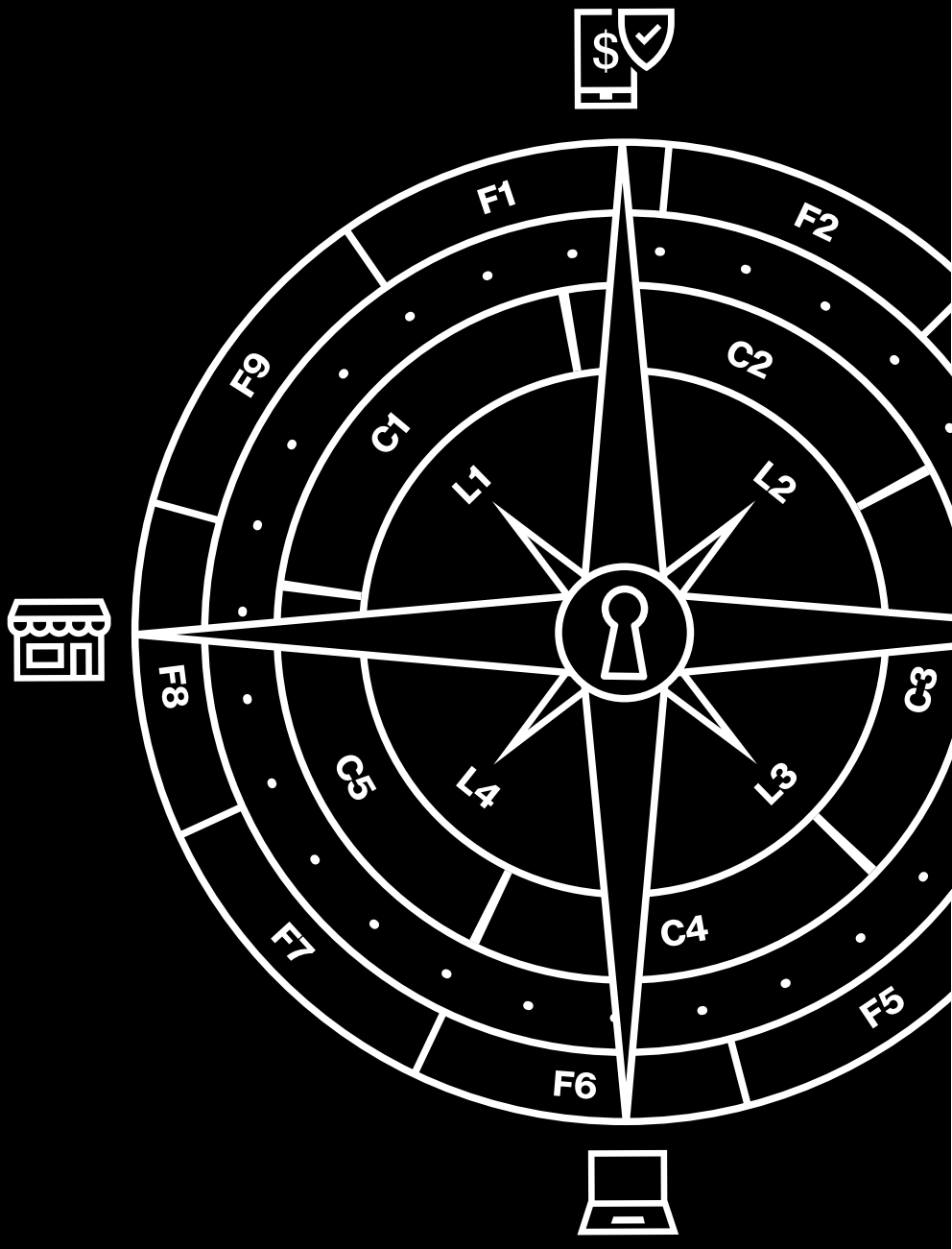
Payment Security Report 2019

Überblick über den Einzelhandel



verizon

Der Einzelhandelsmarkt ist hart umkämpft und Einzelhändler können nur bestehen, wenn sie die Wünsche ihrer Kunden erfüllen. Dabei spielt der Datenschutz eine immer größere Rolle.

Nur 7 % der Kunden würden nach einer Datenschutzverletzung weiterhin bei einem betroffenen Unternehmen einkaufen. 69 % der Kunden würden ein Unternehmen nach einer Datenschutzverletzung meiden, selbst wenn es bessere Preise als Mitbewerber anbieten würde.[1] Damit wird der Schutz von Zahlungskartendaten überlebenswichtig.

Wenn Einzelhändler konsistent für effektive Sicherheitsmaßnahmen sorgen und die Anforderungen des Payment Card Industry Data Security Standard (PCI DSS) erfüllen können, gewinnen sie das Vertrauen der Kunden und verschaffen sich damit einen Wettbewerbsvorteil. Dazu müssen sie jedoch ihre Datenschutz- und Compliance-Programme (Data Protection and Compliance Program, DPCP) weiterentwickeln.

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, beispielsweise dem Verizon 9-5-4 Compliance Program Performance Evaluation Framework, Datenschutz und Compliance verbessern lassen.

Trotz Chipkarten und PIN werden im Einzelhandel weiterhin Daten gestohlen.

Bis vor vier Jahren wurden Kartendaten vor allem an Kassensystemen abgegriffen.[2] Seither sind diese Betrugsverfahren zurückgegangen, vermutlich weil sie sich aufgrund der EMV-Technologie (Europay, Mastercard und Visa) nicht mehr lohnen. Stattdessen treten nun mehr Datendiebstähle in Webanwendungen auf.[3] Sicherheitsverletzungen sind nach wie vor ein Problem und Einzelhändler müssen wachsam bleiben.

Im PSR 2019 stellen wir detailliertere Informationen zu Datenschutzverletzungen bereit. Diese Untersuchungsergebnisse wurden zwischen 2016 und 2018 bei den PCI Forensic Investigations (PFIs) des VTRAC-Ermittlungsteams (Verizon Threat Research Advisory Center) erfasst. Daten zu Langzeittrends zeigen, dass im Einzelhandel ein größerer Teil der bestätigten Datenschutzverletzungen auftritt als in den anderen untersuchten Branchen (Hotel- und Gaststättengewerbe, Finanzdienstleister und IT-Services).

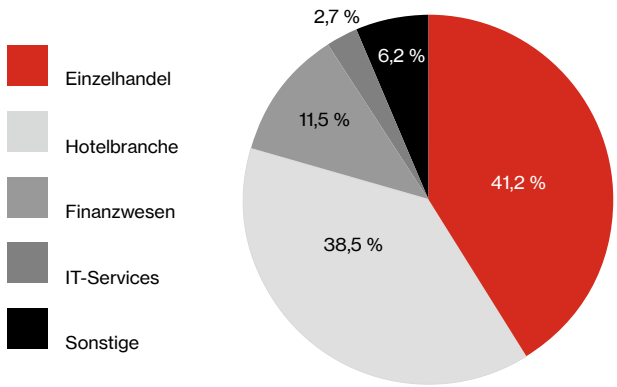


Abbildung 1: Bestätigte Datenschutzverletzungen nach Branche, Sechsjahrestrend, weltweite Verizon PFI-Einsätze 2010–2016

Laut unseren Daten sind vor allem Online-Händler von Datendiebstahl betroffen. Der Verizon Data Breach Investigations Report 2019 zeigt, dass Hacker den Einzelhandel vor allem aus finanziellen Motiven, zum Spaß und im Rahmen von Cyberspionagekampagnen angreifen. Unter anderem stehlen sie personenbezogene Daten aus Prämienprogrammen.

Der Schutz der Zahlungskarten ist entscheidend – aber nicht alle Unternehmen erreichen vollständige Compliance.

Es gibt aber Methoden, mit denen der Schutz der Zahlungskarten 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“.

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

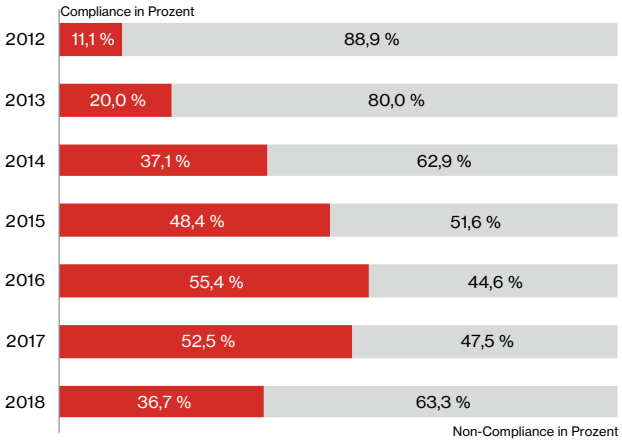


Abbildung 2: Vollständige Compliance nach Jahr

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.

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.

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: Die Kontrolllücke ist 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 leider nicht einmal ein Viertel aller Unternehmen (20,4 %).

Starker Rückgang der Compliance im Einzelhandel

Laut PSR 2019 verzeichneten alle Branchen einen Rückgang bei der vollständigen Compliance mit den PCI-DSS-Anforderungen. Im Einzelhandel lag sie 2017 bei 50,0 %, im vergangenen Jahr sogar bei 56,3 %, aber dieses Jahr nur noch bei 36,4 %.

Der Einzelhandel erreichte dieses Jahr eine ähnliche PCI-DSS-Compliance-Rate wie die IT-Services und lag damit vor dem Hotel- und Gaststättengewerbe (26,3 %), aber hinter den Finanzdienstleistern, die mit 39,0 % die Liste der untersuchten Branchen anführen.

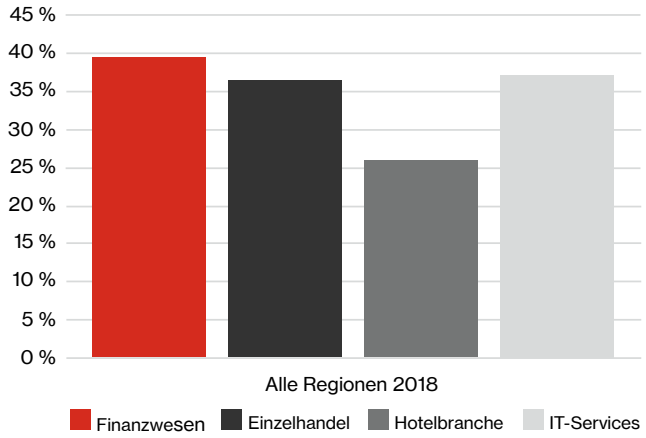


Abbildung 3: Weltweite Compliance nach Branche

Positive Ergebnisse

Laut PSR 2019 schnitt der Einzelhandel bei der Verschlüsselung der Daten bei der Übertragung (PCI-DSS-Anforderung 4) und dem Schutz vor Malware (Anforderung 5) gut ab. Die Branche konnte die Kontrolllücke in beiden Bereichen verringern und erreichte eine größere Compliance als die anderen Sektoren.

Auch bei der Authentifizierung des Zugriffs (Anforderung 8) zum Schutz vor Datendiebstahl erzielte der Einzelhandel gute Ergebnisse. Er konnte die Kontrolllücke reduzieren und erreichte zu 70,5 % vollständige Compliance. Damit lag er vor den Finanzdienstleistern und den IT-Services.

Eine weitere deutliche Verbesserung ist bei der Verfolgung und Überwachung des Datenzugriffs (Anforderung 10) zu erkennen. Der Einzelhandel erzielte in diesem Bereich die höchste Compliance (81,8 %) der vier untersuchten Branchen.

Negative Ergebnisse

Der Einzelhandel behielt in zu vielen relevanten Systemen und Anwendungen die Standardeinstellungen der Hersteller bei (Anforderung 2). Die Kontrolllücke war mit 12,4 % beträchtlich.

Auch beim zuverlässigen Sicherheitsmanagement (Anforderung 12) verzeichnete die Branche einen deutlichen Rückgang. Die Kontrolllücke wuchs im Vergleich zu dem Bericht aus dem Vorjahr um 18,2 Prozentpunkte auf 56,8 %.

Interessante Ergebnisse

Bei der Erkennung und Abwehr von Bedrohungen schnitt der Einzelhandel von allen untersuchten Branchen am schlechtesten ab. Zu den Problembereichen gehörten:

- Nutzeridentifizierung und Überprüfung ihrer Zugriffsrechte (Prüfverfahren 10.2.5)
- Nutzung eines geeigneten Prozesses für die Auswahl von Dienstanbietern (Prüfverfahren 12.8.3)
- Erkennung nicht autorisierter WLAN-Zugriffspunkte (Prüfverfahren 11.1.2)
- Pflege eines Notfallplans (Incident-Response-Plan, IR, Prüfverfahren 12.10)

Empfehlungen

Ändern Sie die Standardeinstellungen der Hersteller

Unternehmen, die die Standardpasswörter und -einstellungen der Anbieter ändern, sind besser vor Angriffen geschützt. Das sollte für alle Unternehmen höchste Priorität haben. Ein Pluspunkt: Die meisten Unternehmen haben Mitarbeiter, die über die erforderlichen Kenntnisse verfügen.

Investieren Sie in die Vorbereitung auf Vorfälle

Cyber-Sicherheitsvorfälle sind nahezu unvermeidbar, doch wie Sie darauf reagieren kann entscheidend sein. Wenn Einzelhändler potenzielle Sicherheitsprobleme identifizieren, zeitnah auf Vorfälle reagieren und eine Sicherheitsstrategie haben, können sie im Notfall schneller reagieren und den Schaden rascher beheben. Weitere Informationen zu den Vorteilen und zur richtigen Implementierung eines Notfallplans finden Sie im Verizon Incident Preparedness and Response (VIPR) Report.

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.

Verbessern Sie den Reifegrad Ihres Compliance-Programms

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 sowie Datenschutz und Compliance gewährleisten können.

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

Machen Sie die Zahlungssicherheit zum Teil Ihres Markenimages

Der Rückgang bei der PCI-DSS-Compliance im Einzelhandel sollte Sie nicht abschrecken, denn obwohl die Branche im PSR 2019 eher mittelmäßig abgeschnitten hat, gibt es durchaus richtlinienkonforme Einzelhändler. Wenn Sie ein ausgereiftes Compliance-Programm entwickeln, können Sie sich wie diese Branchenführer einen Wettbewerbsvorteil verschaffen und eine Marke aufbauen, der die Kunden vertrauen.

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 Die Daten stammen aus dem Verizon-Bericht „Wettbewerbsvorteile durch eine moderne CX: Risiken und Potenzial eines Kundenerlebnisses der nächsten Generation“ aus dem Jahr 2019, der auf einer Online-Umfrage unter 6.000 Teilnehmern in 15 Ländern sowie qualitativen Interviews mit CX-Fachleuten basiert. Die Untersuchung wurde von Longitude, einem Unternehmen der Financial Times Group, durchgeführt. https://enterprise.verizon.com/resources/reports/2019/winning_the_cx_war.pdf

2 Verizon Data Breach Investigations Report 2019 https://enterprise.verizon.com/resources/reports/dbir/

3 Ebd.