AKAMAI-LÖSUNGSÜBERBLICK

Finanzinstitute mit Akamai auf PCI DSS-Compliance vorbereiten

Da PCI DSS v4.0 die bedeutendsten Änderungen an den Sicherheitsstandards der Zahlungskartenbranche seit 2004 mit sich bringt, müssen sich Finanzinstitute schnell anpassen, um die Compliance zu sichern. Das umfassende Rahmenwerk, das vom PCI Security Standards Council aufgestellt wurde, schreibt strenge Maßnahmen zum Schutz von Karteninhaberdaten vor. Die Lösungen von Akamai ermöglichen es Finanzinstituten, diese neuen Anforderungen durch erweiterte Sicherheitsfunktionen, kontinuierliche Überwachung und gründliche Penetrationstests zu erfüllen. Unsere Tools wurden entwickelt, um die Compliance zu optimieren, Kundendaten zu schützen und Ihr Unternehmen dabei zu unterstützen, bis zur PCI-Frist im März 2025 bereit zu sein.

Einheitliche Compliance: Vereinfachung von PCI DSS mit einem Anbieter

Für Finanzinstitute umfasst die PCI DSS-Compliance zur Erfüllung der Anforderungen nicht nur Mitarbeiterschulungen und Unternehmensrichtlinien, sondern auch fortschrittliche Sicherheitssoftware. Angesichts der umfassenden Anforderungen bedeutet dies häufig die Zusammenarbeit mit mehreren Anbietern. Einige Anforderungen erfordern möglicherweise eine Firewall, während andere das Identitätsmanagement betreffen. Finanzinstitute, die einen einzigen Anbieter mit integrierter Technologie finden, profitieren von einem vereinfachten Auditprozess und verbesserter Sicherheit für die Finanzdaten ihrer Kunden. Die Einführung robuster Cybersicherheitslösungen im Rahmen einer breiteren Sicherheitsstrategie, die diese Anforderungen erfüllen, kann langfristig zu Kosteneinsparungen und geringerer Komplexität führen. Das Lösungsportfolio von Akamai erfüllt umfassend bestehende und kommende PCI DSS-Anforderungen und bietet Finanzinstituten ein nahtloses Nutzererlebnis.

Vorteile

- **Optimierung der Sicherheits- und Compliance-Workflows**
- **Geringerer Aufwand für Audits dank spezieller PCI-Funktionen**
- **Erhalt und Protokollierung verwertbarer PCI-Compliance-Warnungen**
- **Schutz sensibler Finanzdaten**
- **Steigerung der betrieblichen Effizienz und Senkung der Compliance-Kosten**

Bestimmung des Geltungsbereichs

Eine große Herausforderung für Finanzinstitute, die PCI DSS-Anforderungen erfüllen möchten, ist die Frage des Geltungsbereichs. Anwendungen und Netzwerkumgebungen, die im Rahmen der Vorschriften als „im Geltungsbereich“ eingestuft werden, können komplex sein und sich über verschiedene Arten von Infrastruktur, Technologie und mehrere Standorte hinweg erstrecken. Da Finanzinstitute sowohl Cloudinfrastrukturen als auch SaaS-basierte Anwendungen nutzen, fügt diese hybride Umgebung mit On-Premise- und On-Demand-Services eine zusätzliche Ebene der Komplexität hinzu. Für Finanzinstitute, einschließlich solcher mit automatischer Skalierung im E-Commerce-Bereich, kann es besonders schwierig sein, den Standort einer bestimmten Workload jederzeit zu erkennen.

Finanzinstitute haben interne Firewalls, VLANs und Zugriffskontrolllisten eingeführt, um diese Herausforderung des Geltungsbereichs anzugehen. Diese älteren Anwendungen können jedoch oft nicht mit hybriden Umgebungen Schritt halten, was zu zusätzlicher Komplexität, mehr Ausfallzeiten und Betriebsaufwand führt und dabei Sicherheitslücken verursacht.

Akamai Guardicore Segmentation bietet Transparenz in die Karteninhaberdatenumgebung (Cardholder Data Environment, CDE) und ihre Grenzen – ein entscheidender Schritt im Compliance-Prozess. Diese Transparenz hilft Finanzinstituten, mehrere PCI DSS-Anforderungen zu erfüllen und bietet eine umfassende Übersicht über ihr Netzwerk. Zum Beispiel:

- Anforderung 1.2.3 verlangt, dass Unternehmen über ein Diagramm ihres Netzwerks verfügen. Das Dashboard von Akamai Guardicore Segmentation zeigt alle Verbindungen zwischen dem CDE und anderen Netzwerken an und unterstützt Finanzinstitute so bei der Erfüllung dieser Anforderung.
- Anforderung 1.2.4 erfordert, dass Unternehmen ein Datenflussdiagramm pflegen, das aufzeigt, wie Kontodaten über Systeme und Netzwerke hinweg übertragen werden. Das Dashboard von Akamai Guardicore Segmentation unterstützt Finanzinstitute bei der Überprüfung dieser Anforderung, indem die erforderlichen Verbindungen angezeigt werden.

Durchsetzung von Kontrollen

- Anforderung 1.2.5 gibt vor, dass alle zulässigen Services, Protokolle und Ports identifiziert, genehmigt und eindeutig geschäftlich begründet werden müssen. Akamai Guardicore Segmentation ermöglicht es Finanzinstituten, diese Anforderung zu erfüllen, indem Richtlinien implementiert werden, die universell durchgesetzt werden und festlegen, welche Protokolle oder Services zulässig sind und welche nicht.

Clientseitiger Schutz

Finanzinstitute, die Zahlungskartendaten akzeptieren, sind nicht nur für ihre eigenen Umgebungen verantwortlich. Der Einsatz von JavaScript in der modernen Webentwicklung hat zwar für mehr Innovation und Konsistenz gesorgt hat, hat Zahlungskartenverarbeiter aber auch vor neue Herausforderungen gestellt. Die dezentrale clientseitige Ausführung von JavaScript und die Abhängigkeiten von Drittanbietern erschweren es Finanzinstituten die Überwachung und Verwaltung. Angreifer können sich diese Lücke zunutze machen, indem sie schädlichen Code in Websites auf der Clientseite einschleusen, um vertrauliche Daten zu stehlen. Diese Arten von Angriffen – etwa Web-Skimming, Formjacking und Magecart – erfreuen sich immer größerer Beliebtheit, was wiederum zu neuen Anforderungen an den clientseitigen Schutz und die Skriptüberwachung führt.

PCI DSS v4.0 verlangt von Finanzinstituten, alle JavaScript-Vorgänge auf den Zahlungsseiten ihrer öffentlich zugänglichen Website zu verfolgen, zu inventarisieren und zu rechtfertigen. Gemäß Anforderung 6.4.3 müssen sie die Verhaltensintegrität und die Autorisierung aller Skripte gewährleisten und eine Bestandsaufnahme dieser Skripte mit schriftlicher Begründung ihrer jeweiligen Notwendigkeit vorlegen. Darüber hinaus müssen Finanzinstitute gemäß Anforderung 11.6.1 alle nicht autorisierten Änderungen auf ihren Zahlungsseiten erkennen und darauf reagieren. Autorisierte Mitarbeiter müssen über alle Änderungen an HTTP-Kopfzeilen und Inhalten von Zahlungsseiten durch den Kundenbrowser informiert werden. Dazu gehören Indicators of Compromise, Änderungen, Ergänzungen oder Löschvorgänge.

> Mit Akamai Guardicore Segmentation haben wir unsere Angriffsfläche deutlich reduziert, ohne dabei Kosten oder Verzögerungen durch die Aktualisierung älterer Firewalls zu verursachen.
>
> **– Dave Wigley,**
> **CISO, Daiwa Capital Markets Europe**

Zusammenfassend lässt sich sagen, dass Finanzinstitute gemäß PCI DSS v4.0 folgende Verpflichtungen haben:

- Verwalten eines Inventars und Rechtfertigung aller Skripte, die auf Zahlungsseiten ausgeführt werden
- Sicherstellen, dass alle Skripte autorisiert sind und die vorgesehenen Aktionen ausführen
- Einrichten von Erkennungs-, Warnungs- und Reaktionsmechanismen, um unbefugte Änderungen an Skripten, Manipulationen und Datenextraktion auf Zahlungsseiten zu verhindern

Akamai Client-Side Protection & Compliance bietet umfassende Unterstützung für Finanzinstitute bei der Erfüllung der Anforderungen 6.4.3 und 11.6.1 des PCI DSS v4.0. Es verfolgt und inventarisiert Skripte auf Zahlungsseiten, um deren Integrität und Autorisierung zu erhöhen. Sicherheitsteams können den Zweck von Skripten, die auf Zahlungsseiten ausgeführt werden, problemlos mit vordefinierten Begründungen und automatisierten Regeln begründen. Die Lösung überwacht außerdem Änderungen an HTTP-Headern und den Schutz von Zahlungsseiten, um vor Seitenmanipulationen zu schützen. Ein umfassendes Dashboard und spezielle PCI-Warnmeldungen erleichtern die schnelle Reaktion auf Ereignisse mit Compliance-Bezug und liefern Nachweise für Audits.

Schutz vor Angriffen

Der Schutz von Karteninhaberdaten ist ein Grundprinzip von PCI DSS. Mit der zunehmenden Verbreitung von Webanwendungen und APIs können diese Daten aber auch zu Einstiegspunkten für Angreifer werden. Zur Erfüllung von PCI DSS benötigen Finanzinstitute einen starken Schutz vor Malware, Zero-Day-Angriffen und anderen Aktivitäten, die zu Datenlecks führen können.

Akamai App & API Protector mit dem Maleware Protection-Modul kann Finanzinstitute dabei unterstützen, sich vor dem Verlust von Zahlungskartendaten zu schützen, indem Dateien an der Edge gescannt werden, bevor sie in das Netzwerk eindringen und Malware verbreiten können. APIs können neue Schwachstellen verursachen, die Angreifer, die Zahlungskartendaten abgreifen wollen, ausnutzen können. Viele Finanzinstitute haben nicht einmal einen Überblick über all ihre APIs, geschweige denn können sie nachweisen, dass diese sicher sind. Jede API, die Karteninhaberdaten empfängt oder überträgt, fällt in den Geltungsbereich des PCI DSS, d. h. Finanzinstitute müssen die API-Entwicklung und -Authentifizierung überwachen und diese APIs schützen.

Akamai API Security automatisiert die kontinuierliche Erkennung von APIs in Ihrer gesamten Umgebung. Der API und dem Endpunkt wird eine Risikobewertung zugewiesen, indem APIs mit vorhandener Dokumentation verglichen und Sicherheits-, Entwickler- und API-Teams über Fehlkonfigurationen und Schwachstellen benachrichtigt werden. Diese kontinuierliche Automatisierung sorgt dafür, dass Schwachstellen auch bei jeder Aktualisierung Ihres API-Bestands bewertet werden.

Fazit

Während das ultimative Ziel der Implementierung von PCI DSS-Kontrollen darin besteht, Karteninhaberdaten und damit auch Ihre Kunden und Ihr Unternehmen zu schützen, müssen Finanzinstitute auch die Auditoren zufrieden stellen. Und genau hier bietet ein einziger Anbieter deutliche Vorteile. Mit Echtzeit- und Verlaufsansichten Ihres Netzwerks können Sie viele Aspekte ihres Audits schneller und einfacher erfüllen. Darüber hinaus kann die Zusammenarbeit mit einem einzigen Anbieter, der nachweislich führend in der Branche ist – und über eine Reihe von Kunden verfügt, die die PCI DSS-Anforderungen bereits erfolgreich erfüllen – zu reibungsloseren Umsetzungen, schnelleren Audits und fortlaufendem Compliance-Support führen. Dank der umfassenden Transparenz und der integrierten Lösungen von Akamai können Finanzinstitute ihre Compliance-Maßnahmen optimieren und ihre Abwehrmaßnahmen gegen sich ständig weiterentwickelnde Bedrohungen stärken.

Weitere Informationen erhalten Sie unter akamai.com oder vom Vertriebsteam von Akamai.