FORTRA™

WHITEPAPER

PCI DSS 4.0-Compliance

Mit diesen Tipps schaffen Sie es rechtzeitig!

Die Aufrechterhaltung der Compliance ist eine schwierige Aufgabe, sowohl vom Umfang her, als auch in der praktischen Umsetzung. Unternehmen müssen eine Vielzahl unterschiedlicher Richtlinien erfüllen, deren Anzahl ständig weiter wächst. Die Compliance-Regularien werden immer strenger; Unternehmen und Finanzinstitute müssen sich mit den neuen Anforderungen des Payment Card Industry Data Security Standard (PCI DSS) 4.0 vertraut machen, da die Implementierungsfrist bis 2024 läuft.

Die Erfüllung neuer oder aktualisierter Standards ist manchmal einfacher gesagt als getan. Tatsächlich haben die Unternehmen alle Hände voll zu tun mit den alltäglichen Problemen der Cybersicherheit. Die Compliance-Anforderungen verschiebt man dann häufig, bis sie unbedingt angegangen werden müssen. Dies gilt vor allem für Unternehmen, die mehr Ressourcen, Zeit und Personal, sowie eine umfassende Strategie für robuste Sicherheit und Compliance benötigen.

Talentdefizite und unterbesetzte Arbeitsgruppen sind in allen Branchen ein echtes Problem. Zeit und Mitarbeiter sind knapp und die Unternehmen neigen dazu, sich auf dringende Aufgaben anstatt auf langfristige Projekte zu fokussieren. Dieser Ansatz führt häufig zur Compliance-Torschlusspanik.

Einzelhändler und Finanzunternehmen haben aber die Möglichkeit, ihre täglichen Sicherheitsabläufe und -anforderungen durchzuführen und gleichzeitig ihre PCI DSS 4.0-Compliance aufzubauen. Sie können das schaffen, indem sie eine "touch it once"- Strategie anwenden und zwei Aufgaben in einem Schritt lösen: sich um die täglichen Prioritäten zu kümmern und effizient auf PCI DSS 4.0 umzustellen.

Dabei geht es darum, beide Punkte so zu erledigen, dass man nicht mehr darauf zurückkommen muss. Das ist so etwas wie ein Ethos, ein Denkprozess, eine Idee. Jedes Mal, wenn Sie einen Geschäftsprozess erstellen, tun Sie das mit der Haltung „wie werden wir dadurch sicherer und erfüllen den Standard PCI DSS 4.0 besser?“

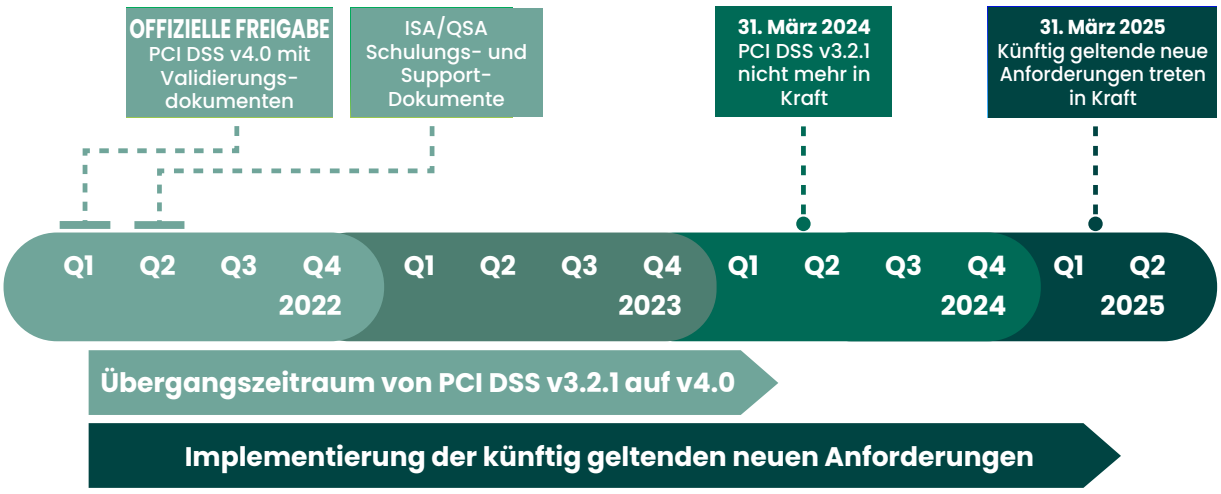
Dieser Leitfaden soll Ihnen dabei helfen, zu verstehen, worum es bei der Einhaltung von PCI DSS 4.0 geht. Gleichzeitig soll ein nach Prioritäten geordneter Fahrplan für die Einhaltung der Vorschriften erstellt werden, der Ihr Unternehmen gleichzeitig vor den alltäglichen Cyberrisiken und -bedrohungen schützt.

PCI DSS 4.0: Was ist neu daran?

Der Payment Card Industry Data Security Standard (PCI DSS) wurde 2006 mit dem Ziel entwickelt, Unternehmen, die Zahlkartendaten verarbeiten, speichern oder übertragen, dabei zu unterstützen, den Diebstahl von Karteninhaberdaten zu verhindern. PCI DSS wurde zwar speziell für ein Umfeld mit Zahlkartenkontodaten entwickelt, kann aber auch vor Bedrohungen schützen und andere Elemente des Zahlungssystems sichern.

Im Rahmen von PCI DSS 4.0 wurde eine überlappende Auslauffrist für PCI DSS Version 3.2.1 festgelegt, um den Übergang zwischen den Versionen zu erleichtern. Die Überlappung verschafft Unternehmen Zeit, sich mit der neuen Version vertraut zu machen und die notwendigen Änderungen zu planen und umzusetzen. Das folgende Diagramm, das mit freundlicher Genehmigung des PCI Security Standards Council (SSC) wiedergegeben wird, gibt einen Überblick über den Zeitplan für die Umsetzung von PCI DSS 4.0.

PCI DSS v4.0 Implementierungszeitachse



PCI DSSv3.2.1 bleibt nach der Veröffentlichung von v4.0 noch zwei Jahre lang aktiv. Dies verschafft Unternehmen Zeit, sich mit der neuen Version vertraut zu machen und die notwendigen Änderungen zu planen und umzusetzen.

Es gibt vier Hauptgründe für die Änderungen in der Version 4.0:

- Sicherstellen, dass der Standard die Anforderungen für sichere digitale Zahlungen erfüllt
- Die Sicherheit als kontinuierlichen dynamischen Prozess fördern
- Die Validierungsverfahren robuster gestalten
- Mögliche zusätzliche Methoden zu unterstützen, die die gleichen Sicherheitsziele erreichen.

Außerdem enthält die neue Version das Konzept des individuell angepassten Ansatzes. Dahinter steht der Gedanke, dass nicht alle Sicherheitsansätze gleich sind und es möglicherweise viele Wege geben kann, ein Sicherheitsziel zu erreichen. Die Version 4.0 ermöglicht die individuelle Anpassung der Anforderungen und Testverfahren auf Basis dieses Ansatzes.

Viele Unternehmen haben Sicherheitslösungen, die das Sicherheitsziel einer Anforderung erfüllen. Der individuell angepasste Ansatz ermöglicht es den Unternehmen, zu zeigen, wie ihre spezielle Lösung das Sicherheitsziel erreicht und das Risiko angeht, indem sie eine alternative Möglichkeit zur Erfüllung der Anforderung bietet.

Die gute Nachricht ist, dass sich die 12 Kernanforderungen des PCI DSS im Zuge des PCI DSS v4.0 nicht grundlegend ändern, da sie die zentrale Grundlage für den Schutz von Zahlkartendaten darstellen. Die Anforderungen sind jetzt jedoch als ergebnisgestützte Aussagen formuliert, mit einem Fokus auf die Implementierung der Sicherheitskontrolle. Bei vielen Anforderungen wird dies erreicht, indem man einfach die Angabe, was implementiert werden "muss" abändert zu einer Angabe, was das resultierende Sicherheitsergebnis "ist".

Die größten Änderungen beziehen sich auf die Authentifizierung und die Datenverschlüsselung. Da sich der Zahlungsverkehr allmählich in die Cloud verlagert hat, konzentriert sich der PCI DSS auf die Anwendung robusterer Authentifizierungsstandards für die Anmeldung für Zahlungs- und Kontrollprozesse. Zu den neuen Anforderungen gehört die Verwendung einer mehrstufigen Authentifizierung für alle Konten, die auf Karteninhaberdaten zugreifen, und nicht nur für die Administratoren, die auf die Umgebung der Karteninhaberdaten zugreifen. Außerdem beinhaltet PCI DSS 4.0 eine breitere Anwendbarkeit für die Verschlüsselung der Karteninhaberdaten, die nun auf vertrauenswürdige Netzwerke erweitert wird. Die gesamte Liste der Änderungen finden Sie im Leitfaden Summary of Changes.

Ein priorisierter Ansatz für die Compliance-Regularien nach PCI DSS 4.0

Der PCI DSS bietet durch seinen umfassenden Charakter eine Vielzahl von Sicherheitsinformationen — so viele Informationen, dass sich einige Personen, die für die Sicherheit von Zahlungskontodaten verantwortlich sind, möglicherweise fragen, wo sie anfangen sollen. Das PCI Security Standards Council hat einen priorisierten Ansatz für die Compliance entwickelt, der Unternehmen dabei hilft, das Risiko bereits in einer frühen Phase der PCI DSS-Compliance zu reduzieren.

In dem Leitfaden heißt es: *„Der priorisierte Ansatz ordnet alle PCI DSS-Anforderungen in sechs risikogestützte Sicherheitsmeilensteine ein, die Unternehmen dabei helfen sollen, sich auf dem Weg zur PCI DSS-Compliance Stück für Stück gegen die größten Risikofaktoren und eskalierenden Bedrohungen zu schützen.“*

Der priorisierte Ansatz für PCI DSS umfasst sechs Meilensteine:

1. **Speichern Sie keine unnötigen sensiblen Authentifizierungsdaten und begrenzen Sie die Aufbewahrung der Karteninhaberdaten.** Die Unternehmen können zunächst die Folgen einer Verletzung begrenzen, indem sensible Authentifizierungsdaten und andere Kontodaten gar nicht erst gespeichert werden.
2. **Schützen Sie Zugriffspunkte für Systeme und Netze und seien Sie für die Abwehr einer Verletzung bereit.**
3. **Sichere Zahlungsanwendungen.** Schwächen bei diesen Apps sind ein gängiger Zugriffsweg für die Verletzung von Systemen und den nicht autorisierten Zugriff auf Karteninhaberdaten.
4. **Überwachen und kontrollieren Sie den Zugriff auf Ihre Systeme.** Behalten Sie den klaren Überblick, wer, worauf, wann und wie auf die Karteninhaberdaten-Umgebung zugreift.
5. **Schützen Sie gespeicherte Karteninhaberdaten.** Falls die Speicherung der Karteninhaberdaten eine geschäftliche Notwendigkeit ist, implementieren Sie Kontrollen für den Schutz dieser Daten.
6. **Schließen Sie die verbleibenden Compliance-Aufgaben ab und stellen Sie sicher, dass alle Kontrollen umgesetzt sind.**

Diese Meilensteine sollen Unternehmen dabei helfen, sich Stück für Stück gegen die größten Risikofaktoren und Bedrohungen zu schützen, während sie sich auf dem Weg zur Einhaltung des PCI DSS 4.0 befinden.

Der priorisierte Ansatz und seine Meilensteine bringen sämtlichen Unternehmen folgende Vorteile:

- Einen strukturierten Ansatz für das Angehen von Risiken in der Reihenfolge ihrer Priorität
- „Schnelle Erfolge“ durch die Nutzung eines realistischen Ansatzes für die Cybersicherheit und die PCI DSS 4.0-Compliance
- Finanzielle und operative Planung
- Objektive und messbare Fortschrittsindikatoren

Alltägliche bewährte Praktiken für den Aufbau Ihrer PCI DSS 4.0-Compliance

Die Einhaltung des PCI DSS Version 4.0 mag schwierig sein, aber der Standard stellt eine verbesserte Möglichkeit dar, die fortschrittlichen Taktiken von Cyber-Kriminellen zu entschärfen. Lesen Sie zunächst den Standard PCI DSS 4.0 und machen Sie sich mit den wichtigsten Änderungen vertraut, die sich auf Ihren Compliance-Prozess auswirken könnten. Beginnen Sie dann mit der Ausarbeitung von Plänen zur Umsetzung der Änderungen in Ihren Cybersicherheitsprozessen, damit Sie auf dem richtigen Weg zur PCI DSS 4.0-Compliance bleiben.

Die folgenden Abschnitte führen Sie durch die 12 Standardanforderungen und bieten Ihnen alltägliche bewährte Praktiken, die es Ihnen ermöglichen, Ihr Unternehmen vor täglichen Bedrohungen zu schützen und gleichzeitig Ihre PCI DSS 4.0-Compliance zu verbessern. Für eine detailliertere Ansicht, siehe PCI DSS-Ressourcen.

Anforderung 1: Setzen Sie Netzwerk-Sicherheitskontrollen um und halten Sie diese aufrecht

Netzwerk-Firewalls sind sehr wichtig für Ihre Sicherheit. Allerdings reicht es für den Schutz nicht aus, einfach nur eine Firewall um das Netzwerk Ihres Unternehmens zu installieren.

1. **Erstellen Sie eine Ausgangs-Konfiguration für die Firewall:** Dokumentieren Sie vor der Implementierung von Firewall-Einstellungen die Einstellungen und Verfahren, z. B. die Hardware-Sicherheitseinstellungen, die für die Geschäftstätigkeit erforderlichen Port- oder Dienstregeln, die Begründung dieser Regeln und berücksichtigen Sie sowohl den eingehenden als auch den ausgehenden Datenverkehr.
2. **Testen Sie sämtliche Einstellungen:** Testen Sie nach der Durchführung der Konfigurationseinstellungen die Firewall extern und intern, um die Korrektheit der Einstellungen zu bestätigen.
3. **Begrenzen Sie den ausgehenden Datenverkehr (nicht nur den eingehenden):** Oft machen wir uns zu viele Gedanken über die Sperrung eingehender Ports und müssen uns daran erinnern, den ausgehenden Datenverkehr innerhalb des Netzwerks auf das Notwendige zu beschränken. Das begrenzt die Möglichkeiten von Angreifern, Daten auszuschleusen.
4. **Konfigurieren Sie die Firewalls auf persönlichen Mobilgeräten:** Richten Sie persönliche Firewalls auf mobilen Rechnerplattformen ein, um die Angriffsfläche zu begrenzen und die Verbreitung von Malware zu minimieren, wenn diese mit ungesicherten Netzwerken verbunden sind.
5. **Deaktivieren Sie die externe Firewall-Verwaltung:** Verwalten Sie die Firewall ausschließlich von innerhalb Ihres Netzwerks. Deaktivieren Sie externe Verwaltungsdienste, außer diese sind Teil einer sicher verwalteten Firewall-Infrastruktur.

Anforderung 2: Wenden Sie sichere Konfigurationen auf alle Systemkomponenten an

1. **Ändern Sie die Standardeinstellungen, um inhärente Schwächen zu verringern:** Geräte werden mit Werkseinstellungen ausgeliefert, z.B. Benutzernamen und Kennwörtern. Standardeinstellungen erleichtern die Installation und den Support von Geräten, aber sie bedeuten auch, dass jedes Modell mit demselben Benutzernamen und Kennwort ausgestattet ist. Wenn lediglich die Standardeinstellungen modifiziert werden, dann bietet dies Angreifern einen einfachen Zugriffsweg auf Ihre Umgebung. Das Ändern der Herstellereinstellungen auf jedem System, das auf Karteninhaberdaten zugreift, ist sehr wichtig.
2. **Machen Sie die Karteninhaber-Datenumgebung (Cardholder Data Environment, CDE) entsprechend den bewährten Praktiken der Branche widerstandsfähig:** Jegliches System in ihrer CDE muss widerstandsfähig gemacht werden, bevor es in den aktiven Betrieb geht. Das Ziel der Abhärtung eines Systems dient dem Entfernen unnötiger Funktionen und der sicheren Konfiguration der notwendigen Funktionen. Jede Anwendung und jedes Gerät, die/das mit einem System verbunden ist, birgt Schwächen. Gemäß PCI DSS-Anforderung 2.2 müssen Sie "*alle bekannten Sicherheitsschwachstellen beheben und mit branchenweit anerkannten Standards zur Systemhärtung umsetzen.*"
3. **Achten Sie auf Einheitlichkeit und halten Sie den Bestand aktuell:** Sobald die Systemhärtung implementiert und dokumentiert ist, müssen die Einstellungen einheitlich auf alle Systeme im Umfeld angewandt werden. Sobald jedes System und Gerät in der Domäne korrekt konfiguriert ist, müssen Sie die Verantwortlichkeit für die Aktualisierung des Bestands zuweisen. Auf diese Weise können nicht genehmigte Anwendungen und Systeme identifiziert und entfernt werden.

Anforderung 3: Schützen Sie gespeicherte Kontendaten

1. **Wissen, wo sich Ihre Daten befinden:** Verwenden Sie ein Datenerkennungsprogramm, um den Speicherort unverschlüsselter Daten zu ermitteln, damit Sie diese löschen oder verschlüsseln können. Dieses hilft auch dabei, zu bestimmen, welcher Prozess oder Ablauf möglicherweise repariert werden muss. Karteninhaberdaten können aufgrund mangelhafter Prozesse oder Fehlkonfigurationen leicht öffentlich werden. Suchen Sie zunächst am vermuteten Speicherort und untersuchen Sie dann alle Orte, an denen sie nicht abgelegt sein sollten.
2. **Verschlüsseln Sie alle ihre gespeicherten Daten:** Gespeicherte Kartendaten müssen mithilfe eines branchengängigen Algorithmus verschlüsselt werden. Viele Unternehmen haben unbeabsichtigt unverschlüsselte Primary Account Numbers (PAN). Die Unternehmen müssen nicht nur die Kartendaten verschlüsseln, sondern auch die Kodierungsschlüssel schützen. Wenn der Speicherort des Kodierungsschlüssels nicht nur eine solide Verwaltung geschützt wird, dann ist das so, als ließen Sie Ihren Haustürschlüssel im Schloss der Haustür stecken.
3. **Minimieren Sie die vorhandenen Daten:** Behalten Sie keine Daten, die Sie nicht brauchen. Minimieren Sie den Umfang von PCI DSS und fragen Sie sich, ob Sie wirklich eine Datenspeicherung benötigen.

Anforderung 4: Schutz von Karteninhaberdaten mit starker Kryptografie bei der Übertragung über offene, öffentliche Netzwerke

1. **Sichern Sie Daten, die über offene und öffentliche Netzwerke übertragen werden:** Stellen Sie fest, wohin Sie die Karteninhaberdaten versenden. Sie müssen Ihre Daten für den Versand über offene und öffentliche Netzwerke verschlüsseln.
2. **Verwenden Sie keine veralteten SSL/TLS-Versionen mehr:** Ältere SSL- und TLS-Versionen haben bekanntermaßen Sicherheitsschwächen. Sie müssen die Verwendung dieser veralteten Verschlüsselungsprotokolle einstellen, es sei denn, die Geschäftsanforderungen erfordern die Aufrechterhaltung der Abwärtskompatibilität, z. B. für die Verwendung von POS-Hardware, die neuere Versionen von Secure TLS nicht unterstützt.

Anforderung 5: Schutz von Systemen und Netzwerken vor Malware

1. **Aktualisieren Sie regelmäßig den Virenschutz:** Ein wachsames Schwachstellenmanagement ist der effektivste Weg, um das Zeitfenster für eine Gefährdung proaktiv zu verkleinern und so die Möglichkeiten für Angreifer, in Ihre Systeme einzudringen und erfolgreich wertvolle Daten zu stehlen, erheblich zu reduzieren. Teil Ihres Schwachstellenmanagements sollte ein aktualisiertes Virenschutzprogramm sein.

Anforderung 6: Entwickeln und Pflegen von Sicherheitssystemen und -software.

1. **Systeme regelmäßig aktualisieren und Patches installieren:** Die zeitnahe Implementierung von Sicherheitsupdates ist entscheidend für Ihre Sicherheitssituation. Installieren Sie auf allen kritischen Komponenten in Ihrer Umgebung Patches, z.B. auf Browsern, Firewalls, Anwendungen, Datenbanken, POS-Terminals und Betriebssystemen. Aktualisieren Sie Ihre Software regelmäßig, um die PCI DSS-Anforderung 6.3.3 zu erfüllen, die besagt, dass Unternehmen „kritische Patches innerhalb eines Monats nach Veröffentlichung installieren" müssen. Denken Sie an kritische Software-Installationen, wie z.B. Anwendungen für Kreditkartenzahlungen und mobile Geräte. Eine weitere Möglichkeit, Schwachstellen zu beseitigen, ist das Schwachstellen-Scannen, die beste Methode, um bekannte Sicherheitslücken aufzuspüren, die Cyberkriminelle ausnutzen können, um sich Zugang zu einem Unternehmen zu verschaffen und es zu gefährden.
2. **Etablieren sicherer Software-Entwicklungsprozesse:** Falls Sie Zahlungsanwendungen in Ihrem Unternehmen entwickeln, müssen Sie strenge Entwicklungsprozesse und sichere Kodierungsrichtlinien anwenden. Denken Sie daran, Anwendungen gemäß branchenweit anerkannten Standards wie OWASP zu entwickeln und zu testen.
3. **Installation von Firewalls für Internetanwendungen:** Die PCI DSS-Anforderung 6.4 schreibt die regelmäßige Überwachung, Erkennung und Verhinderung von Internet-gestützten Angriffen durch den Schutz von öffentlich zugänglichen Internetanwendungen durch Web Application Firewalls (WAF) vor. Diese Lösungen sind auf die Überwachung und Blockierung von schädlichem Internet-gestützten Datenverkehr spezialisiert.

Anforderung 7: Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten

1. **Beschränken Sie den Zugriff auf Daten und Systeme:** Sie sollten über ein aufgabenbasiertes Zugriffskontrollsystem (RBAC) mit einer definierten und aktuellen Liste von Aufgaben im Unternehmen verfügen, die den Zugriff auf Karteninhaberdaten

auf einer Need-to-know-Basis gewährt. Die Beschränkung des Zugriffs verhindert den Zugang zu sensiblen Daten durch nicht autorisierte Personen.

Anforderung 8: Identifizierung von Nutzern und Authentifizierung des Zugriffs

1. **Entwickeln Sie Vorgehensweisen für starke, einmalige Kennwörter und nutzen Sie einen Kennwort-Manager:** Wenn ein Benutzername oder ein Kennwort nicht den Anforderungen an Länge, Eindeutigkeit und Komplexität entspricht, wird er/es zu einer Schwachstelle. Um die durch die menschliche Natur bedingten Begrenzungen und Risiken auszugleichen, sollten Sie den Einsatz einer unternehmensweiten Kennwortverwaltungssoftware in Betracht ziehen, damit die Komplexität der Passwörter die Nutzererfahrung nicht beeinträchtigt.
2. **Robuste Kontenverwaltung:** PCI DSS verlangt die Deaktivierung von Standard-Konten und einmalige Benutzer- und Admin-Konten-Namen. Ein Unternehmen sorgt für mehr Sicherheit, wenn es einem möglichen Angreifer mehr Hindernisse in den Weg stellt.
3. **Implementieren Sie die Multi-Faktor-Authentifizierung:** Ein einziges Kennwort, egal, wie stark es ist, darf nicht die einzige Sicherheitsmaßnahme sein. Die Multi-Faktor-Authentifizierung (MFA) ist die wirkungsvollste Lösung für die Sicherung des Fernzugriffs. Sie ist eine der neuen Anforderungen von PCI DSS 4.0. Ihre Authentifizierungsverfahren sollten band-extern und unabhängig voneinander sein. Es sollte eine physische Trennung zwischen den Authentifizierungsfaktoren geben, so dass der Zugriff auf einen Faktor nicht auch den Zugriff auf einen anderen Faktor gewährt. Falls ein Faktor unsicher ist, dann beeinträchtigt dies nicht die Integrität und Vertraulichkeit anderer Faktoren. Darüber hinaus fordert PCI DSS, dass Sie „ *eine Multi-Faktor-Authentifizierung für alle Fernzugriffe auf das Netzwerk (sowohl für Benutzer als auch für Administratoren, einschließlich des Zugriffs durch Dritte für Support oder Wartung) von außerhalb des Netzwerks des Unternehmens einführen.*"

Anforderung 9: Beschränkung des physischen Zugangs

1. **Steuern Sie den physischen Zugang zu Ihren Geschäftsräumen:** Reduzieren Sie physische Sicherheitsrisiken durch die Implementierung von Sicherheitsrichtlinien, die die Sicherheit wichtiger Anlagen und Daten vor Ort gewährleisten. Sie können diese kritischen Anlagen beispielsweise in einer gesicherten Einrichtung schützen. Sie könnten auch den Zugang für Außenstehende auf einen überwachten Eingang beschränken und von Nicht-Mitarbeitern verlangen, Besucherausweise zu tragen.
2. **Behalten Sie den Überblick über POS-Terminals:** Unternehmen, die POS-Systeme oder mobile Zahlungsgeräte verwenden, müssen eine aktualisierte Liste aller Geräte führen, diese Geräte regelmäßig überprüfen und Mitarbeiter schulen, die täglich mit kartengestützten Geräten umgehen.

Anforderung 10: Protokollierung und Überwachung jedes Zugriffs

1. **Prüfen Sie regelmäßig die Systemprotokolle und -warnungen:** Systeme, die Protokolle führen, überwachen Netzwerkaktivitäten, untersuchen Systemereignisse, warnen vor fragwürdigen Aktivitäten und zeichnen Benutzeraktivitäten auf, die in Ihrer Umgebung stattfinden. Das Erstellen und die Übertragung von Protokollen an einen zentralen Ort, einen Protokollserver in den Geschäftsräumen oder einen Internet-Dienst, sind erforderlich. Um nach Fehlern, Unregelmäßigkeiten oder verdächtigen, vom Üblichen abweichenden Aktivitäten zu suchen, sollten die Unternehmen ihre Aufzeichnungen täglich analysieren. Ein effektiveres Sicherheitsprogramm und eine schnellere Reaktion auf Sicherheitsvorfälle sind die Vorteile einer regelmäßigen Protokollüberwachung. Die Protokollanalyse zeigt nicht nur, dass Sie sich zur Einhaltung der PCI DSS-Regeln verpflichtet haben, sondern hilft in Kombination mit einer regelmäßige Überwachung auch, ein- und ausgehende Bedrohungen abzuwehren.

Anforderung 11: Regelmäßiges Testen der Sicherheit von Systemen und Netzwerken

1. **Erfassen Sie Ihre Umgebung, suchen Sie regelmäßig nach Schwachstellen und führen Sie Eindringtests durch:** Angreifer können sich über Schwachstellen in Browsern, E-Mail-Clients, POS-Software, Betriebssystemen und Server-Schnittstellen Zugang zu einer bestimmten Umgebung verschaffen. Viele der neu aufgedeckten Fehler und Schwachstellen können behoben werden, bevor Angreifer sie ausnutzen können, indem Sicherheitsupdates und Patches für Systeme in Umgebungen mit Karteninhaber- oder sensiblen Daten installiert werden. Für das Auffinden und Beheben von Schwachstellen ist ein Schwachstellen-Scanverfahren hilfreich. Code-Tests und unabhängige Eindringtests können viele der Schwachstellen aufdecken, die häufig im Anwendungscode benutzerdefinierter interner

Anwendungen zu finden sind. Eindringtests und Schwachstellenscans ergänzen einander und tragen zur Erreichung des höchsten Grades der Netzwerksicherheit bei. Diese Scans und Tests sind die beste Verteidigungslinie bei der Identifizierung von Schwachstellen, so dass Unternehmen diese vor dem Einsatz korrigieren können.

Anforderung 12: Unterstützung der Informationssicherheit durch Richtlinien und Programme

1. **Dokumentieren und aktualisieren Sie regelmäßig alle Sicherheitspraktiken im Unternehmen:** Sämtlichen Mitarbeitern sollten die schriftlichen Vorgehensweisen leicht zugänglich sein. Im Falle einer Verletzung kann die Dokumentation dabei helfen, Ihr Unternehmen vor einer möglichen Haftung zu schützen. Vollständig und genau niedergeschriebene Sicherheitsrichtlinien und -verfahren erleichtern es den Ermittlern, sich ein Bild von den Sicherheitsmaßnahmen Ihres Unternehmens zu machen, und zeigen, wie proaktiv und engagiert Ihr Unternehmen in Sachen Sicherheit agiert. Die Unternehmen sollten Ihre Dokumentation über Sicherheitsmaßnahmen und Maßnahmen im Rahmen der PCI DSS 4.0-Compliance regelmäßig aktualisieren.
2. **Etablieren eines Prozesses zur Risikoeinschätzung:** PCI schreibt vor, dass jede Organisation eine jährliche Risikoeinschätzung durchzuführen hat, die zentrale Ressourcen, Bedrohungen, Schwächen und Gefahren feststellt. Unternehmen können durch diese Maßnahme Informationssicherheitsbedrohungen identifizieren, organisieren und verwalten. Ein Bestandteil der Risikobewertung ist es, den ermittelten Bedrohungen eine Rangfolge oder Punktzahl zuzuweisen. Dies gibt Ihnen eine Leitlinie an die Hand, welche Schwachpunkte zuerst angegangen werden sollten und ermöglicht die Festlegung von Prioritäten. Indem Sie Risiken methodisch klassifizieren, bewerten und entschärfen, können Sie das Zeitfenster verkleinern, in dem ein Angreifer Zugang zu Ihren Systemen erhält, diese beschädigt und schließlich den Angriff beendet.
3. **Den Vorfallsreaktionsplan erstellen und testen:** Sie müssen sich auf die Auswirkungen einer Datenpanne vorbereiten. Sie sind dafür verantwortlich, die Kontrolle über den Vorfall zu behalten, den Schaden für die Kunden zu minimieren, die Kosten im Zusammenhang mit einer Datenschutzverletzung gering zu halten, ordnungsgemäß mit den verschiedenen Behörden zu kommunizieren, wie es die verschiedenen Standards und Vorschriften vorsehen, und Ihr Unternehmen zu schützen. Eine effektive Vorfallsreaktionsstrategie kann die Auswirkungen von Sicherheitsverletzungen vermindern, Bußgelder niedrig halten, negative Publicity minimieren und die Rückkehr zum normalen Betrieb beschleunigen.
4. **Bereitstellung einer Sensibilisierungsschulung für alle Mitarbeiter:** Die meisten Sicherheitsverletzungen sind auf menschliche Fehler zurückzuführen. Zwar sind viele Mitarbeiter nicht böswillig, aber sie vergessen häufig bewährte Sicherheitsverfahren oder wissen nicht genau, was von ihnen erwartet wird. Leider nutzen viele Kriminelle menschliche Fehler aus, um private Informationen zu erhalten. Den Mitarbeitern müssen spezifische Leitlinien an die Hand gegeben werden und es muss eine fortlaufende Schulung stattfinden. Die Mitarbeiter werden durch ein Programm zur Sensibilisierung für Sicherheitsfragen, das häufige Schulungen umfasst, an den Stellenwert von Sicherheit erinnert, insbesondere indem sie über neue Sicherheitsrichtlinien und -verfahren auf dem Laufenden gehalten werden.

Abschließende Gedanken

Bis zum Ablauf der Frist für die Umsetzung der PCI DSS 4.0-Compliance 2024 ist noch genügend Zeit. Beginnen Sie möglichst früh damit und sie beschreiten den richtigen Weg zur Umstellung. Warten Sie mit der Umstellung auf PCI DSS 4.0 nicht bis 2024. Verteilen Sie Ihre Bemühungen und aktualisieren Sie nach und nach auf PCI DSS 4.0.

Denken Sie an Ihren zukünftigen Bedarf und flechten Sie diesen in Ihre Unternehmensstrategie und Ihr Sicherheitsprogramm ein, damit Sie Ihre Zeit effektiv nutzen können. Konzentrieren Sie sich auf Punkte, die generell langfristig von Vorteil für das Unternehmen sind.

Wie Fortra dabei helfen kann

Fortras Portfolio an Cybersecurity- und Compliance-Angeboten bietet eine breite Palette an Lösungen und Dienstleistungen, die Unternehmen dabei unterstützen, die Anforderungen von PCI DSS 4.0 zu erfüllen und die täglichen Herausforderungen beim Schutz des Unternehmens vor Risiken und Bedrohungen zu meistern. In der folgenden Tabelle werden die Anforderungen von PCI DSS 4.0 den Lösungen von Fortra gegenübergestellt.

PCI DSS 4.0-Anforderungen	Fortra-Lösung
Anforderung 1 Setzen Sie Netzwerk-Sicherheitskontrollen um und halten Sie diese aufrecht	
Anforderung 2 Wenden Sie sichere Konfigurationen an	Die Tripwire Enterprise-Sicherheitskonfigurationsmanagement-Funktionalität von Fortra stellt sicher, dass Unternehmen die Konfigurationen von Netzwerken, Servern, Firewalls und allen anderen Komponenten überwachen.
Anforderung 3 Schützen Sie gespeicherte Kontendaten	Mit dem Fortra-Produkt Digital Guardian Enterprise DLP können Kunden vordefinierte PCI-Richtlinien verwenden, um den Ausgang von Kreditkarteninformationen über eine Vielzahl von gemeinsamen Austrittspunkten zu überwachen und zu blockieren. Die Fortra-Anwendungen Digital Guardian Network DLP untersuchen den gesamten Netzwerkverkehr und setzen vorkonfigurierte Richtlinien für PCI und andere Compliance-Anforderungen zum Schutz von Daten durch.
Anforderung 4 Schutz von Karteninhaberdaten mit starker Kryptografie bei der Übertragung über offene, öffentliche Netzwerke	GoAnywhere MFT von Fortra ist eine sichere Managed-File-Transfer-Lösung, die Benutzern hilft, sensible Datenübertragungen konform mit PCI DSS zu halten. Secure Collaboration von Fortra schützt Dateien, die sensible PII- und PCI-Daten enthalten, egal, wohin und wie sie weitergegeben werden. Unternehmen können den Zugriff auf Karteninhaberdaten verschlüsseln und kontrollieren sowie die Daten verfolgen, prüfen und den Zugriff darauf widerrufen.
Anforderung 5 Schutz von Systemen und Netzwerken vor Malware	Powertech Antivirus von Fortra schützt Ihre Server vor einer Vielzahl von Viren, Malware, Ransomware und weiteren Bedrohungen.
Anforderung 6 Entwickeln und Pflegen von Sicherheitssystemen und -software	Beyond Security von Fortra hilft bei der Erkennung von Anwendungsschwachstellen in einem frühen Stadium des Entwicklungsprozesses mit Hilfe von Dynamic Application Security Testing (DAST)- und Static Application Security Testing (SAST)-Lösungen. Fortras Lösungen für das Schwachstellenmanagement helfen dabei, Schwachstellen in Ihrer Umgebung zu identifizieren und zu priorisieren, um Sicherheitslücken zu schließen, bevor Angreifer diese entdecken. Die Konfigurationsmanagement-Funktionen von Tripwire Enterprise von Fortra helfen dabei, ungeplante Änderungen in Ihrer Umgebung zu erkennen und die Systemintegrität zu gewährleisten. Alert Logic MDR Essentials von Fortra umfasst Tools zur Bewertung und Verwaltung des Gefährdungsgrads, die externe, netzwerk- und agentenbasierte Scans nutzen, um einen Panoramablick auf die Gefährdung in IT-Umgebungen vor Ort und in der Cloud zu erstellen. Alert Logic von Fortra ist ein zugelassener PCI-Scan-Anbieter. Alert Logic Managed WAF von Fortra schützt Internetanwendungen durch kontinuierliche Erkennung und Abwehr von Internet-gestützten Angriffen.
Anforderung 7 Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten	Die Access Assurance Suite der Core Security von Fortra hilft bei der Identifizierung und Zugriffskontrolle in Ihrem gesamten Unternehmen über eine einzige Schnittstelle. Core Privileged Access Manager (BoKS) unterstützt Sie bei der Kontrolle des Zugriffs auf kritische Systeme und Informationen und der entsprechenden Berechtigungen.
Anforderung 8 Identifizierung von Nutzern und Authentifizierung des Zugriffs	Bei Core Password von Fortra handelt es sich um eine führende Lösung für sicheres Self-Service-Kennwortmanagement mit mehreren Zugangsoptionen, robuster Service-Desk-Integration und der Möglichkeit, konsistente Kennwortrichtlinien für jedes System, jede Anwendung und jedes Internetportal durchzusetzen.

PCI DSS 4.0-Anforderungen	Fortra-Lösung
Anforderung 9 Beschränkung des physischen Zugangs	
Anforderung 10 Protokollierung und Überwachung jedes Zugriffs	DasTripwire LogCenter von Fortra ist eine Correlation Engine, die eine zentrale Erfassung, Analyse und Bereitstellung von Protokollen ermöglicht. Der Dienst Alert Logic MDR Professional von Fortra sorgt für die Verwaltung, Speicherung und Analyse von Protokollen über verdächtige/schädliche Aktivitäten zum Zeitpunkt der Aufnahme, wobei fortschrittliche Analyseverfahren wie UBAD zum Einsatz kommen und gegebenenfalls von einem SOC-Analysten ausgewertet werden. Alert Logic Health Console und Network Health View überwachen den Zustand der Alert Logic Security Appliances und informieren darüber.
Anforderung 11 Regelmäßiges Testen der Sicherheit von Systemen und Netzwerken	Die Integritätsverwaltungsfähigkeiten von Tripwire Enterprise von Fortra sorgen für ein klares Bild und zeigen, wann und wo Änderungen durchgeführt wurden. Als PCI Approved Scanning Vendor (ASV) unterstützt Fortra Sie mit seinen Lösungen für das Schwachstellenmanagement bei der Durchführung umfassender Sicherheitsbewertungen, die es Ihnen ermöglichen, die für Ihr Unternehmen wichtigsten Risiken zu priorisieren. Alert Logic MDR Essentials von Fortra umfasst Tools zur Bewertung und Verwaltung des Gefährdungsgrads, die externe, netzwerk- und agentenbasierte Scans nutzen, um einen Panoramablick auf die Gefährdung in IT-Umgebungen vor Ort und in der Cloud zu erstellen. Alert Logic von Fortra ist ein zugelassener PCI-Scan-Anbieter. Core Security Core Impact von Fortra hilft bei der effizienten Durchführung fortgeschrittener Eindringtests. Mit geführter Automatisierung und zertifizierten Exploits können Sie Ihre Umgebung sicher mit denselben Techniken testen, die die heutigen Gegenspieler nutzen.
Anforderung 12 Unterstützung der Informationssicherheit durch Richtlinien und Programme	Terranova Security von Fortra bietet einen zielgerichteten, ansprechenden und praktischen auf den Menschen ausgerichteten Ansatz für die Sicherheitsbewusstseins-Schulung und umfasst ein Schulungsmodul speziell für PCI DSS.

Wenn Sie nicht über die Kapazität verfügen, all diese Aktivitäten zu verwalten, können unsere auf Tripwire und AlertLogic gestützten Services-Teams als Erweiterung Ihres Teams fungieren, um Ihre Sicherheitsrisiken zu verringern und die PCI DSS 4.0-Compliance zu vereinfachen.

Wenn Sie mehr darüber erfahren möchten, wie Fortra Sie bei der Umsetzung der PCI DSS 4.0-Compliance unterstützten kann, sehen Sie sich unsere zusätzlichen PCI-Ressourcen an oder wenden Sie sich an uns. Wir hören Ihnen gerne zu uns möchten Sie unterstützen.

FORTRA™

Fortra.com

Über Fortra

Fortra ist ein Cybersicherheits-Unternehmen wie kein zweites. Wir schaffen eine einfachere, stärkere Zukunft für unsere Kunden. Unsere bewährten Experten und unser Portfolio an integrierten und skalierbaren Lösungen bringen Ausgewogenheit und Kontrolle in Unternehmen auf der ganzen Welt. Wir führen positive Veränderungen herbei und sind Ihr unermüdlicher Verbündeter, der Ihnen bei jedem Schritt Ihrer Reise in Sachen Cybersicherheit ein sicheres Gefühl gibt. Erfahren Sie mehr auf fortra.com.