Bild: Archiv

Der neue Standard versucht dem aktuellen Stand der Technik, wie auch der veränderten Bedrohungslage Rechnung zu tragen.

PCI DSS – nicht nur Banken

Für alle Unternehmen, die mit Kreditkarten in Berührung (Verarbeiten oder Speichern) kommen, müssen die Anforderungen aus der PCI DSS (Payment Card Industry Data Security Standard) umgesetzt werden. Hinter dem Standard stehen die Kreditkartenunternehmen, aber auch viele Banken und Zahlungsdienstleister. Am 31. März 2022 wurde die neue Version 4.0 nach über neun Jahren Abstand seit dem letzten Major-Release veröffentlicht. Verbindlich wird diese für die Unternehmen aber erst per 31. März 2025.

Über vier Jahre dauerte die Fertigstellung der aktuellen Ausgabe der PCI DSS. Bereits Ende 2017 wurde der erste RFC (Request for Comments, Anfrage für Kommentare/Mithilfe) veröffentlicht. Die lange Entwicklungszeit, wie auch der lange Abstand zur vorherigen Version lassen es erahnen, es hat sich einiges am Standard geändert. Und dies ist auch gut so. Eine Aktualisierung war dringend notwendig. Auch wenn der Standard immer technologieunabhängig war und ist, hat sich in den vergangenen Jahren sehr viel in der IT geändert. Auch die Angriffe auf Infrastrukturen haben sich verändert und massiv zugenommen. Der neue Standard versucht dem aktuellen Stand der Technik, wie auch der veränderten Bedrohungslage Rechnung zu tragen. Der Standard ist kostenlos in verschiedenen Sprachen herunterladbar, beispielsweise in Deutsch. Bei Unsicherheiten sollte, und dies ist teilweise auch notwendig, auf die englische Original-Version zurückgegriffen werden.

Neue Anforderungen sind dazu gekommen

Mit dem aktuellen Release sind 64 neue Anforderungen dazu gekommen, unter anderem wird damit auch den aktuellen Gegebenheiten, wie der vermehrten Nutzung der Cloud Rechnung getragen. Die PCI DSS unterscheidet dabei zwischen Händlern (Merchants) und Bezahldienstleistern (Service-Providers). 53 von 64 neuen Anforderungen sind jedoch für alle PCI-relevanten Firmen anwendbar, nur elf gelten ausschliesslich für Bezahldienstleister.

Ein wichtiger Punkt ist Definition des Anwendungsbereichs. Weil dies immer wieder zu Diskussionen während des Audits führte, wurde bereits 2016 ein zusätzliches Dokument zum Thema

Themengebiet	Anforderungen
Ein sicheres Netzwerk und sichere Systeme aufbauen und warten	1. Installation und Wartung von Netzwerksicherheitskontrollen 2. Anwendung sicherer Konfigurationen auf alle Systemkomponenten
Schutz von Kontodaten	3. Schutz von gespeicherten Kontodaten 4. Schutz von Karteninhaberdaten mit starker Kryptographie während der Übertragung über offene, öffentliche Netzwerke
Wartung eines Programms zur Verwaltung von Schwachstellen	5. Schutz aller Systeme und Netzwerke vor bösartiger Software 6. Entwicklung und Wartung sicherer Systeme und Software
Implementierung starker Zugriffskontrollmassnahmen	7. Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten nach geschäftlichem Bedarf 8. Identifizierung von Benutzern und Authentisierung von Zugriff auf Systemkomponenten 9. Beschränkung des physischen Zugriffs auf Karteninhaberdaten
Regelmässige Überwachung und Prüfung der Netzwerke	10. Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten 11. Regelmässige Prüfung der Sicherheit von Systemen und Netzen
Beibehaltung einer Informationssicherheitspolitik	12. Unterstützung der Informationssicherheit durch organisatorische Richtlinien und Programme

Die zwölf Herausforderungen.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Scoping herausgegeben. Es ist aber nur als Empfehlung zu verstehen. Die Änderung hilft nun Unternehmen, die bereits andere Standards wie ISO 27001 umgesetzt haben. Bis anhin war es praktisch nicht möglich, beziehungsweise nur mit einem grossen Aufwand, die beiden in einen Einklang zu bringen. Herausfordernd ist aber mit dieser Anpassung, dass der Anwendungsbereich jährlich (bei Bezahldienstleistern sogar halbjährlich) oder nach bedeutenden Änderungen an der Umgebung überprüft werden muss.

Unverändert sind die zwölf Hauptanforderungen geblieben

Im Unterschied zu anderen Standards und Normen ist die PCI DSS sehr konkret. So umfasst das Dokument in der deutschen Ausgabe 389 Seiten. Neben den Anforderungen an die Umsetzung sind auch Anforderungen an die Auditoren definiert. Zwar helfen die konkreten Massnahmen Unternehmen, schränken aber gleichzeitig die Freiheit auch wieder ein. Die Auditoren haben damit auch nicht die Freiheit eine etwas anders als gewohnte Massnahme zu akzeptieren. Unverändert geblieben sind die zwölf Hauptanforderungen (Bild).

Hinweis: Für die Vorgänger-Version 3.2.1 ist ein Mapping-Guide zum NIST Cybersecurity Framework vorhanden, welches wir in der Ausgabe Maschinenbau 2022/6 ausführlicher angeschaut haben. Vermutlich wird dieser Leitfaden auch bald für die aktuelle Version veröffentlicht.

Jede dieser Hauptanforderungen ist viele Teil-Anforderungen unterteilt. Jede Anforderung wird detailliert beschrieben und umfasst die folgenden Informationen:

- Titel: organisiert und beschreibt die Anforderungen
- Definierte Ansatzanforderungen: beschreibt das Verfahren zur Implementierung
- Zielsetzung: ist das beabsichtigte Ziel oder das Ergebnis der Anforderung
- Testprozeduren: beschreibt das Verfahren zur Prüfung
- Zweck: beschreibt das Ziel, den Nutzen oder die Bedrohung, die vermieden werden soll
- Gute Praxis: kann vom Unternehmen berücksichtigt werden, wenn sie eine Anforderung definiert (oder anders formuliert, Beispiele zur Umsetzung)
- Definitionen: Begriffe, die zum Verständnis beitragen können
- Beispiele: beschreiben Möglichkeiten, wie eine Anforderung erfüllt werden kann
- Weitere Informationen: beinhalten Verweise auf relevante externe Dokumentation

Auch wenn ein Unternehmen keine Kreditkarten-Informationen verarbeitet, lohnt es sich die zwölf Haupt- und die diversen Teilanforderungen genauer anzuschauen und zu prüfen, was im eigenen Unternehmen umgesetzt werden kann, zum Beispiel die durchgängige Nutzung von MFA (Multi-Factor-Authentication), also einem zweiten Faktor beim Login wie SMS oder Authenticator-App. Weiter gehören umfassende Security-Awareness-Trainings oder regelmässige Schwachstellensuchen dazu. Schon allein mit diesen Schritten kann die Informationssicherheit bereits nachhaltig erhöht werden. Zwar ist nun eine neue Version verfügbar. Trotzdem kann sich ein Unternehmen Zeit lassen. Bis zum 31. März 2024 kann noch die Version 3.2.1 verwendet werden. Ein Jahr später, das heisst ab dem 1. April 2025 wird eine (Re-)Zertifizierung nur noch nach der aktuellen Ausgabe möglich sein, da ab dann die neuen Anforderungen verpflichtend sind. Trotz der langen Übergangsfrist sollten sich die Unternehmen, die mit Kreditkartendaten Berührungspunkte haben, bereits jetzt mit diesen Anforderungen auseinandersetzen und diese möglichst bald einführen.