Viele Unternehmen erfüllen den Standard schon jetzt

Wie Sie dem PCI:DSS-Standard furchtlos gegenübertreten

Um Kreditkartenmissbrauch zu unterbinden, gibt es den Payment Card Industry Data Security Standard (PCI:DSS). Er ist für Unternehmen verbindlich, die Kreditkartendaten erfassen, verarbeiten oder speichern. Ihr Unternehmen gehört dazu? Dann zeigen Sie der Geschäftsleitung, dass sie, wenn sie wichtige Datenschutzanforderungen umgesetzt hat, auch schon die meisten Komponenten des PCI-Standards erfüllt.

PCI:DSS sorgt für mehr Sicherheit

Mit den Möglichkeiten des Internets stiegen in den letzten Jahren auch die Einkäufe mit Kreditkarte immens. Leider erhöhte sich damit zugleich der Missbrauch von Kreditkarten.

Kreditkartenunternehmen einigten sich auf einen Sicherheitsstandard

Im Jahr 2005 erstellten daraufhin die größten Kreditkartenunternehmen einen einheitlichen Sicherheitsstandard, den Payment Card Industry Data Security Standard, kurz PCI:DSS.

Die Umsetzung hinkt

Dieser Standard sollte bei allen Partnerunternehmen mit mindestens 1 Million Transaktionen im Jahr zum 01.01.2008 umgesetzt worden sein.

Doch selbst von Unternehmen, die schon zuvor diesen Standard zertifizieren lassen sollten, gibt es nur wenige, die dieser Anforderung nachgekommen sind.

Die meisten der insgesamt 12 Forderungen sind oft schon erfüllt

Die Unternehmen scheuen anscheinend den finanziellen Aufwand und nehmen lieber

eventuelle Schadens-ersatzverpflichtungen in Kauf.

Dabei erfüllen verantwortungsvolle Unternehmen ohnehin schon die notwendigsten Anforderungen für eine erfolgreiche Zertifizierung. Dies gilt insbesondere für Unternehmen, die dem Datenschutz und v.a. dem § 9 BDSG mit seinen Anlagen Rechnung tragen. Dies sei hier einmal vor Augen geführt:

1. Erstellen einer angepassten Firewallkonfiguration

Welches Unternehmen mit Internetzugang kann heutzutage keine Firewall mit entsprechender Sicherheitskonfiguration vorweisen? Ein verantwortungsvolles Unternehmen wird hier sicher die Anforderungen erfüllen.

2. Änderung der Auslieferungskennwörter

Ein Administrator, der nicht umgehend die Kennwörter neuer Systeme ändert, hat seinen Job nicht verstanden. So ein Versäumnis wird kaum noch anzutreffen sein!

3. Schutz der Karteninhaberdaten

Eine Maßnahme, die mit Respekt vor dem Datenschutz selbstverständlich ist! Ein verantwortungsvolles Unternehmen wird den Zugang zu diesen Daten nur unter erheblichen Sicherheitsvorkehrungen zulassen und idealerweise physikalisch vom restlichen Systembetrieb trennen oder zumindest verschlüsselt ablegen.

4. Verschlüsselte Übertragung von Karteninhaberdaten

Oftmals bereits ein Bestandteil der zuvor genannten und erfüllten Anforderung. Diese Anforderung nennt aber auch explizit die Anlage zu § 9 BDSG unter der Weitergabekontrolle.

5. Regelmäßige Aktualisierung der Antiviren-Patterns und der Antiviren-Software

Dies sind Standard-Einstellungen bei Auslieferung. Und eine fehlende Update-Lizenz des Antiviren-Herstellers ist nicht mehr zeitgemäß.

6. Nutzung sicherer Systeme

Wer seine Systeme nicht regelmäßig patcht, hat die letzten Jahre verschlafen. Der erfahrene IT-Administrator wird Patches allerdings vor dem Einsatz in kritischen Systemen testen.

7. Beschränkung des Zugriffs auf geschäftliche Zwecke

Auch diese Anforderung wird bereits durch die Anlage zu § 9 BDSG mit der Zweckbindung abgedeckt. Die geforderte Datensparsamkeit verlangt ebenfalls Enthaltsamkeit bei der Datennutzung.

8. Verwendung eindeutiger User-IDs

Kein Standard ohne diese Forderung! Missbräuche müssen eindeutig nachvollziehbar sein. Auch dies ist in der Anlage zu § 9 BDSG enthalten und fordert über eine

Eingabekontrolle die eindeutige Zuordnung der User-ID.

9. Beschränkung des Zutritts zu Speichersystemen, Speicherung der Karteninhaberdaten

Bereits der erste Absatz der Anlage zu § 9 BDSG fordert eine Zutrittskontrolle. Da diese Daten ohnehin zumeist in Rechenzentren abgelegt werden und diese in der Regel mit einer Zutrittskontrolle versehen sind, wird auch diese Anforderung den meisten Unternehmen keine Probleme bereiten.

10. Führen von Zugriffsprotokollen für Netzwerkressourcen und Karteninhaberdaten

Auch die Anlage zu § 9 BDSG fordert die Protokollierung der Zugriffe, die zumindest in den Ereignisprotokollen von Windows-2003-Servern und in den syslogs der Linux-Systeme per Vorgabe aktiv ist.

Die Protokollierung der Zugriffe auf Karteninhaberdaten muss u.U. noch angepasst werden, je nach gewählter Schutzmaßnahme dieser Daten.

11. Regelmäßige Tests der Sicherheit

Penetrationstests sind Standards in diversen Sicherheitsanforderungen und werden regelmäßig von Wirtschaftsprüfern eingefordert. Es ist wahrscheinlich, dass ein verantwortungsvolles Unternehmen auch diesen Anforderungen bereits nachkommt.

12. Erstellen einer Richtlinie zur Informationssicherheit

Zugegeben, hier wird zum ersten Mal ein größerer Aufwand deutlich, der über die üblichen Anforderungen der Informationssicherheit hinausgeht.

Dennoch sind diese Anforderungen den Unternehmen meist klar und müssen nur noch zu Papier gebracht werden. Unternehmen, die bereits ein Informationssicherheits-Management-System etabliert haben, werden diesen Prozess mit einem müden Lächeln übergehen.

Ganz ohne Aufwand geht es nicht

Natürlich muss sich auch ein Sicherheitsbeauftragter um die Dokumentation der PCI:DSS-Compliance kümmern und etwaige Missstände beheben.

Aber es gibt noch eine weitere Forderung, die die üblichen Sicherheitsmaßnahmen nicht abdecken: Die Unternehmen müssen sich einem vierteljährlichen Schwachstellenscan durch einen beim PCI-Standard-Council zugelassenen Scanner unterziehen.

Eine Liste der sogenannten Approved Scanning Vendors (ASVs) findet sich auf der Seite des PCI Security Standards (http://www.pcisecuritystandards.org).

Meist reicht eine Selbstauskunft

Die meisten Unternehmen müssen den Nachweis der PCI:DSS-Konformität nur mit einer Selbstauskunft führen.

Lediglich Unternehmen mit mehr als sechs Millionen Transaktionen müssen diesen Standard gegenüber einem vom PCI Standard Council akkreditierten Qualified Security Assessor (QSA) in einer detaillierteren Form nachweisen.

Fehlende Umsetzung gibt Platz für Verbesserungen

Die QSAs wissen, dass der Standard jung ist. Sie werden ihn daher noch nicht bis ins letzte Detail einfordern. Stattdessen werden sie froh sein, in Ihrem Unternehmen einen verantwortungsbewussten Partner zu finden.

Thomas Ili
Thomas Ili ist Inhaber der Hamburger Unternehmensberatung Abakus-IT, geprüfter Auditor der ISO-27001-Systeme, CISA und DSB.

Veröffentlicht:
20.02.2008

Zurück zur Übersicht

Verweise

- Datenschutz PRAXIS 03/08