PCI-DSS Compliance auf dem Tiefstand

Von Gabriel Leperlier

Mehr als 15 Jahre nach der Einführung des PCI-DSS-Standards ist eine flächendeckende Umsetzung nicht nur nicht erreicht, sondern die Compliance-Quote ist auf einen neuen Tiefstand gefallen, sagt Gabriel Leperlier. Und für 2020 ist schon das vierte Update des Standards geplant. Lob hat der Autor am ehesten für die Finanzbranche. Die Gastronomie konnte sich als einzige Branche zumindest verbessern, am schlechtesten sieht es im Einzelhandel aus. PCI-DSS-Compliance lohnt sich jedoch. Denn wo der Standard umgesetzt wurde, gab es bisher noch keine Kompromittierung von Kartentaten. Red.

Bei Cyberattacken geht es den Angreifern häufig um die auf Zahlungskarten hinterlegten persönlichen und finanziellen Kundeninformationen. Der Payment Card Industry Data Security Standard (PCI DSS) soll dabei helfen, die Zahlungsdaten der Kunden ab dem Zeitpunkt des Kaufs zu schützen. Umso überraschender ist das Ergebnis einer Untersuchung von Verizon, die zeigt, dass immer weniger Unternehmen diesen Standard einhalten. Da für 2020 die Veröffentlichung des vierten Updates des PCI DSS-Standards geplant ist, sollten Unternehmen ihre Vorhaben zur Einhaltung der Vorschriften überdenken und neu strukturieren.

Als Visa 2004 den PCI DSS ins Leben rief, gingen viele Experten davon aus, dass Organisationen innerhalb von fünf Jahren eine effektive und nachhaltige Einhaltung der Vorschriften erreichen würden. Über 15 Jahre später ist die Zahl der Unternehmen, die tatsächlich diese Vorgaben einhalten, weltweit von 52,5 Prozent (PSR 2018) auf einen Tiefstand von 36,7 Prozent (PSR 2019) gesunken. Positiv entwickelt haben sich Unternehmen in der Region Asien-Pazifik (APAC), die zu 69,6 Prozent die Vorschriften vollständig einhalten. In Europa, dem Nahen Osten und Afrika (EMEA) gelang dies 48 Prozent, während es in Nord- und Südamerika nur 20,4 Prozent waren.

Industrien entwickeln sich unterschiedlich

Ein Blick auf zentrale Branchen zeigt, dass die Vorgaben ganz unterschiedlich eingehalten werden. Auch die Gründe für die Nichteinhaltung unterscheiden sich. Es sind daher branchenspezifische Maßnahmen notwendig, um eine bessere Compliance zu erreichen. Hier ein Blick auf den Einzelhandel, das Gastgewerbe und den Finanzsektor.

Im Einzelhandel wurden noch im Jahr 2015 Daten überwiegend am Verkaufspunkt kompromittiert. Seitdem in den USA aber Europay, Mastercard und Visa (EMV) neue Technologien eingeführt haben, scheint sich der Wert bei einem Kartenbetrug verringert zu haben. Die Untersuchungen zeigen, dass Daten-Kompromittierungen heute vor allem bei Web-Anwendungen auftreten. Jedoch konnten Sicherheitsverletzungen noch nicht vollständig beseitigt werden, weshalb Einzelhändler auch weiterhin beim Schutz von Kartendaten wachsam bleiben sollten. Die Compliance-Quote lag bei Einzelhandelsunternehmen bei 26,3 Prozent. Der gleiche Wert wurden bei Anbietern von IT-Dienstleistungen ermittelt.

Probleme bei der Einhaltung des PCI DSS entstanden durch die Verwendung von Default-Einstellungen der Hersteller und bei der Erfüllung von Anforderungen eines guten Sicherheitsmanagements. Dies spiegelt sich auch darin wider, dass der Einzelhandel die niedrigste Bewertung aller untersuchten Branchen bei der Vorbereitung auf Daten-Kompromittie-

Gabriel Leperlier, Senior Manager Security Consulting, Verizon EMEA, Marseille

rungen erhielt. Probleme bereiteten vor allem die Identifizierung von Nutzern, dass sie die jeweils passenden Zugangsberechtigungen haben, die mangelnde Sorgfalt bei der Beauftragung von Dienstleistern, dass sie nicht autorisierte drahtlose Zugangspunkte entdecken können und dass ein Plan zur Reaktion auf Vorfälle (Incident Response Plan) gepflegt wird.

Gastgewerbe als einzige Branche verbessert

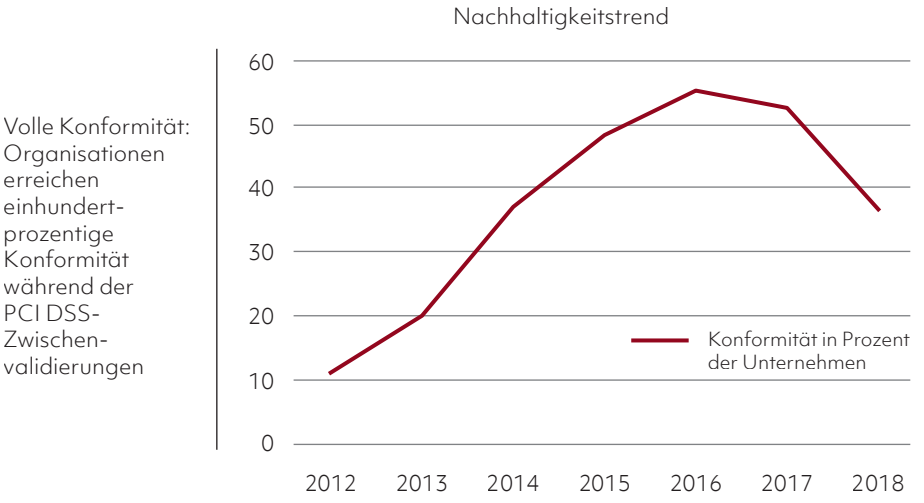
Obwohl das Gastgewerbe immer noch die niedrigste Wertung für die Verschlüsselung von Daten bei der Übertragung hatte, war es die einzige Branche, die sich in dieser Kategorie im Vergleich zum Vorjahr steigern konnte. Die Unternehmen aus dem Gastgewerbe haben sich außerdem beim Schutz vor Malware mehr als alle anderen Branchen verbessert und ihre Konformität auf 84,2 Prozent erhöht.

Das Gastgewerbe war auch der einzige Sektor innerhalb des PSR 2019, der seine Fähigkeiten zur Kontrolle des physischen Zugangs im Vergleich zum Vorjahr verbessern konnte, wodurch sich die Compliance-Rate auf 63,2 Prozent erhöhte. Zwar blieb das Gastgewerbe beim Schutz der gespeicherten Karteninhaberdaten hinter anderen Branchen zurück, aber es steht hierbei auch vor einzigartigen Herausforderungen, einschließlich fehlender ausgereifter Lösungen für Gastgewerbeumgebungen. Die Branche hatte am meisten zu kämpfen mit der Benutzeridentifikation und -authentifizierung, der Überprüfung und dem Testen des Reaktionsplans für Vorfälle sowie der Schulung zu den Verantwortlichkeiten bei Verstößen.

Finanzbranche mit Luft nach oben

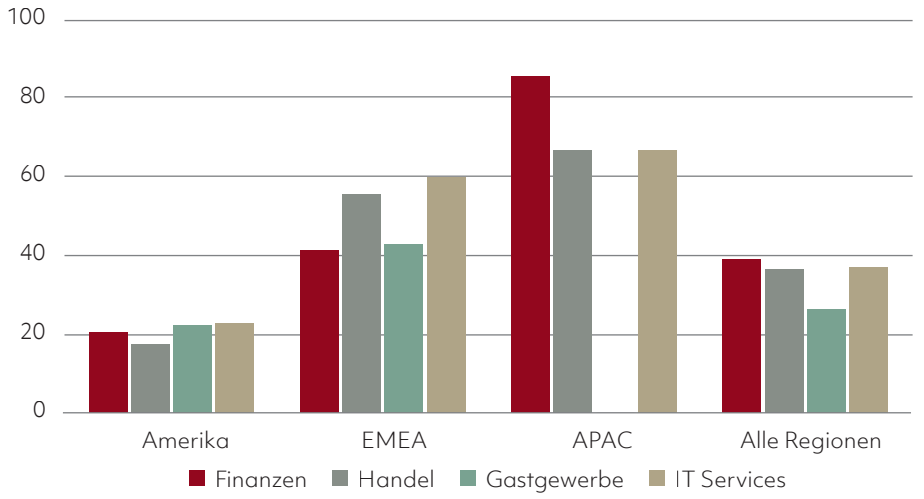
Finanzdienstleiser operieren in einem sich ständig veränderten Markt. Ihre Kunden verlange neue Wege, um personalisierte Transaktionen zu tätigen – insbesondere über ihre mobilen Geräte. Auch gibt es immer neue Anbieter aus anderen Branchen, die Finanzprodukte anbieten. In diesem wettbewerbsorientierten und stark regulierten Umfeld kann die Fähigkeit, Daten von Zahlungskarten effektiv zu schützen, ein entscheidendes Unter-

Abbildung 1: PCI DSS Interims-Validation-Compliance-Trend von 2012 bis 2018



Quelle: 6 Year Trend Verizon PFI global caseload 2010 - 2016

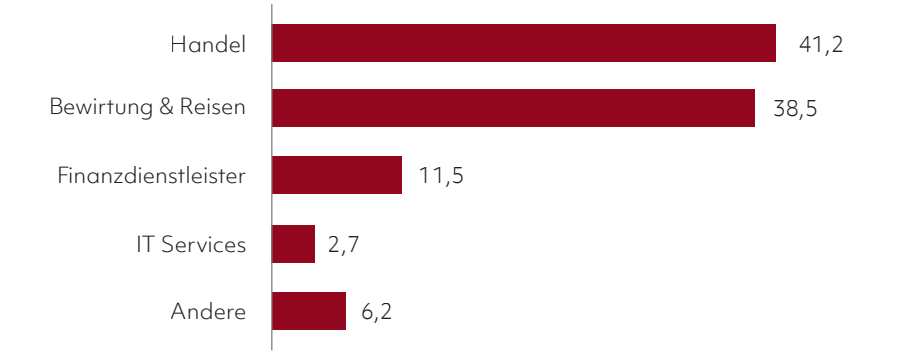
Abbildung 2: Globale PCI DSS Compliance für vier Branchen



in Prozent

Quelle: 6 Year Trend Verizon PFI global caseload 2010 - 2016

Abbildung 3: Bestätigte globale Datenverletzungen mit Zahlungskarten



in Prozent, 6-Jahres-Trend für Fälle 2010- bis 2016

Quelle: 6 Year Trend Verizon PFI global caseload 2010-2016

scheidungsmerkmal sein. Die Kunden erwarten, dass Finanzdienstleister die Notwendigkeit von Zahlungssicherheit besser verstehen als andere Unternehmen. Diese Erwartung wird mit den Daten aus dem PSR 2019 belegt: Der Finanzsektor hat die Anforderungen des PCI DSS besser als jede andere Branche erfüllt. Jedoch gibt es auch hier noch Verbesserungspotenzial, beispielsweise bei der Verschlüsselung von Daten während der Übertragung und beim Schutz vor Malware.

Bei der Implementierung von Schutzmaßnahmen ist ein erster Schritt eine detaillierte Analyse der vorhandenen Fähigkeiten zur Abwehr von Cyberangriffen sowie der vorhandenen Prozesse.

Neues Framework hilft bei der Zahlungssicherheit

Organisationen investieren viel Zeit und Geld in Initiativen zur Einhaltung von Datenschutzbestimmungen. Allerdings sind diese Programme oft wirkungslos – sie sehen zwar auf dem Papier gut aus, sind aber nicht in der Lage, einer professionellen Sicherheitsanalyse standzuhalten. Chief Information Security Officers konzentrieren sich immer noch auf die Einhaltung grundlegender Kontrollaktivitäten, anstatt auf die Kompetenzen und den Entwicklungsstand beim Datenschutz zu achten. Sie benötigen daher einen klaren und leicht verständlichen Leitfaden, der ihnen hilft, messbare Ergebnisse und vorhersehbare Resultate zu erzielen.

In der Praxis sind Datenschutz und Compliance alltägliche Herausforderungen. Unternehmen glauben daher, dass sie mit einem universellen Ansatz effektiven und nachhaltigen Datenschutz erreichen können. In der Realität ist die Frage der Sicherheit jedoch komplizierter.

In früheren Payments Security Reports hat Verizon Methoden dargestellt, die Unternehmen bei der Verwaltung ihrer Data Protection Compliance Programme (DPCPs) helfen. Diese wurden nun zum Verizon 9-5-4 Compliance Program Performance Framework zusammengeführt – einem Leitfaden, der Organisationen bei der Entwicklung und Verbesserung ihrer Fähigkeiten und der Prozessreife unterstützt.

Für viele noch ein langer Weg

Das 9-5-4 Framework hilft Organisationen dabei, reproduzierbare, konsistente und vorhersehbare Ergebnisse zu erzielen. Dafür bietet das Verfahren eine Anleitung, um neun Faktoren für Kontrolleffizienz und Nachhaltigkeit abzubilden und zu überwachen. Dazu zählen Control Environment, Control Design, Control Risk, Control Robustness, Control Resilience, Control Lifecycle Management, Performance Management und Maturity Measurement sowie eine Selbstbewertung.

Aus den Ergebnissen des aktuellen PSR geht hervor, dass viele Organisationen noch einen weiten Weg vor sich haben, wollen sie eine vollständige Compliance erreichen. Mit Einsatz der richtigen Werkzeuge und Initiativen ist dies aber möglich. Der Schlüssel hierbei ist Compliance bei der Zahlungssicherheit. Die Daten des Verizon Threat Research Advisory Center (VTRAC) zeigen zudem, dass eine Compliance-Initiative ohne die richtigen Kontrollen zum Schutz von Daten mit einer Wahrscheinlichkeit von über 95 Prozent nicht nachhaltig ist und dass eine Organisation daher eher Ziel eines Cyberangriffs wird.

Compliance bietet Sicherheit

Schon seit Jahren diskutiert Verizon über den engen Zusammenhang zwischen der mangelhaften Einhaltung des PCI DSS-Standards und Cyber-Kompromittierungen. Wer PCI DSS erfolgreich umsetzt, wurde offenbar auch noch nicht Opfer einer Kompromittierung von Zahlungskartendaten – es sind zumindest keine öffentlichen Berichte über erfolgreiche Cyberangriffe verfügbar. Dies zeigt, dass Compliance in der Praxis tatsächlich wirkungsvoll ist. ■

Zehn Fragen zum Reifegrad von Data-Protection-Compliance-Initiativen

Transparenz, Kontrolle und Vorhersehbarkeit sind wichtige Faktoren für ein erfolgreiches Compliance-Management. Um den Reifegrad von Data-Protection-Compliance-Initiativen voranzubringen, sollten sich Verantwortliche die folgenden zehn Fragen stellen.

1. Welche Daten liegen vor, wo sind sie gespeichert und wie fließen sie durch die Organisation?

2. Sind die Daten sicher genug?

3. Wie hoch ist das Vertrauen, dass die richtigen Kontrollen wirksam und an den richtigen Stellen durchgeführt werden?

4. Wie vorhersehbar sind Durchführung und Einhaltung von Data-Protection-Compliance-Initiativen?

5. Wie werden die Qualität und Nachhaltigkeit der wichtigsten Datenschutz- und Compliance-Prozesse sichergestellt? Ist bekannt, aus welchen Elementen diese Prozesse bestehen?

6. Wie schnell können Abweichungen von Richtlinien, Standards und Verfahren erkannt und darauf reagiert werden?

7. Gibt es Kontrollen, um die Wirksamkeit und den Reifegrad von Data-Protection-Compliance-Initiativen zu messen?

8. Woraus lässt sich schließen, dass die passenden Aktivitäten zur Datensicherheit zur richtigen Zeit priorisiert werden?

9. Wie werden die fünf Einschränkungen der organisatorischen Leistungsfähigkeit gesteuert: Kapazität, Fähigkeit, Kompetenz, Engagement und Kommunikation?

10. Wie gut ist das Verständnis der neun Faktoren der Steuerungseffektivität und Nachhaltigkeit? Auf welche Zielreifegrade soll auf lange Sicht hin gearbeitet werden?