Die **Compliance** für Zahlungssicherheit lässt nach

Von Gabriel Leperlier

Quelle: pixabay

Die Einhaltung des PCI-DSS-Standards zum Schutz von Zahlungsdaten ist wieder rückläufig. Nur noch 46,4 Prozent der Unternehmen in Europa können eine vollständige Compliance aufrechterhalten, so das Ergebnis des Verizon Payment Security Report 2018. Das liegt daran, dass PCI-DSS-Compliance kein einmaliges Projekt, sondern ein fortlaufendes Verfahren ist, das sich Veränderungen im Unternehmen und an neue Technologien anpassen muss. Es braucht deshalb klare Kontrollstrukturen. Red.

Verbraucher und Dienstleister verlassen sich darauf, dass Unternehmen ihre Zahlungsdaten effektiv schützen. Untersuchungen zeigen jedoch, dass die Einhaltung des Payment Card Industry Data Security Standard (PCI DSS), dem Standard zum Schutz dieser Daten, rückläufig ist.

In den Jahren 2010 bis 2016 dokumentierte der Verizon Payment Security Report (PSR) eine Verbesserung bei der Einhaltung des Payment Card Industry Data Security Standards (PCI DSS). In der aktuellen Ausgabe zeigt sich dagegen ein Abwärtstrend: Mehr Unternehmen als zuvor halten die Compliance-Bewertungen nicht vollständig oder gar nicht ein. Dieser Trend ist alarmierend, denn PCI DSS unterstützt dabei, die Kartenzahlungssysteme vor Datenverletzungen und dem Diebstahl von Inhaberdaten zu schützen.

Regionale Unterschiede

Daten aus dem Jahr 2017, die von den Verizon PCI DSS Qualified Security Assessors (QSAs) erhoben wurden, zeigen, dass die PCI-Compliance bei global tätigen Unternehmen abnimmt: Nur 52,4 Prozent konnten 2017 eine vollständige Compliance aufrechterhalten, 2016 waren es noch 55,4 Prozent.

Dabei gab es deutliche regionale Unterschiede: Mit 77,8 Prozent ist bei Unternehmen in der Asien-Pazifikregion vollständige Compliance eher wahrscheinlich als in Europa (46,4 Prozent) oder Nord- und Südamerika (39,7 Prozent). Die Unterschiede sind auf das Timing geografischer Compliance-Rollout-Strategien, kulturelle Wertschätzung von Auszeichnungen und Anerkennungen sowie auf die Ausgereiftheit von IT-Systemen zurückzuführen. Wird beispielsweise ein Compliance-Projekt in einer Region gestartet und dann weltweit ausgerollt, profitieren andere Regionen von den dort zuvor gewonnenen Erkenntnissen.

Zum Autor

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

Keine Branche ist wie die andere, und das gilt auch für die Einhaltung der Zahlungssicherheit in unterschiedlichen Industrien. Eine erfolgreiche Compliance-Strategie passt nicht automatisch für alle anderen Industrien, da verschiedene Branchen unterschiedliche Risiken haben, die mit ihren spezifischen Aktivitäten verbunden sind.

Erhebliche Lücken zwischen den Geschäftsbereichen

Nach Geschäftsfeldern gegliedert, stehen Unternehmen für IT-Services weiterhin an erster Stelle, wenn es um Compliance geht, wobei über drei Viertel der Unternehmen (77,8 Prozent) den sogenannten Vollstatus erreichen. Einzelhandel (56,3 Prozent) und Finanzdienstleistungen (47,9 Prozent) lagen deutlich vor dem Hotel- und Gaststättengewerbe (38,5 Prozent), das die geringste Compliance-Nachhaltigkeit aufwies.

Da Unternehmen oft PCI-DSS-Compliance-Projekte starten, um die Sicherheitsanforderungen von Datenschutzbestimmungen wie der Europäischen Datenschutzverordnung (DSGVO) zu erfüllen, ist diese Lücke zwischen den verschiedenen Geschäftsbereichen, die täglich mit elektronischen Zahlungen zu tun haben, erheblich.

Während einige Unternehmen die gesamte Norm einhalten müssen, um PCI DSS-zertifiziert zu werden, müssen sich die Einzelhandelsgeschäfte speziell auf die Sicherheit ihrer Zahlungsterminals konzentrieren. Im E-Commerce dagegen sollten sich die Maßnahmen auf alle internen und externen Scans im Zusammenhang mit dem Webserver konzentrieren. Weiterhin auf das „Hardening", also das Absichern von Komponenten, sowie auf „Key Management for Databases". Schließlich müssen Financial Services in allen Bereichen des Standards eine gute Bewertung erhalten. Dieser Sektor steht häufig vor Herausforderungen, wenn es um die Einhaltung der Vorgaben bei Kapitel 6 „Entwickeln und Pflegen sicherer Systeme" und Kapitel 2 „Verwenden Sie keine vom Hersteller gelieferten Standardeinstellungen" geht.

Es fehlt an Compliance-Strukturen

Im Laufe der Jahre hat sich gezeigt, dass es vielen Organisation schwerfällt, die Compliance einzuhalten. Wenn spezialisierte PCI-Compliance-Projektleiter während des Projektes das Team verlassen, geht das Wissen um den Compliance-Status eines Unternehmens verloren. Häufig fehlt auch eine klare Struktur zur Aufrechterhaltung der Compliance oder es erhalten nicht ausreichend qualifizierte Mitarbeiter die Verantwortung.

Neun Faktoren können Unternehmen dabei unterstützen, ihr Compliance-Level aufrechtzuerhalten. Ziel ist es, eine klare Struktur und Methodik bereitzustellen, um den Compliance-Mitarbeitern einerseits zu helfen, sie andererseits aber auch in die Lage zu versetzen, den Compliance-Dialog mit ihrem Management zu eröffnen und die Erläuterung einfacher nachvollziehbar zu halten.

1. Kontrollumgebung: Nachhaltigkeit und Wirksamkeit der zwölf Kernanforderungen sind von einer funktionierenden Kontrollumgebung abhängig.

2. Kontrollaufbau: Ein ordnungsgemäßer Kontrollbetrieb zur Erfüllung der DSS-Sicherheitskontrollziele benötigt einen durchdachten Kontrollaufbau.

3. Kontrollrisiko: Ohne kontinuierliche Wartung und Pflege (Sicherheitstests, Risikomanagement) können Kontrollen mit der Zeit an Wirksamkeit verlieren und schließlich ausfallen. Um das Ausfallen von Kontrollen zu minimieren, ist ein integriertes Management des Kontrollrisikos erforderlich.

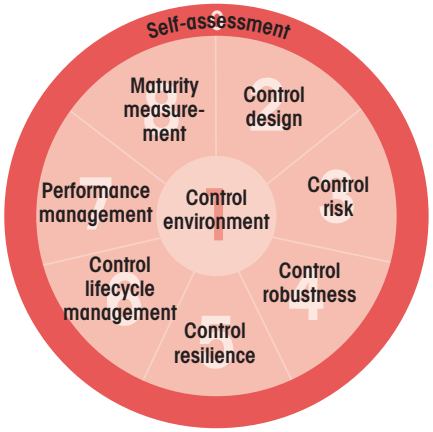
4. Kontrollrobustheit: Kontrollen finden in einem dynamischen Geschäfts- sowie sich permanent ändernden Bedrohungsumfeld statt. Sie müssen robust sein, um unerwünschten Veränderungen standhalten zu können, damit sie funktionsfähig bleiben und gemäß ihren Spezifikationen arbeiten, zum Beispiel bei Konfigurierungsstandards, Zugangskontrolle und System-Hardening.

5. Widerstandsfähigkeit von Kontrollen: Sicherheitskontrollen können immer wieder versagen, auch wenn man zur Erhöhung der Robustheit zusätzliche Kontroll-Layer hinzufügt. Daher ist im Sinne von Wirksamkeit und Nachhaltigkeit Widerstandsfähigkeit der Kontrollen durch proaktives Erkennen und rasche Wiederherstellung nach einem Ausfall unverzichtbar.

6. Lifecycle-Management von Kontrollen: Um all das zu erreichen, sollten Unternehmen Sicherheitskontrollen in jedem Stadium ihres Lebenszyklus von ihrer Einrichtung bis zur Außerbetriebnahme überwachen und aktiv managen.

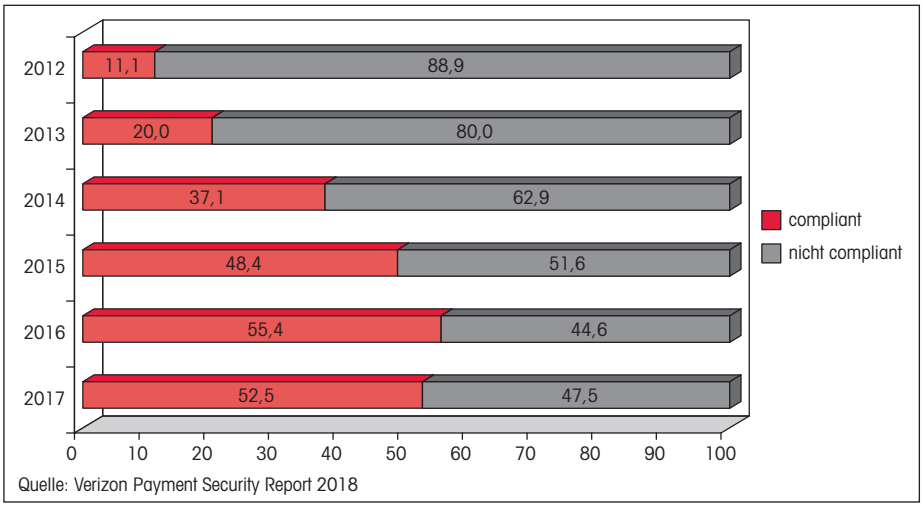
7. Performance-Management: Die Wirksamkeit von Kontrollen lässt sich verbessern, wenn Standards zur Messung der tatsächlichen Performance des Kontrollumfeldes definiert und kommuniziert werden. Dies trägt zu prognostizierbaren Ergebnissen der Datenschutz- und Compliance-Aktivitäten bei. Dadurch sind die

Abbildung 2: Neun Faktoren zur Aufrechterhaltung der Compliance



Quelle: Verizon

Abbildung 1: PCI-DSS-Compliance von Unternehmen 2012 bis 2017 (Angaben in Prozent)



Quelle: Verizon Payment Security Report 2018

frühzeitige Identifizierung und Behebung von Performance-Abweichungen möglich.

8. Reifegradmessung: Eine Kontrollumgebung sollte niemals stagnieren – sie muss sich kontinuierlich verbessern. Dazu benötigen Unternehmen eine Roadmap, einen Zielwert für die Prozess- und Kompetenzreife, um den Grad der Formvorschriften und die Optimierung von Prozessen zu verfolgen und so zu zeigen, wie nah die Entwicklungsprozesse am Ende sind und sich kontinuierlich verbessern können.

9. Selbstbeurteilung: Zur Erfüllung all dessen sind entsprechende Inhouse-Kapazitäten gefordert: Ressourcen (Personal, Prozesse, Technologie), Fähigkeiten (unterstützende Prozesse), Kompetenzen (Fertigkeiten, Wissen, Erfahrung) sowie Engagement (der Wille, Compliance-Anforderungen durchgängig einzuhalten) – kurz gesagt, Selbstbeurteilungsvermögen.

Verfahren fortlaufend anpassen

Das Bestehen der PCI-Konformitätsprüfung bedeutet nicht, dass die Systeme tatsächlich als sicher gelten. Vielmehr wird gezeigt, dass es während des Bewertungszeitraums, in der Regel ein oder zwei Wochen, keine Anzeichen von Verstößen gab. Weiterhin ist zu beachten, dass die Einhaltung des PCI-DSS-Standards kein einmaliges Projekt ist, sondern ein fortlaufendes Verfahren, das sich an die sich ändernden Bedürfnisse der Unternehmen und an neue Technologien anpassen muss.

Darüber hinaus sollten wirkungsvolle Compliance-Prozesse von oben angestoßen werden. Häufig werden jedoch Fortschritte oder Herausforderungen nicht klar an die Führungsebene kommuniziert oder von den leitenden Managern nicht verstanden. Durch die Strukturierung des Compliance-Prozesses und in Gesprächen zu den neun Faktoren der Kontrolleffektivität können Führungskräfte ein besseres Verständnis des Prozesses erlangen und klarer kommunizieren.