**WHITE PAPER** | DEZEMBER 2015

# Gewährleistung der PCI-Compliance

## durch Privileged Access Management

# Kurzfassung

## Ausgangssituation

Unternehmen, die Transaktionen mit Kredit-/Debitkarten tätigen, haben es zunehmend schwerer, die Vorgaben zur Einhaltung von Vorschriften umzusetzen. Insbesondere müssen sie die Vorgaben des Payment Card Industry Data Security Standard (PCI DSS) in der Version 3 umsetzen, der im Januar 2015 in Kraft trat.[1] Der PCI DSS v3 stellt verschiedene Anforderungen an die Absicherung relevanter Systeme und Netzwerke in Unternehmen und schließt auch die Karteninhaberdatenumgebung (Cardholder Data Environment, CDE) mit ein. Durch die Anforderungen an eine strenge Authentifizierung und Access Control für die CDE stehen Unternehmen vor der schwierigen Aufgabe der Implementierung einer mehrstufigen Authentifizierung, von Access Control und von Reporting-Tools für Aktivitäten oder Praktiken, insbesondere für privilegierte oder administrative Zugriffe auf diese Systeme.

## Chance

Die im PCI DSS beschriebenen Anforderungen an das Privileged Access Management zeigen die Risiken eines Missbrauchs von privilegierten Accounts und dem daraus ermöglichten Zugriff auf kritische Unternehmensassets auf. Praktisch alle Security-Vorfälle der letzten Zeit lassen sich auf privilegierte Anwender oder Anmeldeinformationen als Haupteinfallstor für erfolgreich ausgeführte Angriffe zurückführen. Ein effektiver Ansatz für ein Privileged Access Management versetzt Unternehmen in die Lage, jede ausgeführte Aktivität zu überwachen, zu protokollieren und einzuschränken, die über einen privilegierten Account ausgeführt wird, z. B. über den eines Netzwerk-, System- oder Datenbankadministrators. Dadurch erhalten Unternehmen eine bessere Transparenz und Kontrolle über die Aktivitäten ihrer privilegierten Anwender mit ihren besonderen Zugriffsrechten auf die wichtigsten Unternehmensassets. Ohne so einen Ansatz haben viele Unternehmen nicht nur Probleme, die Anforderungen des PCI DSS v3 hinsichtlich Identifizierung, Authentifizierung und Access Control zu erfüllen, sondern sie können auch nicht das Risiko von Sicherheitsverstößen und Angriffen verringern.

## Nutzen

Ein mehrstufiger Ansatz für das Privileged Access Management, wie ihn die einfach bereitzustellende Lösung CA Privileged Access Manager verfolgt, kann Unternehmen dabei helfen, die Anforderungen des PCI DSS v3 zu erfüllen. So können sie nur ihre CDEs, sondern ihre gesamte unternehmensweite hybride IT, einschließlich ihrer Netzwerk-, Server-, virtuellen und Cloud-Umgebungen, besser schützen. Auf diese Weise verbessern Unternehmen ihre Security zum Schutz vor Sicherheitsverstößen und minimieren das Risiko, die Vorschriften des PCI DSS nicht zu befolgen oder gar zu verletzen.

**Abschnitt 1:**

# Die Notwendigkeit eines Privileged Access Management

Nie zuvor war ein Privileged Access Management so notwendig wie heute. Eine Studie nach der anderen zeigt das systematische Versagen der traditionellen Security-Strategien auf. Einige behaupten sogar, dass praktisch jedes Unternehmen zu jedem beliebigen Zeitpunkt mindestens einer aktiven Kompromittierung ausgesetzt ist.[2] Die Medien berichten regelmäßig über Datenschutzverletzungen im großen Stil, wie z. B. Ende 2013 bei Target, 2014 bei Home Depot und 2015 beim Office of Personnel Management, bei denen von Drittanbietern gestohlene Anmeldeinformationen verwendet wurden. Der „2014 Data Breach Investigations Report" von Verizon bezeichnet gestohlene Anmeldeinformationen als die größte Bedrohung für Unternehmen.[3]

Häufig sind sich Unternehmen nicht der Risiken bewusst, die durch ihre privilegierten Accounts und deren hohe Anzahl entstehen können. Privilegierte Accounts werden nicht nur an die Mitarbeiter eines Unternehmens vergeben, sondern auch an Drittanbieter wie etwa Zulieferer, Auftragnehmer und andere, die technischen Support für Systeme, Netzwerkgeräte und Anwendungen leisten. Ein einzelnes Unternehmen kann über Tausende, wenn nicht sogar über Zehntausende von privilegierten Accounts verfügen, von denen jeder für sich ein Sicherheitsrisiko für das Unternehmen darstellt.

Die Idee hinter einem Privileged Access Management besteht darin, eine größere Zurechenbarkeit und Transparenz für die Handlungen von Administratoren zu erreichen. Beim traditionellen Modell wurde ganz einfach allen Administratoren blind vertraut, aber diese naive Einstellung übersieht zwei wichtige Probleme: die Möglichkeit, dass ein verärgerter Administrator zu einer Insider-Bedrohung wird, und die Auswirkungen, wenn ein administrativer Account durch einen externen Angreifer kompromittiert wird (insbesondere dann, wenn dieser Administrator ein Zulieferer oder Drittanbieter ist).

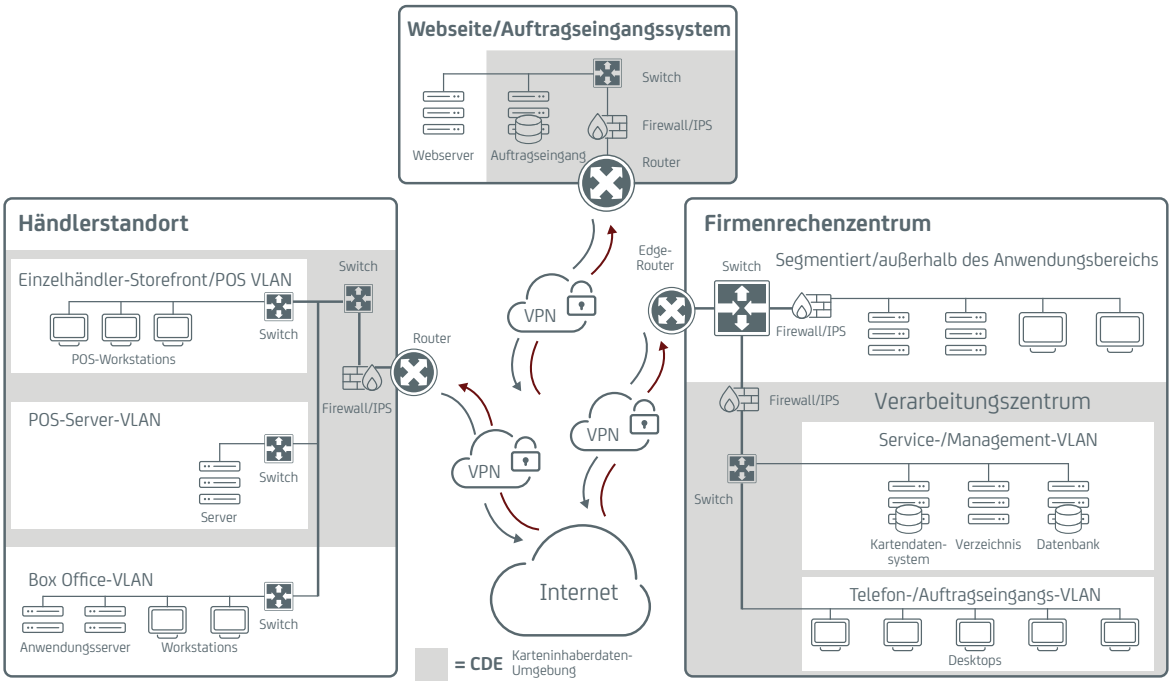
Eine Lösung kann es sein, ein „Zero Trust"-Modell einzuführen. Diesen Ansatz verfolgt CA Privileged Access Manager (früher Xceedium Xsuite) – eine wichtige Komponente der Lösungen für das Privileged Access Management von CA Technologies. Hierbei wird davon ausgegangen, dass auch Administratoren nicht vollständig vertraut werden kann. Mit diesem Modell wird die Anzahl der Sicherheitsverstöße sowie der Schweregrad der Verstöße, die immer noch auftreten werden, reduziert. Bis zu einem gewissen Grad spiegeln die Anforderungen im PCI DSS dieses „Zero Trust"-Modell wider, so z. B. in Anforderung 7.1.2: „Beschränken Sie Zugriffsrechte für privilegierte Benutzer-IDs auf die geringstmöglichen Privilegien, mit denen Arbeitsaufträge noch ausgeführt werden können."

Obgleich die Einhaltung von PCI-Vorschriften eine solide Grundlage für den Schutz von CDEs darstellt, sind das simple „Überprüfen der Verpackung" und lediglich die Erfüllung der minimalen Anforderungen keine ausreichenden Abwehrmaßnahmen gegen heutige Bedrohungen. Ein gutes Privileged Access Management geht noch weiter als die PCI-Anforderungen, um einen besseren Schutz für die CDE eines Unternehmens zu gewährleisten.

Neben der Einhaltung der PCI-Vorschriften gibt es noch weitere Gründe, warum ein Privileged Access Management eingeführt werden sollte: Durchbrechen der Angriffsabläufe (Kill Chain), Minimieren der Risiken durch Insider, Protokollieren und Überwachen von Befehlen und Entfernen fest codierter Passwörter.

**Abb. A: Umfang der Anforderungen des PCI DSS**

PCI DSS v3 erfordert Maßnahmen zum Schutz der Cardholder Data Environment (CDE)




## Durchbrechen der Kill Chain

Das grundlegende Konzept einer Kill Chain besteht darin, dass ein Angreifer einem wiederkehrenden Muster folgt, um Zugriff auf ein System zu erlangen (oder diesen Zugriff auszuweiten), und dann versucht, seine Berechtigungen zu erweitern. Mit diesen Berechtigungen versucht der Angreifer, Zugriff auf ein anderes System zu erlangen oder den bestehenden Zugriff auszuweiten, um anschließend erneut seine Berechtigungen zu erweitern. Diese Angriffsabläufe werden so lange fortgesetzt, bis er sein eigentliches Ziel erreicht hat. Kann diese „Kill Chain" an irgendeiner Stelle durchbrochen werden, wird der Angriff gestoppt, bevor er sein eigentliches Ziel erreicht hat.

CA Privileged Access Manager stellt geeignete Funktionen bereit, mit denen Sie diese Kill Chain durchbrechen können. So unterstützt CA Privileged Access Manager beispielsweise die mehrstufige Authentifizierung für privilegierte Accounts, was eine Kompromittierung deutlich erschwert, weil ein Angreifer für einen einzelnen Account unterschiedliche Anmeldeinformationen kompromittieren muss. Außerdem reduziert die Vergabe der geringstmöglichen Zugriffsrechte, mit denen privilegierte Accounts Befehle für jede CDE-Komponente ausführen können, den Zugriff auf vertrauliche Informationen und erschwert es Angreifern, unberechtigten Zugriff auf wichtige Daten zu erhalten.

Ein weiterer Faktor, wie CA Privileged Access Manager dabei hilft, die Kill Chain zu durchbrechen, ist die Unterstützung für Netzwerksegmentierung. Dies grenzt ein, auf welche Subnets ein bestimmter privilegierter Account zugreifen kann und welche Systeme in einem Subnet er verwalten kann. Die Netzwerksegmentierung kann helfen zu verhindern, dass sich ein Angreifer von einem System zum anderen weiter vorarbeitet, und seine Sichtweite auf das Netzwerk eines Unternehmens einschränken. Auf ähnliche Weise nutzt CA Privileged Access Manager einen Socket Filter Agent (SFA), der verhindert, dass ein Administrator eine nicht autorisierte Netzwerkverbindung zu einem anderen System herstellt, indem er z. B. versucht, einen SSH- oder TELNET-Befehl an einen Host auszugeben, der nicht durch die Richtlinien von CA Privileged Access Manager autorisiert ist.

All diese Funktionen von CA Privileged Access Manager werden von Stellen wie Mandiant zum Schutz gegen Kreditkartenbetrug empfohlen.[4]

### Minimieren der Risiken durch Insider

Die PCI-Anforderungen richten sich zwar vornehmlich gegen externe Angreifer, aber sie berücksichtigen auch die Bedrohung durch Insider, die für heutige Unternehmen ein dringendes Problem darstellt. Einer Studie zufolge sollen mehr als 10 Prozent aller Mitarbeiter schon einmal aus Profitgier Mitarbeiterinformationen gestohlen haben oder jemanden kennen, der das getan hat.[5]

CA Privileged Access Manager kann auf mehrere Weisen dabei helfen, die Risiken durch Insider zu minimieren. Zunächst kann die Umsetzung des Prinzips der geringstmöglichen Zugriffsrechte deutlich einschränken, welche Befehle ein Insider eingeben kann und an welche CDE-Komponenten er solche Befehle senden kann. Das allein begrenzt schon den Schaden, den ein Insider verursachen kann. Außerdem bietet die Überwachung und die Protokollierung aller Aktivitäten von privilegierten Accounts eine detaillierte Aufzeichnung sämtlicher eingegebenen Befehle, die sich nicht nur zu einer allgemeinen (gemeinsam genutzten) ID, sondern bis zu einer einzelnen Person zurückverfolgen lassen.

### Überwachung und Protokollierung von Befehlen

Ganz gleich, wie leistungsstark eine Security ist – es verbleiben immer Schwachpunkte. Deswegen sind Sicherheitsverstöße in allen Umgebungen unvermeidbar. Da CA Privileged Access Manager sämtliche Aktivitäten von privilegierten Accounts überwacht und protokolliert, werden die forensischen Verfahren deutlich vereinfacht, mit denen bestimmt werden kann, wie ein erfolgreicher Angreifer nicht autorisierte administrative Anmeldeinformationen verwendet hat.

### Entfernen fest codierter Passwörter

Viele Softwareentwickler, Administratoren und andere haben lange Zeit die Methode angewandt, Passwörter in Scripts, Quellcodes oder sonstwo fest zu codieren. Dieses Vorgehen lässt eine kritische Schwachstelle entstehen, weil Softwareentwickler, Tester und andere auf diese Passwörter zugreifen können und weil auch Angreifer wissen, wo sie danach suchen müssen, wenn sie ein System infiltrieren möchten. Damit erhalten Angreifer dann die Möglichkeit, auf andere Systeme zuzugreifen, wie etwa Datenbanken mit Kreditkarteninformationen. CA Privileged Access Manager stellt Funktionen für eine Authentifizierung „Anwendung-zu-Anwendung“ bereit, die fest codierte Passwörter überflüssig machen.

---

**Abschnitt 2:**

## Unterstützung der Einhaltung von PCI-Vorschriften durch Privileged Access Management

Wie zuvor beschrieben, spielt das Privileged Access Management eine wichtige Rolle bei der Einhaltung von PCI-Vorschriften. In typischen Unternehmensumgebungen können viele PCI-Anforderungen ohne eine Lösung für das Privileged Access Management ganz einfach nicht erfüllt werden. So musste z. B. ein großer Einzelhändler eine Geldbuße von monatlich 100.000 USD bezahlen, weil er die PCI-Anforderungen für Identifizierung, Authentifizierung und Access Control nicht erfüllt hatte. Durch Aufnahme von CA Privileged Access Manager in sein Portfolio von Security-Lösungen konnte er schließlich alle Anforderungen erfüllen und weitere Geldbußen vermeiden.

CA Privileged Access Manager unterstützt jede der folgenden PCI-Anforderungen.[6]

### Anforderung 2: Verwenden Sie keine der vom Anbieter festgelegten Standardeinstellungen für Systempasswörter und andere Sicherheitsparameter.

CA Privileged Access Manager unterstützt diese Anforderung auf zweierlei Weise. Erstens können während der Systembereitstellung Kontrolle über die Einstellungen der privilegierten Accounts übernommen und ihre Standardpasswörter zurückgesetzt werden. Zweitens kann eingeschränkt werden, welche Protokolle (z. B. SSH oder SSL/TLS) für den administrativen Fernzugriff verwendet werden dürfen. So wird verhindert, dass mit unsicheren Protokollen eine Systemadministration über Netzwerke ausgeführt werden kann.

## Anforderung 6: Gewährleisten Sie die Entwicklung und Maintainance sicherer Systeme und Anwendungen.

Ein wesentlicher Teil dieser Anforderung besteht aus der ordnungsgemäßen Handhabung von Anmeldeinformationen und der Aufgabentrennung in Entwicklungs-, Testing- und Produktionsumgebungen. CA Privileged Access Manager erzwingt in allen diesen Umgebungen eine rollenbasierte Access Control für privilegierte Accounts und unterstützt eine Aufgabentrennung. Dies erleichtert das Entfernen von Accounts aus Entwicklung, Testing und anderen Bereichen, die für die Bereitstellung eines Systems oder einer Anwendung nicht mehr erforderlich sind.

## Anforderung 7: Beschränken Sie den Zugriff auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf.

CA Privileged Access Manager ermöglicht es Unternehmen, das häufig unbeachtete Prinzip der geringstmöglichen Zugriffsrechte umzusetzen. Insbesondere das „Zero Trust"-Modell von CA Privileged Access Manager erzwingt eine spezifische Access Control für einzelne privilegierte Anwender oder Gruppen solcher Anwender (z. B. Datenbankadministratoren). Dadurch kann eingeschränkt werden, auf welche Systemkomponenten – also Server, Netzwerkgeräte und Anwendungen – einzelne privilegierte Anwender oder Anwendergruppen zugreifen können und welche Befehle sie auf jeder dieser Komponenten ausführen dürfen. Außerdem lässt sich CA Privileged Access Manager in Active Directory, LDAP und andere Unternehmensverzeichnisse integrieren, um eine Wiederverwendung ihrer Rollen und Gruppendefinitionen zu gewährleisten.

## Anforderung 8: Identifizieren und authentifizieren Sie Zugriffe auf Systemkomponenten.

Nahezu alle Bereiche der Anforderung 8 werden von CA Privileged Access Manager explizit unterstützt. CA Privileged Access Manager weist allen privilegierten Anwendern eine eindeutige ID zu, stellt alle Standardfunktionen für das Passwortmanagement bereit und unterstützt eine Vielzahl ein- und mehrstufiger Authentifizierungstechnologien. Im Einzelnen unterstützt CA Privileged Access Manager Anforderung 8 wie folgt:

- **8.1:** CA Privileged Access Management ermöglicht die eindeutige Identifikation jedes privilegierten Anwenders auch dann, wenn Unternehmen „gemeinsam genutzte Accounts" für bestimmte Infrastrukturkomponenten, wie etwa Router, verwenden. Unter privilegierten Anwendern wird eine Aufgabentrennung erzwungen. Durch Standardfunktionen können Zugriffsrechte unmittelbar entzogen, inaktive privilegierte Accounts deaktiviert sowie Richtlinien für die Sperrung nach fehlgeschlagenen Authentifizierungsversuchen und die erneute Authentifizierung nach Session-Timeouts erzwungen werden.
- **8.2:** Die Lösung kann in viele Authentifizierungsmethoden integriert werden, die eine Authentifizierung aller privilegierten Anwender erfordert. Sie speichert Passwörter und andere Anmeldeinformationen (wie etwa private kryptografische Schlüssel) in einem stark verschlüsselten Kennwortspeicher und überträgt diese ausschließlich über verschlüsselte Kanäle. Dabei werden Richtlinien für Länge, Qualität, Alterung und Wiederverwendbarkeit von Passwörtern erzwungen.
- **8.3:** Es werden zahlreiche mehrstufige Authentifizierungsmethoden sowie RADIUS, X.509-Zertifikate und Smartcards unterstützt.
- **8.5, 8.6:** Unternehmen können „gemeinsam genutzte Accounts" im Hintergrund nutzen und gleichzeitig die eindeutige Identifizierung und Authentifizierung jedes privilegierten Anwenders, einschließlich aller Drittanbieter, erreichen. Diese eindeutige Identifizierung unterstützt die Verwendung von Smartcards, digitalen Zertifikaten, kryptografischen Tokens und anderen nicht passwortbasierten Formen von Anmeldeinformationen.
- **8.7:** Der direkte Zugriff auf Datenbanken mit Kreditkarteninformationen wird auf autorisierte Datenbankadministratoren beschränkt. Diese „Anwendung-zu-Anwendung"-Unterstützung stellt sicher, dass Personen keinen Zugriff auf Anmeldeinformationen für Anwendungen erhalten oder diese wiederverwenden können.

## Anforderung 10: Verfolgen und überwachen Sie sämtliche Zugriffe auf Netzwerkressourcen und Karteninhaberdaten.

Wie schon bei Anforderung 8 unterstützt CA Privileged Access Manager auch nahezu alle Bereiche der Anforderung 10. CA Privileged Access Manager protokolliert und zeichnet alle Aktivitäten jedes privilegierten Accounts auf. Dies umfasst sowohl Auditaufzeichnungen im Systemprotokollformat als auch einem digitalen Videorekorder ähnelnde Aufzeichnungen

von Administrator-Sessions, die Tags enthalten, um eine zügige Überprüfung auf potentielle Richtlinienverstöße durchzuführen. CA Privileged Access Manager unterstützt Anforderung 10 wie folgt:

- **10.1:** CA Privileged Access Manager ordnet jede Instanz eines privilegierten Zugriffs einer spezifischen Person zu. Für alle privilegierten Zugriffe durch Personen auf Systemkomponenten wird ein Prüfprotokoll erstellt.
- **10.2:** Es werden sowohl eine systemeigene Protokollierung als auch ein Systemprotokoll zur Erzeugung von Prüfprotokollen verwendet, die alle Aktionen sämtlicher privilegierten Anwender aufzeichnen, die auf Servern, Netzwerkgeräten, Datenbanken und anderen Anwendungen ausgeführt werden. Darin sind alle Aktivitäten der identifizierten und authentifizierten privilegierten Accounts aufgezeichnet. Der Zugriff auf die Prüfprotokolle ist beschränkt, sodass nur autorisierte Anwender sie überprüfen können, wobei auch jede dieser Überprüfungen protokolliert wird.
- **10.3:** Es erfolgt eine Aufzeichnung aller durch PCI vorgeschriebenen Felder für jedes protokollierte Ereignis, einschließlich Anwenderidentifizierung, Ereignistyp, Datum und Uhrzeit, Erfolg oder Fehlschlag, Ereignisursprung und Identität der betroffenen Ressource (Hostname etc.).
- **10.4:** Zur Uhrensynchronisierung wird eine Zeitsynchronisationstechnologie (z. B. das Network Time Protocol [NTP]) verwendet.
- **10.5:** Es werden Hashing-Techniken zur Identifizierung jeglicher Manipulationsversuche an Auditprotokollen und Aufzeichnungen eingesetzt. Durch die Weiterleitung von Systemprotokollen an einen zentralen Protokollspeicher werden Backups von Auditaufzeichnungen erstellt.
- **10.7:** Durch die Verwendung von Systemprotokollen und die Unterstützung für ihre Weiterleitung können Auditaufzeichnungen so lange wie erforderlich aufbewahrt werden.

### Anforderung 10: Erlassen Sie eine Richtlinie zur Informationssicherheit für das gesamte Personal.

CA Privileged Access Manager ermöglicht das Erlassen und das Erzwingen von Richtlinien für privilegierte Anwender. Außerdem protokolliert CA Privileged Access Manager sämtliche versuchten Verstöße gegen diese Richtlinien, welche anschließend in die Prozesse für die Risikobewertung mit einfließen.

### CDE-Schutz aus der Perspektive der Serverkontrolle

Das Privileged Access Management von CA Technologies unterstützt auch zusätzliche Anforderungen an eine lokalisierte, sehr spezifische Access Control beim Host, um einen noch besseren Schutz kritischer Ressourcen, wie etwa die CDE, bereitzustellen. CA Privileged Access Manager Server Control bietet eine weitere wichtige Security-Ebene für Serverplattformen, die eine spezifische Access Control, eine richtlinienbasierte Verwaltung und ein sicheres Auditing zum Schutz elektronischer Assets ermöglicht. Der Zugriff auf Serverressourcen, Programme, Dateien und Prozesse kann durch Zugriffsrichtlinien mit einer Vielzahl von Kriterien reguliert werden.

---

**Abschnitt 3:**

## Änderungen beim PCI DSS von v2 zu v3

Bei dem Update des PCI DSS von v2 auf v3 wurden wichtige Schutzmechanismen für CDEs hinzugefügt, wie z. B.:

- Es soll eine Netzwerksegmentierung für die CDE implementiert werden, um eine bessere Trennung von Teilbereichen der CDE zu erreichen. Dadurch soll sichergestellt werden, dass der gesamte Datenverkehr zwischen den Systemkomponenten dokumentiert und ein Auditing sämtlicher Aktivitäten von privilegierten Anwendern durchgeführt wird.
- Es soll ein Testing zur CDE-Perimeterdurchdringung durchgeführt werden.
- Es sollen ein Management für Anmeldeinformationen, eine Access Control nach dem Prinzip der geringstmöglichen Zugriffsrechte und ein Auditing für alle CDE-Zugriffe eingeführt werden.
- Die Security-Kontrollen für Service Provider müssen verschärft werden.[7]

Diese Schutzmechanismen unterstreichen die Notwendigkeit zum Einsatz einer Lösung für das Privileged Access Management wie CA Privileged Access Manager, um die CDE zu schützen und die PCI-Anforderungen zu erfüllen. In vielen Umgebungen stellt das Privileged Access Management die einzige Möglichkeit dar, das Prinzip der geringstmöglichen Zugriffsrechte auf Administratorebene und eine differenzierte Protokollierung von Administratoraktivitäten effektiv implementieren zu können. Zusätzlich dazu kann sich dieser Ansatz für die Implementierung einer Netzwerksegmentierung sowie bei der Überwachung sämtlicher Aktivitäten mit Datenverkehr zwischen einzelnen Netzwerksegmenten als sehr wertvoll erweisen.

Das Update des PCI DSS enthält noch weitere Änderungen in Bezug auf das Privileged Access Management. Insbesondere in der Anforderung 8 kam es hinsichtlich der Identifizierung und Authentifizierung zu großen Neustrukturierungen, sodass diese Anforderung auf den ersten Blick stark verändert erscheint. Die Änderungen beziehen sich jedoch vorwiegend auf die Strukturierung der Anforderung.

Die wichtigste Änderung ist die Aufnahme von Anforderung 8.6: „Bei Verwendung von Authentifizierungsmechanismen ohne Passwort, wie etwa kryptografische Tokens oder Smartcards, darf der Authentifizierungsmechanismus nur für einen Anwender verfügbar sein. Gemeinsam genutzte Authentifizierungsmechanismen sind nicht gestattet.“ Wie im vorangegangenen Abschnitt beschrieben, erfüllt CA Privileged Access Manager diese Anforderung.

---

**Abschnitt 4:**

# Nutzen

Unternehmen, die eine Lösung für das Privileged Access Management implementiert haben, erhalten ein erhöhtes Securitylevel, verringern die Risiken durch externe und interne Angreifer und verbessern die Einhaltung von Vorschriften wie dem PCI DSS.

CA Privileged Access Manager kann Unternehmen durch die folgenden Punkte nicht nur in Bezug auf die Einhaltung des PCI DSS helfen, sondern auch zur Verbesserung ihrer Security insgesamt einen effektiven Beitrag leisten:

- **Kostenreduzierung:** CA Privileged Access Manager kann Ihnen dabei helfen, die Kosten für PCI DSS-Audits deutlich zu senken, insbesondere durch die einfache und sehr kostengünstige Möglichkeit zur logischen Segmentierung von Netzwerken in Unternehmen. Es ist ein Proxy-artiges Gerät, das auf der Anwendungsebene des Netzwerks arbeitet und steuert, welche privilegierten Anwender auf die Systeme zugreifen dürfen. Die logische Segmentierung der Managementebene ermöglicht es Unternehmen, vorhandene physische Netzwerktopologien aufrechtzuerhalten und gleichzeitig Systeme mit Karteninhaberdaten abzutrennen und sie mit einer strengen Access Control zu versehen. Durch diesen Ansatz von CA Privileged Access Manager können Unternehmen Systeme mit Karteninhaberdaten logisch isolieren und dadurch den Umfang von PCI-Audits begrenzen, ohne dass hierbei die hohen Kosten für eine physische Segmentierung von Netzwerken anfallen.
- **Verbesserte Security:** Die tiefgreifende Verteidigungsstrategie („Defense in Depth“) von CA Privileged Access Manager unterstützt Unternehmen bei der Implementierung einer Reihe umfassender Sicherheitskontrollen. Sie reduzieren Risiken durch privilegierte Anwender, bieten einen besseren Schutz gegen externe Gefahren und helfen, Sicherheitsverstöße zu verhindern oder ihre Auswirkungen zu minimieren.
- **Schnellere Time-to-Protection und einfacheres Management:** Durch einfache Bereitstellung und Management über eine einzelne Plattform kann eine beschleunigte und verbesserte Kontrolle privilegierter Zugriffe und der Schutz von Anmeldeinformationen für Systeme im gesamten hybriden Unternehmen erreicht werden. Dies umfasst traditionelle Rechenzentren, virtualisierte Umgebungen, öffentliche Clouds oder jegliche Kombination aus ihnen, ohne dass dabei der unnötige Aufwand entsteht, der normalerweise mit alternativen Ansätzen verbunden ist.

**Abschnitt 5:**

# Fazit

Zur Gewährleistung der Einhaltung der PCI-Vorschriften ist ein Privileged Access Management praktisch unerlässlich. Aber seine Bedeutung geht über die alleinige Erfüllung von PCI-Anforderungen hinaus. Es versetzt Unternehmen in die Lage, ihre gesamte Security zu verbessern und sich gegen die heutigen externen und internen Gefahren zu wappnen. CA Privileged Access Manager bietet eine effektive Möglichkeit zur Implementierung eines Privileged Access Management, um sowohl die PCI-Vorschriften als auch andere Security-Anforderungen einzuhalten.

Mit CA Privileged Access Manager können Unternehmen Folgendes erreichen:

- Reduzierung der Kosten für die Einhaltung von PCI-Vorschriften durch Erfüllung vieler PCI-Anforderungen mit einer einzelnen Standardlösung, die sich in die bereits vorhandenen Lösungen eines Unternehmens nahtlos integrieren lässt
- Senkung sicherheitsbezogener Ausgaben und Wahrung des Unternehmensrufes durch Verhinderung zahlreicher Sicherheitsverstöße und Minimierung der Auswirkungen aller nicht verhinderten Verstöße

**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 PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

2 Cisco 2014 Annual Security Report, http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

3 Verizon 2014 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2014/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR

4 M-Trends 2014: Beyond the Breach, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

5 Data Leakage Worldwide: The High Cost of Insider Threats, http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.pdf

6 PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

7 PCI DSS Summary of Changes v2.0 to v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids



CS200-163851_1215