

# 2020 Payment Security Report

Informationsblatt

**In zu wenigen Unternehmen herrscht Klarheit darüber, warum bei der Datensicherheit und Compliance keine zuverlässigen Ergebnisse erzielt werden. Der Verizon 2020 Payment Security Report (PSR) – ein einzigartiger Forschungsbericht, der in diesem Jahr zum 10. Mal erscheint – untersucht die Herausforderungen, vor denen CISOs beim Konzipieren, Umsetzen und Pflegen einer effektiven und nachhaltigen, programmatischen Sicherheitsstrategie stehen.**

## Die Compliance geht weiter zurück.

Die Vorgaben des Payment Card Industry Data Security Standard (PCI DSS) werden immer öfter verletzt. Der 2020 PSR untersucht nicht nur, wie viele Unternehmen einmal im Jahr ihre Compliance nachweisen können, sondern vor allem auch, wie erfolgreich dieselben Standards über längere Zeit aufrechterhalten werden.

Warum beispielsweise werden technologische Lösungen bevorzugt implementiert, während der Verbesserung des Reifegrads von Fertigkeiten und Prozessen nicht genug Aufmerksamkeit gewidmet wird? Wie können Führungskräfte sich auf diese Situation einstellen und innovativ handeln, um ihre Sicherheitskultur weiterzuentwickeln und zu verbessern? Wir erläutern die größten Sicherheitsgefahren und stellen Vorgehensweisen vor, mit denen CISOs ihre Herausforderungen im Bereich Datensicherheits-Compliance schultern können. Wir untersuchen die wichtigsten Komponenten eines erfolgreichen Compliance-Programms, das auch in schwierigen Zeiten mit sich ändernden Umweltbedingungen seinen Zweck erfüllt.

**Die Hauptmotivation der Cyber-Kriminellen ist und bleibt die finanzielle Bereicherung; sie steckt hinter nahezu 9 von 10 (86 %) Datendiebstählen. Im Einzelhandel waren 99 % der Vorfälle finanziell motiviert. Dabei sind Zahlungsdaten nach wie vor die begehrteste und lukrativste Beute der Verbrecher. Inzwischen sind allerdings nicht mehr Point-of-Sale-Geräte (POS), sondern Web-Anwendungen der Hauptvektor für Angriffe auf diesen Sektor.<sup>1</sup>**

## Inhalte des 2020 PSR:

- Die nachlassende Compliance mit dem PCI DSS
- Warum CISOs oft nicht die Aufmerksamkeit der Unternehmensführung gewinnen können
- Die 7 schlimmsten Fällen beim strategischen Datensicherheitsmanagement
- Die 5 Komponenten einer leistungsstarken Datensicherheitsumgebung
- Der Referenzkalender für die PCI-DSS-Compliance

## Die wichtigsten Ergebnisse im Überblick

Viele Unternehmen scheitern bei der Durchsetzung von Datensicherheit und Compliance an fehlenden Ressourcen oder unzureichender Unterstützung durch die Führungsetage. In zu vielen Unternehmen sind die Datensicherheitsstrategien auch nicht an den Routinebetrieb und die Unternehmensstrategien angepasst.

CISOs bekommen zu geringe Budgets und zu wenig Personal und stehen daher ständig vor einem Berg drängender Alltagsprobleme. Das führt zu kurzfristigem Denken: Es muss schnell eine Technologie gegen das Problem her, aber sie kommen nie dazu, mit der Unternehmensführung strategische Pläne für langfristige Lösungen zu entwickeln. Das Scheitern dieser Notlösungen ist unvermeidlich, und viele CISOs suchen sich nach etwa zwei Jahren eine neue Position. Der neue CISO durchläuft dann oft denselben Kreislauf.

Das Ergebnis: die PCI-DSS-Compliance sinkt von Jahr zu Jahr. Der 2020 PSR deckt auf, dass nur 27,9 % der Unternehmen bei ihrer Zwischensvalidierung 2019 eine volle Compliance erreichten – 8,8 % weniger als 2018, als bereits ein Rückgang gegenüber 2017 um 5 Prozentpunkte verzeichnet wurde. Die Hauptmotivation der Cyber-Kriminellen ist und bleibt die finanzielle Bereicherung; sie steckt hinter nahezu 9 von 10 (86 %) Datendiebstählen. Im Einzelhandel waren 99 % der Vorfälle finanziell motiviert. Dabei sind Zahlungsdaten nach wie vor die begehrteste und lukrativste Beute der Verbrecher. Inzwischen sind allerdings nicht mehr Point-of-Sale-Geräte (POS), sondern Web-Anwendungen der Hauptvektor für Angriffe auf diesen Sektor.<sup>1</sup>

Der PSR untersucht Einzelheiten und Ursachen der Herausforderungen, vor denen CISOs stehen, und deren Auswirkungen auf den Verfall der Compliance. Der Bericht beschreibt zudem sieben „Fallstricke“ beim Datensicherheitsmanagement. Die aufgedeckten Probleme sind nicht technischer Natur, können also nicht durch den Erwerb neuer Tools, Apps oder Hardware gelöst werden. Es handelt sich vielmehr um organisatorische Probleme, deren Lösung ausgereifte Führungsqualitäten erfordert:

- Erstellung genau definierter Prozesse
- Aufbau eines Geschäftsmodells für die Sicherheit
- Definition einer soliden Sicherheitsstrategie, die durch Betriebsmodelle und ein Framework für die Sicherheit untermauert wird
- Entwicklung von Sicherheitsprogrammen und -projekten für den Ausbau von Kompetenzen und die Reifung von Prozessen

### Weitere Informationen:

Den vollständigen Verizon 2020 PSR (auf Englisch) finden Sie unter [verizon.com/paymentsecurityreport](https://www.verizon.com/paymentsecurityreport). Sie möchten sich genauer darüber informieren, wie Sie Ihr Compliance-Management oder Ihre Sicherheitsmaßnahmen beim Schutz von Zahlungskarten optimieren können? Dann kontaktieren Sie Ihren Business Account Manager bei Verizon oder schreiben Sie eine E-Mail an [paymentsecurity@verizon.com](mailto:paymentsecurity@verizon.com).

---

### So können wir Ihnen helfen

Unser QSA-Pool (Qualified Security Assessors) gehört – laut der Rangliste des PCI SSC (Payment Card Industry Security Standards Council) – zu den größten der Welt. Somit sind wir perfekt aufgestellt, um Kunden bei der Einhaltung der PCI-Compliance und der Reduzierung des Unternehmensrisikos durch einen konsistenten, praktischen Ansatz beim Schutz von Zahlungskarten unter die Arme zu greifen.

Wir haben:

- Unternehmen in 61 Ländern mit PCI-Services unterstützt.
- mehr als 180 Sicherheitsberater in 30 Ländern im Einsatz.
- seit 2009 über 18.000 Bewertungen durchgeführt.
- seit 1999 Sicherheits-Beratungsdienste und seit 2003 unsere PCI-Compliance-Dienste bereitgestellt.

