereitstellungsoption erhält ein Unternehmen auf jeden Fall eine Lösung, mit der es seine gesamte hybride Cloud-Infrastruktur verwalten kann.

11. An der Cloud ausgerichtete Architektur und Vorgehensweise

Die zahlreichen in die Architektur von CA Privileged Access Manager integrierten Funktionen sorgen dafür, dass sich die Lösung hervorragend in hybride Cloud-Umgebungen einfügt. Dazu drei Beispiele:

- Automatische Erkennung und Schutz: In hybride Cloud-Umgebungen können die Systemoperatoren eine beliebige Anzahl Systeme mit einem einzigen Befehl erstellen (oder stilllegen). CA Privileged Access Manager trägt diesem Fall Rechnung, indem die Lösung gültige APIs für die automatische Erkennung virtualisierter Ressourcen und Cloud-Ressourcen einsetzt und dann entsprechende Richtlinien für die Anmeldeinformationen und das Access Management provisioniert (bzw. deprovisioniert).
- Vermeidung von Identitätsinseln (d. h. Identity Federation): Eine Möglichkeit, wie CA Privileged Access Manager isolierte Identitätsinseln vermeidet, ist, die Identitätsinfrastruktur zu verwenden, die das Unternehmen bereits im Einsatz hat. Eine andere Möglichkeit, speziell für AWS-Implementierungen, besteht in der Unterstützung kurzlebiger Anwender. Dies ist ein Ansatz, bei dem die Unternehmen keine separaten Identitätsinformationen im Subsystem AWS Identity and Access Management pflegen müssen.
- Automatisierung: Eine umfassende API ermöglicht den programmgesteuerten Zugriff auf alle CA Privileged Access Manager-Funktionen (z. B. über externe Verwaltungs- und Orchestrierungssysteme).

12. Cloud-fähige Skalierbarkeit und Zuverlässigkeit

Das Management privilegierter Anmeldeinformationen ist für die IT-Infrastruktur eines Unternehmens ein wirklich kritischer Aspekt. Dies gilt umso mehr, wenn die Implementierung auch A2A-Szenarien unterstützen soll, die vollkommen automatisiert ablaufen. Zu diesem Zweck enthält CA Privileged Access Manager eine systemeigene Funktionalität für Clustering und Lastverteilung, die die Anforderungen an Hochverfügbarkeit und Skalierbarkeit selbst der größten und anspruchsvollsten Umgebungen erfüllt. Im Vergleich zu den herkömmlichen Alternativen besteht bei CA Privileged Access Manager keine Notwendigkeit, in separate, externe Lastverteiler zu investieren. Es gibt keine Leistungsverzögerungen, wie sie bei Aktiv-Passiv-Ansätzen üblich sind, und es ist nicht erforderlich, zusätzliche „optionale" Funktionen zu lizenzieren. Auf Wunsch – und sofern dies im Hinblick auf die Latenz aus betrieblicher Sicht unterstützt wird – können CA Privileged Access Manager-Cluster sogar so konfiguriert werden, dass eine Redundanz über geografisch verteilte Rechenzentren und Cloud-Umgebungen ermöglicht wird.

CA Privileged Access Manager stellt eine Lösung der nächsten Generation für das Management privilegierter Anmeldeinformationen bereit, die die Securityrisiken im gesamten hybriden Unternehmen minimiert und die Unternehmenseffizienz erhöht.

Abschnitt 4:

Fazit: Die Herausforderungen beim Management privilegierter Anmeldeinformationen im Cloud-Zeitalter meistern

Anmeldeinformationen für privilegierte Accounts zu verwalten und zu schützen, ist eine wesentliche Voraussetzung zur Minimierung von Risiken und zur Erfüllung von Compliance-Anforderungen. Dies ist ein Problem, das zudem immer komplexer und bedeutsamer wird, da mit den hybriden Cloud-Umgebungen Verwaltungskonsolen mit beispielloser Leistung eingeführt werden, mit denen es möglich ist, praktisch Hunderte von Zielsystemen mit nur wenigen Mausklicks hinzuzufügen bzw. zu entfernen.

Unternehmen, die diesen so wichtigen Aspekt ihrer Strategie für Informationssicherheit angehen möchten, müssen die infrage kommenden Lösungen im Hinblick auf die Kontrolltiefe, den Leistungsumfang und den Grad der Cloud-Unterstützung hin untersuchen. Wie in diesem Dokument erörtert, erfüllt CA Privileged Access Manager alle drei dieser Anforderungen und gibt modernen Unternehmen alles an die Hand, was sie brauchen, nämlich eine Lösung der nächsten Generation für das Management privilegierter Anmeldeinformationen, die die IT-Risiken reduziert, die Unternehmenseffizienz erhöht und bereits getätigte Investitionen schützt, da sie herkömmliche und virtualisierte Infrastrukturen wie auch hybride Cloud-Infrastrukturen unterstützt.

Kontaktieren Sie CA Technologies unter ca.com/de.

CA Technologies (NASDAQ: CA) entwickelt Software, die Unternehmen bei der Umstellung auf die Application Economy unterstützt. Software steht in allen Branchen und in allen Unternehmen im Mittelpunkt. Ob Planung, Entwicklung, Management oder Security – CA Technologies arbeitet weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen abwickeln und kommunizieren, in mobilen, privaten und öffentlichen Cloud-Umgebungen oder in verteilten Systemen und Mainframe-Umgebungen neu zu gestalten. Weitere Informationen finden Sie unter ca.com/de.

1 2015 Verizon Data Breach Investigations Report

2 *„New Platforms, New Requirements. Privileged Identity Management for the Hybrid Cloud“*, White Paper von CA Technologies, März 2013

3 *„Managing SSH Keys for Automated Access – Current Recommended Practice“*, IETF-Entwurf, April 2013

CS200-169152_1215