PCI DSS: **Compliance** hilft gegen **Cyberangriffe**

Von Gabriel Leperlier

PCI-DSS-Compliance ist kein Selbstzweck, so Gabriel Leperlier. Sondern die Einhaltung der Vorgaben hilft effektiv dabei, sich gegen Cyberangriffe zu wehren. Das setzt freilich voraus, dass PCI DSS nicht als einmaliges Projekt, sondern als laufender Prozess verstanden wird. Und daran fehlt es häufig noch. Die Kontrolllücken werden sogar größer. Mangelnde Compliance bei PCI DSS kann auch mit Problemen bei der General Data Protection Regulation zusammenhängen. Das kann dann richtig teuer werden. Red.

Die Anzahl der Cyberangriffe steigt weltweit – umso mehr rückt die Sicherheit von Zahlungskarten für Unternehmen und Verbraucher gleichermaßen in den Fokus. Der Payment Card Industry Data Security Standard (PCI DSS) unterstützt Unternehmen, die Kartenzahlungen nutzen, dabei, ihre Zahlungssysteme vor Missbrauch und Diebstahl von Karteninhaberinformationen zu schützen. Dennoch nehmen einige Organisationen eine langfristige Compliance auf die leichte Schulter und achten nicht darauf, kontinuierlich die nötigen Standards einzuhalten.

Die aktuellen Ergebnisse des Verizon 2017 Payment Security Report (2017 PSR) zeigen, dass es eine deutliche Verbindung zwischen der Einhaltung von Standards und der Fähigkeit, sich gegen Cyberangriffe zu wehren, gibt. Bei allen Datenmissbräuchen im Kontext mit Zahlungskarten, die untersucht wurden, war kein einziges Unternehmen zum Zeitpunkt des Vorfalls vollständig konform und erfüllte weniger als zehn der zwölf wichtigsten vorgegebenen PCI-DSS-Anforderungen. Die Auswirkungen eines Datenmissbrauchs sind signifikant und wirken sich nicht nur finanziell auf den Umsatz aus, sondern auch auf die Reputation der Marke und die Kundenloyalität.

PCI-DSS-Compliance erreichen und halten

Dazu werden die Sanktionen gegen Unternehmen, die sich nicht ausreichend schützen, strenger und viele Unternehmen, die in der EU operieren, unterstehen in Kürze der neuen General Data Protection Regulation (GDPR). Der Report zeigt zudem, dass die PCI-DSS-Compliance sich weltweit insgesamt verbessert hat: 55,4 Prozent der befragten Unternehmen bestanden 2016 ihre Interimsbewertung, 2015 waren es nur 48,4 Prozent.

Zum Autor

Gabriel Leperlier, Head of Continental Europe Security Assurance GRC/PCI, Verizon Enterprise Solutions, Marseille

Dennoch müssen Unternehmen beim PCI DSS nicht nur 100 Prozent Compliance erreichen, sondern dieses Ergebnis auch halten, das heißt alle anwendbaren Sicherheitskontrollen müssen kontinuierlich eingesetzt werden. Fast die Hälfte der Unternehmen, die die Validierung bestehen (44,6 Prozent), sind jedoch nach einem Jahr meist bereits nicht mehr konform – viele sogar schon früher.

Vorbild IT-Branche

Laut Report schnitt die IT-Service-Branche von allen untersuchten Schlüsselbranchen am besten ab. Global erreichten drei Fünftel (61,3 Prozent) der IT-Service-Unternehmen in der Bewertung 2016 eine vollständige Compliance, gefolgt von Finanzdienstleistungsunternehmen (59,1 Prozent – umfasst auch Versicherungen), Retail (50 Prozent) und dem Gastgewerbe (42,9 Prozent).

Die Compliance-Herausforderungen variieren je nach Branche, zum Beispiel:

- Einzelhandel: Sicherheitstests, verschlüsselte Datenübertragung und Authentifizierung;
- Hotels und Gaststätten sowie Reisen: Stärkung der Sicherheit, Schutz von Daten bei der Übertragung sowie physische Sicherheit;

- Finanzdienstleistungen: Sicherheitsprozeduren, sichere Konfigurationen, Schutz von Daten bei der Übertragung, Schwachstellen-Management sowie übergreifendes Risikomanagement.

„Kontrolllücken" beachten

Ein Blick auf die PCI-Kontrollmechanismen, die in Unternehmen eigentlich vorhanden sein sollten (etwa Sicherheits-Checks, Penetrationstests), offenbart dem Report zufolge, dass es eine zunehmend größere Kontrolllücke gibt. Mit anderen Worten: Zahlreiche dieser grundlegenden Dinge waren schlicht nicht vorhanden.

Effektive Kontrollen erfordern Verfahren, die ein Verständnis für Gefährdungspotenzial fördern und Kontrollen einführen, um ebendiese Risiken zu adressieren sowie die Datenschutzziele des Karteninhabers verfolgen. Diese umfassen effektive und effiziente Prozesse, zuverlässigen Datenschutz und Compliance bezüglich Richtlinien, Vorschriften und gültigen Gesetzen. 2015 fehlten bei Unternehmen, die bei der Interimsprüfung durchfielen, durchschnittlich 12,4 Prozent der Kontrollen; 2016 sind es 13 Prozent.

Konzepte für das Control-Lifecycle-Management

Viele Unternehmen betrachten PCI-DSS-Kontrollvorgaben nach wie vor isoliert und nicht als Teil des Großen und Ganzen – häufig fehlt ein Konzept für das Control-Lifecycle-Management. Dies ist meist auf einen Mangel an qualifizierten Fachkräften in der eigenen Organisation zurückzuführen. Oft wird ein Projekt gestartet, die Compliance erreicht und dann einfach nicht beibehalten, da Mitarbeiter mit dem nötigen Wissen das Unternehmen verlassen. Die Compliance sinkt und das Programm muss von neuem gestartet werden. Oder unqualifizierte Mitarbeiter werden damit beauftragt, die Compliance des PCI-Standards aufrechtzuerhalten. Diese haben dann aber oftmals nicht das Wissen, um dieses Ziel tatsächlich zu erreichen.

Die interne Kompetenz kann drastisch verbessert werden durch eine externe Anleitung, die den kompletten Lifecycle umfasst, sowie durch kontinuierliche Trainings.

Sicherheitskontrollen kontinuierlich hoch halten

Sicherheit kann nur über wirksame Kontrollen erreicht werden. Dabei muss durchgehend überprüft werden, dass sie zu jeder Zeit effektiv arbeiten – und natürlich müssen sie direkt angepasst werden, falls dies nicht der Fall ist. Diese Organisationen setzen zusätzliche Kontrollen (über die PCI DSS hinaus) ein, um eine widerstandsfähige und nachhaltige Kontrollumgebung zu schaffen, die auch künftigen Risiken standhält.

Sicherheitskontrollen kontinuierlich hoch zu halten, ist eine große Herausforderung. Unternehmen sind ständig im Wandel und so können bestehende Sicherheitskontrollen schnell an ihre Grenzen stoßen oder nicht mehr zweckmäßig sein.

Wie können Unternehmen Sicherheitskontrollen etablieren, diesen Herausforderungen standhalten? Folgende Punkte sind zu beachten:

- Nachhaltigkeit und Belastbarkeit in den Fokus der Compliance-Bestrebungen stellen: Organisationen, die sich auf die langfristige Wirksamkeit ihrer Sicherheitskontrollen konzentrieren, haben einen wichtigen Vorteil gegenüber denen, die sich ausschließlich auf die Einhaltung von Vorschriften wie PCI DSS, Health Insurance Portability und Accountability Act von 1996 (HIPAA) konzentrieren.

- Sicherheitskontrollen in alltägliche Verfahren integrieren: Wenn Kontrollen nicht ressourceneffizient und budgetfreundlich sind, sollten sie nicht fortgeführt werden.

- Flexibel bleiben: Unternehmen ändern sich ständig, ebenso wie die Bedrohungen, denen sie gegenüberstehen. Unternehmen sollten in regelmäßigen Abständen die Wirksamkeit der Kontrollen kontrollieren, um schnell reagieren und Anforderungen ändern zu können.

Mitarbeiter vom ersten Tag an einbeziehen: Compliance sollte bereits bei der Einarbeitung der Mitarbeiter im Fokus stehen. Wichtig ist, dass jeder genau versteht, was von ihm erwartet wird.

Passwortrichtlinien überprüfen: Unternehmen sollten einen formalen Passwort-Prozess entwickeln, sodass Anmeldeinformationen organisationsübergreifend stark sind. Zudem sollte ein System installiert werden, das Passwörter regelmäßig überprüft.

PCI DSS und GDPR Compliance in wichtiger Beziehung

Wenn ein Unternehmen damit kämpft, PCI DSS einzuhalten, könnte dies auch ein Indikator dafür sein, dass es Schwierigkeiten haben könnte, die Compliance zur General Data Protection Regulation GDPR zu bewahren. Dies wäre keine Kleinigkeit: So liegen die Höchststrafen für die Verletzung des GDPR immerhin bei satten 20 Millionen Euro und 4 Prozent des weltweiten Umsatzes.

Sowohl PCI DSS als auch GDPR fokussieren sich darauf, wie Unternehmen ihre Kundendaten zu sichern haben – dies allerdings mit jeweils unterschiedlichen Ansätzen. Das GDPR ist viel breiter angelegt als das PCI DSS. Es deckt weitaus mehr Arten von Daten ab und definiert gleichzeitig die Rechte des Einzelnen; beispielsweise das Löschungsrecht, das Einzelpersonen erlaubt, die Löschung ihrer persönlichen Daten zu verlangen. Wie

genau Unternehmen diese Vorgaben einhalten sollen, legt es hingegen nicht dar.

Hier kann das PCI DSS als vorgeschriebener Standard helfen. Während dieser vordergründig zwar vor allem für Daten aus dem Zahlungsverkehr gilt, lassen sich dessen Grundsätze auch auf andere Datentypen übertragen. In den 13 Jahren, die dieser Standard mittlerweile besteht, konnte dieser in puncto Detailliertheit deutlich weiterentwickelt werden, sodass er nun tatsächlich fundierte Orientierung liefert – nicht nur hinsichtlich der Art der Sicherheitskontrollen, die ein Unternehmen implementiert haben sollte, sondern auch, wie diese sich pflegen lassen.

So lässt das Informationskommissariat verlauten: „Im Rahmen des GDPR sind Sie allgemein dazu verpflichtet, technische und organisatorische Maßnahmen zu implementieren, die zeigen, dass Sie den Schutz von Daten in Ihre Prozesse eingebettet und integriert haben."

Unternehmen mit effektiven PCI-DSS-Compliance-Programmen stellen sicher, dass grundlegende Sicherheitsprinzipien auf den Schutz ihrer Zahlungskartendaten angewendet werden. Diese beinhalten:

- das Vorhalten von Daten nur solange, wie unbedingt notwendig und nicht länger;
- Einschränkung von Datenzugriffen abhängig von Notwendigkeit;
- Testen von Sicherheitssystemen hin auf mögliche Schwachstellen;
- Installieren und Kommunizieren von dedizierten Sicherheitsrichtlinien.

Die detaillierte Anleitung, die der PCI-Sicherheitsrat zur Erfüllung dieser Anforderungen zur Verfügung stellt, kann Unternehmen dabei helfen, auch die Einhaltung von GDPR-Vorgaben in Bezug auf den Umgang mit Zahlungsverkehrsdaten zu gewährleisten. Auch könnte sie eine sinnvolle Richtung hinsichtlich der Entwicklung von Kontrollen und Prozessen für andere Formen von persönlich identifizierbaren Daten (PID) vorgeben.

Die ewige Debatte: Compliance versus Sicherheit

Ziel des Payment Security Reports ist es nicht, Leser davon zu überzeugen, dass PCI-Standards eingehalten werden müssen. Vielmehr geht es darum, eine Orientierungshilfe dahingehend zu liefern, wie sich PCI-Compliance konkret umsetzen lässt und erhalten lässt.

Eine PCI-Compliance-Validierung bedeutet nicht, dass Systeme „sicher" sind, sondern nur, dass es während des Beurteilungszeitraums – in der Regel ein oder zwei Wochen – keinen Nachweis für die Nichteinhaltung gab. Sicherheitssysteme werden hingegen oftmals jeden Tag überprüft.

Die Einhaltung des PCI-DSS-Standards ist also kein Projekt, keine einmalige Aktivität, sondern ein laufender Prozess. Ein Programm, das sich an die sich ändernden Bedürfnisse von Unternehmen und neuen Technologien innerhalb des Geschäftsumfeldes anpassen muss. Es ist zudem ein Programm, das zwar von oben aufgesetzt und gesteuert werden, jedoch von jedem Mitarbeiter verstanden und akzeptiert werden sollte.