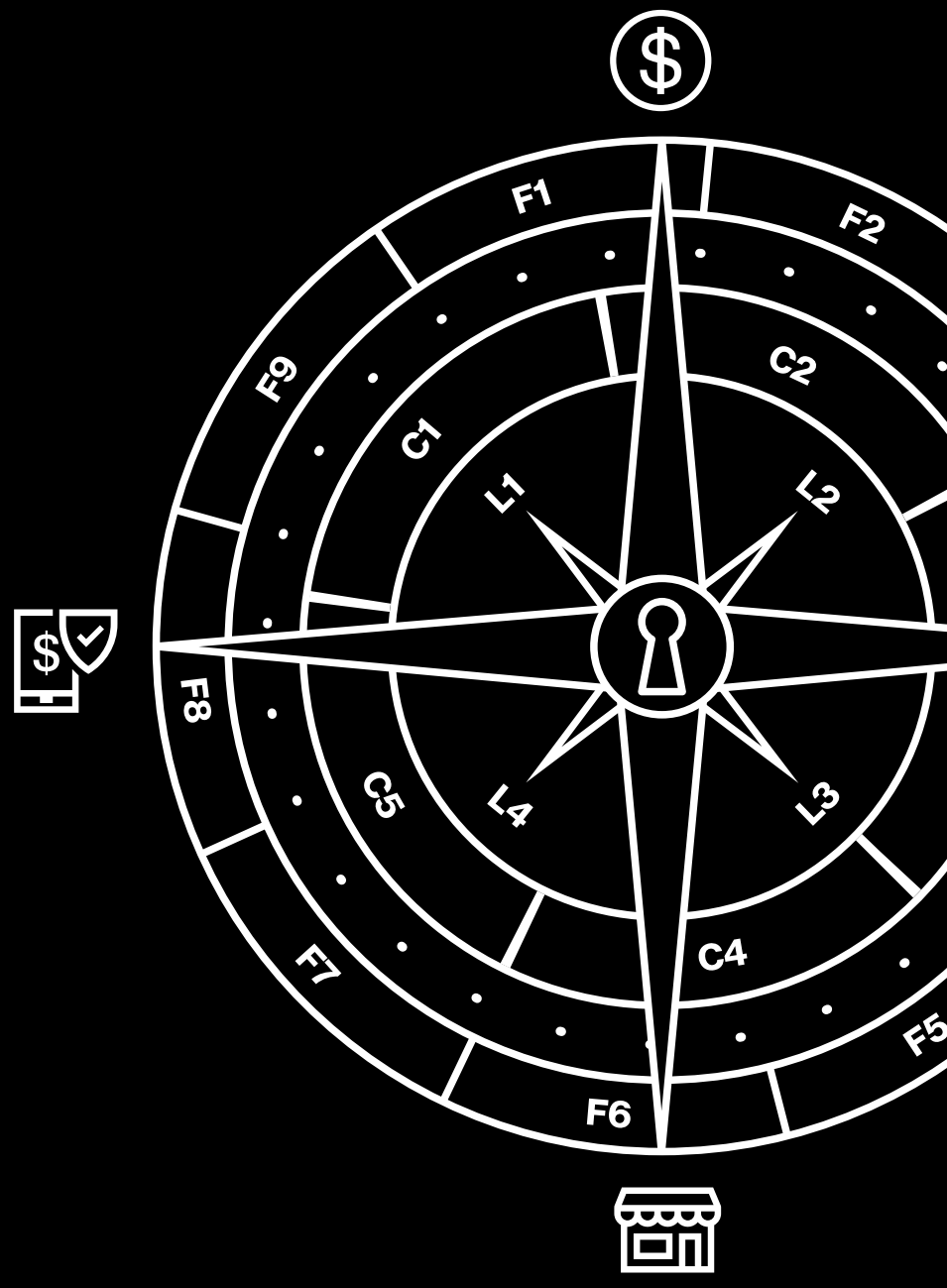
Payment Security Report 2019

Überblick über die Finanzbranche



verizon

Das Geschäftsumfeld der Finanzbranche verändert sich derzeit drastisch. Kunden verlangen neue Kommunikationskanäle und neue Methoden für benutzerspezifische Transaktionen, insbesondere auf Mobilgeräten. Gleichzeitig dringen Unternehmen aus anderen Branchen mit neuen Finanzprodukten in den Markt ein.

In diesem hart umkämpften und stark regulierten Sektor wird der zuverlässige Schutz von Kartendaten immer wichtiger. Die Kunden haben hohe Erwartungen und gehen davon aus, dass Finanzdienstleister mehr über den Datenschutz bei Zahlungsvorgängen wissen als andere Unternehmen.

Verizon veröffentlicht den Payment Security Report (PSR) 2019, um Unternehmen bei diesen Herausforderungen zu unterstützen. Der Bericht liefert einzigartige Informationen zu Sicherheitstrends in der Zahlungskartenbranche. Außerdem erklären wir darin, wie sich mit neuen richtungsweisenden Tools und Leitfäden, beispielsweise dem Verizon 9-5-4 Compliance Program Performance Evaluation Framework, Datenschutz und Compliance verbessern lassen.

Rückschritt statt Fortschritt

Wenn Finanzdienstleister effektive Sicherheitsmaßnahmen zum Schutz der Kartendaten einführen und die PCI-DSS-Anforderungen (Payment Card Industry Data Security Standard) erfüllen, gewinnen sie das Vertrauen der Kunden und verschaffen sich einen Wettbewerbsvorteil. Doch der Verizon PSR 2019 zeigt, dass Finanzdienstleister dabei Unterstützung benötigen.

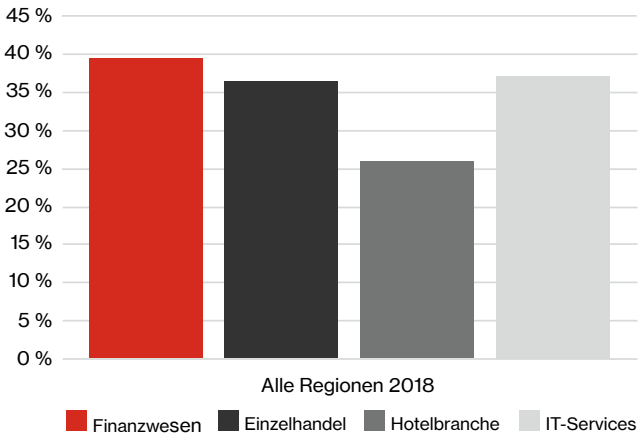


Abbildung 1: Weltweite Compliance nach Branche

In der Finanzbranche ist der Anteil der Unternehmen mit vollständiger PCI-DSS-Compliance mit 39,0 % höher als in den anderen untersuchten Branchen (Einzelhandel, Hotel- und Gaststättengewerbe und IT-Services), doch der Trend ist seit zwei Jahren rückläufig. Im PSR 2017 waren 59,1 % der untersuchten Finanzdienstleister vollständig PCI-DSS-konform, 2018 waren es immerhin noch 47,9 %, in diesem Jahr nur noch 39,0 %.

Was ist PCI DSS?

Führende Kartenanbieter haben den Payment Card Industry Data Security Standard (PCI DSS) zur Vermeidung des Betrugs bei Kartenzahlungen eingeführt. Dabei geht es vorrangig um den Schutz der Kartendaten, aber der Standard basiert auf grundlegenden Sicherheitsprinzipien, die für alle Datentypen gelten. Es werden beispielsweise Aufbewahrungsrichtlinien, Verschlüsselungsmethoden, physische Sicherheitsmaßnahmen, Authentifizierungsmethoden und Zugangskontrollen abgedeckt. Weitere Informationen finden Sie unter pcisecuritystandards.org.

Der Schutz von Zahlungskartendaten ist unverzichtbar – aber trotzdem erreichen nicht alle Unternehmen eine vollständige Compliance.

Die ist nicht nur in der Finanzbranche so. Verizon veröffentlicht den PSR seit neun Jahren und die Rate für die vollständige PCI-DSS-Compliance stieg zunächst in allen Branchen, geht aber seit 2017 kontinuierlich zurück. Andere QSA-Unternehmen (Qualified Security Assessor) verzeichnen ebenfalls einen Rückgang bei der vollständigen Compliance.

Trotz dieses Abwärtstrends blieb die Kontrolllücke (die angibt, wie weit Unternehmen von der vollständigen PCI-DSS-Compliance entfernt sind) mit 7,2 % gegenüber dem Vorjahr unverändert. Betrachtet man nur die Unternehmen, die die Interimsprüfung nicht bestanden haben, zeigt sich eine positivere Entwicklung. Im PSR 2019 ist die Kontrolllücke im Vergleich zum Vorjahr um 6,2 Prozentpunkte auf 10,2 % geschrumpft.

Unternehmen im asiatisch-pazifischen Raum (APAC-Region) schneiden besser ab: 69,6 % erzielten eine vollständige PCI-DSS-Compliance. In Europa, dem Nahen Osten und Afrika (EMEA-Region) erreichten 48,4 % vollständige Compliance. In Nord- und Südamerika sind es allerdings nicht einmal ein Viertel aller Unternehmen (20,4 %).

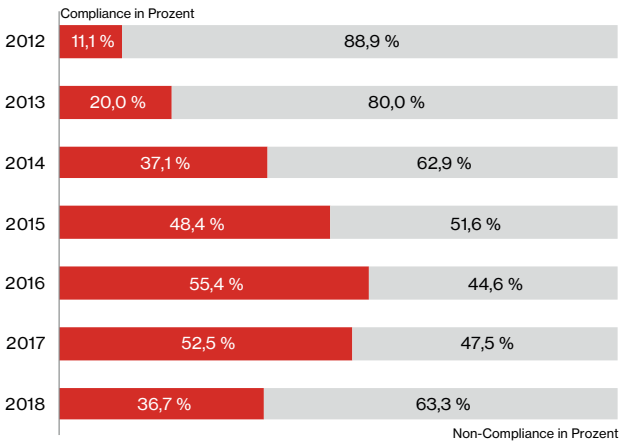


Abbildung 2: Vollständige Compliance nach Jahr

Warum ist die Erfüllung der PCI-DSS-Anforderungen so wichtig?

Wir haben PCI-DSS-Compliance und Sicherheitsverletzungen in Bezug auf Zahlungskartendaten ab dem Jahr 2008 abgeglichen und keinen einzigen Fall gefunden, in dem ein Unternehmen, das zum Zeitpunkt des Vorfalls alle 12 PCI-DSS-Anforderungen erfüllte, einen Verlust von Zahlungskartendaten erlitt.

Es gibt aber Methoden, mit denen der Schutz von Zahlungskartendaten verbessert werden kann. Für den PSR 2018 haben wir ca. 55 Unternehmen befragt und branchenübergreifend gaben 18 % an, kein offizielles Datenschutz- und Compliance-Programm (Data Protection and Compliance Program, DPCP) zu besitzen. Keines der Unternehmen mit einem DPCP bewertete den Reifegrad des Programms als „optimiert“. Das deutet darauf hin, dass bei der Entwicklung und Pflege eines ausgereiften PCI-DSS-Compliance-Programms durchaus Verbesserungsbedarf besteht. Mit einem solchen Programm lässt sich dann wiederum die Zahlungssicherheit verbessern.

18 % der Unternehmen aller Branchen haben kein offizielles Datenschutz- und Compliance-Programm (DPCP). Keines der Unternehmen mit einem DPCP bewertete den Reifegrad des Programms als „optimiert“.

Finanzdienstleister können sich beim Schutz von Zahlungskartendaten nicht auf vorhandene DPCP verlassen.

Positive Ergebnisse

Laut dem PSR 2019 schnitt der Finanzsektor bei der Einhaltung der folgenden PCI-DSS-Anforderungen besser als alle anderen Branchen ab:

- Wartung einer Firewall-Konfiguration (Anforderung 1)
- Änderung der Standardeinstellungen des Herstellers (Anforderung 2)
- Kontrolle des physischen Zugriffs (Anforderung 9)
- Sicherheitsmanagement (Anforderung 12)

Bei der Pflege der Firewalls haben sich die Finanzdienstleister sogar um 2,2 Prozentpunkte verbessert – ein Lichtblick angesichts des allgemeinen Abwärtstrends in allen Branchen. Die Finanzbranche wies in diesem Bereich auch die kleinste Kontrolllücke auf (7,3 %) und kam der vollständigen Compliance damit näher als alle anderen Branchen.

Sie war auch die einzige Branche, die beim Schutz gespeicherter Karteninhaberdaten (Anforderung 3) eine Verbesserung im Vergleich zum PSR 2018 erzielte. Zudem wurde in diesem Bereich die größte Reduzierung der Kontrolllücke erreicht (von 14,1 % auf 5,9 %).

Negative Ergebnisse

Eine der Hauptaufgaben der Finanzdienstleister ist die Übermittlung von Finanzdaten, aber bei der Datenverschlüsselung für die Übertragung (Anforderung 4) besteht durchaus Verbesserungsbedarf. In diesem Bereich verzeichnete das Finanzwesen den stärksten Compliance-Rückgang aller Branchen (17,1 Prozentpunkte).

Auch beim Schutz vor Malware (Anforderung 5) hapert es. Der Sektor erzielte die geringste Gesamt-Compliance (82,9 %) und wies die größte Kontrolllücke (8,5 %) aller untersuchten Branchen auf.

In Bezug auf die PCI-DSS-Anforderung zur Erkennung und Abwehr von Bedrohungen stehen die Finanzdienstleister an zweitletzter Stelle. Das lag zu einem großen Teil an Unzulänglichkeiten bei der konsistenten Verfolgung und Überwachung des Zugriffs (Anforderung 10) und bei der Rekonstruktion von Sicherheitsvorfällen mithilfe von Audit-Trails.

Interessante Ergebnisse

Im PSR 2019 stellen wir detailliertere Informationen zu Datenschutzverletzungen bereit. Diese Untersuchungsergebnisse stammen aus den PCI Forensic Investigations (PFIs) des VTRAC-Ermittlungsteams (Verizon Threat Research Advisory Center). Die Langzeittrends zeigen, dass 11,5 % der bestätigten Datenschutzverletzungen im Finanzwesen auftraten. Das Ergebnis ist zwar nicht katastrophal, aber die Branche könnte sich ein ehrgeizigeres Ziel setzen (zum Beispiel die 2,7 % der IT-Services).

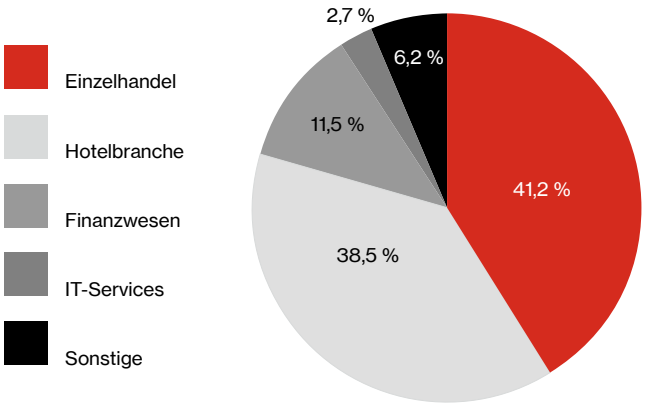


Abbildung 3: Bestätigte Datenschutzverletzungen nach Branche, Sechsjahrestrend, weltweite Verizon PFI-Einsätze 2010–2016

Empfehlungen

Bereiten Sie sich besser auf Vorfälle vor.

Sicherheitsvorfälle sind kaum vermeidbar, doch wie Sie darauf reagieren kann entscheidend sein. Ein zuverlässiger Notfallplan zahlt sich daher in jedem Fall aus. Es müssen auch die richtigen Audit-Trails verfügbar sein. Cybersicherheits- und Compliance-Experten können einem Unternehmen nur helfen, wenn sie die Ereignisse im Detail rekonstruieren können. Weitere Informationen zu den Vorteilen und zur richtigen Implementierung eines Notfallplans finden Sie im Verizon Incident Preparedness and Response (VIPR) Report.

Verbesserung der Sicherheit bei Mobilgeräten

Mobilgeräte kommen weltweit immer häufiger zum Einsatz und der Datenverkehr hat entsprechend stark zugenommen, auch das mobile Banking. Unternehmen sollten sich daher um effektive Sicherheitsmaßnahmen für die Geräte der Mitarbeiter bemühen, einschließlich der privaten Geräte, die die Mitarbeiter am Arbeitsplatz verwenden. Laut dem Verizon Mobile Security Index (MSI) 2019 gibt es in der Finanzbranche immer mehr Sicherheitsverletzungen in Zusammenhang mit Mobilgeräten. Für den Bericht 2018 hatten 25 % der Unternehmen einen Vorfall gemeldet, 2019 waren es schon 42 %.[1] Im aktuellen PSR und MSI informieren wir über die neuesten Bedrohungen und geben Tipps für den Datenschutz auf Mobilgeräten.

Entwicklung der Programmreife

Unternehmen verzichten nicht absichtlich auf gute Compliance-Programme. Die Entwicklung eines guten, ausgereiften Programms ist schwierig, aber mit den richtigen Leitfäden durchaus möglich.

Im PSR 2019 stellen wir das Verizon 9-5-4 Compliance Program Performance Evaluation Framework vor. Darin werden die Erkenntnisse aus früheren PSR und zusätzliche Tipps zusammengefasst, um Unternehmen einen Leitfaden zur Verbesserung des Compliance-Programms an die Hand zu geben. Das Framework ermöglicht eine größere Transparenz und Kontrolle, damit Unternehmen Wiederholbarkeit, Konsistenz und vorhersehbare Ergebnisse erzielen und PCI-DSS-Compliance gewährleisten können.

Abbildung 4: Relationales Modell der neun Faktoren der Kontrolleffektivität und -nachhaltigkeit

Vorreiterrolle

Die Finanzbranche ist bestrebt, die Finanzvorschriften einzuhalten und innovative Technologien zu nutzen. Die Betrugserkennung mithilfe von künstlicher Intelligenz ist nur ein Beispiel für einen Bereich, in dem viele Finanzdienstleister große Fortschritte gemacht haben. Jetzt ist es an der Zeit, diese Erfolge mit zuverlässigen und nachhaltigen PCI-DSS-Compliance-Programmen zu kombinieren. Eine bessere Zahlungssicherheit und PCI-DSS-Compliance können als wichtiges Alleinstellungsmerkmal dienen, das sich dann in einem größeren Kundenvertrauen bemerkbar macht.

Weitere Informationen:

Wenn Sie wissen möchten, wie Sie Ihre Sicherheitsmaßnahmen und Ihr Compliance-Programm verbessern können, besuchen Sie unsere Website unter enterprise.verizon.com/resources/reports/payment-security/ oder wenden Sie sich an Ihren Verizon-Ansprechpartner.

verizon✓

1 „Cybercriminals are banking on mobile devices being unsecured. Are you ready?“, Verizon Mobile Security Index 2019 – Financial services. https://enterprise.verizon.com/resources/reports/mobile-security-index/