LANCOM™ Whitepaper
PCI-Compliance

Einleitung

Mit dem PCI DSS (Payment Card Industry Data Security Standard) haben sich die führenden Anbieter von elektronischen Zahlungssystemen (Kartenbetreiber) im Jahr 2005 auf einen verbindlichen Mindeststandard für die Datensicherheit ihrer Kunden geeinigt. Dieser Standard soll sicherstellen, dass die Kundendaten von Kartenzahlern nicht gestohlen, verändert oder in anderer Art und Weise missbraucht werden. Der Anlass für die Einführung dieses Standards ist der rasante Anstieg von Fällen des Kartenbetrugs. Berichten der Branche zufolge haben die Angriffe auf Einzelhändler, die Kartenzahlung akzeptieren, allein zwischen 2003 und 2006 um mehr als 50% zugenommen. Unternehmen, die Kartenzahlung akzeptieren, werden von den Kreditkartenunternehmen dazu verpflichtet, Ihre Installationen auf PCI DSS Konformität prüfen und zertifizieren zu lassen. Hält man sich nicht an diese Vorgabe, kann das Kreditkarteninstitut außerordenlich den Vertrag kündigen und auch die Haftung für entstandene Schäden überwälzen. Die Zertifizierungsaudits werden von Unternehmen durchgeführt, die sowohl von Mastercard als auch von Visa zum so genannten „Security Assessor" erklärt wurden.

Wirtschaftliche Schäden und Image-Verlust

Der wirtschaftliche Schaden, der durch unzureichende Schutzmaßnahmen gegen Kartenbetrüger entsteht, trifft in der Regel die Einzelhändler selbst – die Kartenbetreiber lehnen die Haftung oft mit Verweis auf vorhandene Sicherheitslücken ab. Darüberhinaus ist der Verlust von Kundenvertrauen eine realistische Bedrohung, wenn ein Einzelhändler aufgrund unzureichender Schutzmaßnahmen Opfer eines Angriffs wird. Durch den Standard entsteht eine erhebliche Erleichterung für die Kartenbetreiber und Einzelhändler, da sie nun einen festen Satz an Anforderungen fordern bzw. erfüllen können und so Rechtssicherheit gewinnen. Gegenüber dem Endkunden kann der Händler eine umfassende Sicherheitsstrategie kommunizieren und so die Datensicherheit und das damit verbundene Vertrauen garantieren. Alle Unternehmen und Händler, die Kartenzahlung akzeptieren, müssen die Bedingungen des Standards erfüllen. Anderenfalls drohen empfindliche Strafen, und die Händler haften bei einem Angriff selbst.

Der PCI-Standard im Detail

Die Verarbeitung der kartenbezogenen Daten erfolgt über verschiedene Komponenten in den Netzwerken der Handelsunternehmen – vom Kartenlesegerät über die Kasse bis zu zentralen Servern und ERP-Systemen. Diese Netzwerke werden mit Hilfe von Routern und Switches realisiert, welche die Verbindung zwischen den einzelnen Komponenten herstellen und die Datenübertragung im lokalen und zu entfernten Netzwerken regeln (bis hin zum Abrechnungsserver der Kartenbetreiber).

Der PCI-Standard legt insbesondere fest, welche Erwartungen die Kreditkartenindustrie an die verwendete IT-Infrastruktur in den Handelsunternehmen stellt. Dabei kann immer nur ein gesamtes System dem Standard genügen, nicht einzelne Geräte oder Teilbereiche. Auch wenn ein großer Teil des Netzwerks technisch gesehen

LANCOM™ Whitepaper
PCI-Compliance

den PCI DSS erfüllen würde, genügt eine einzige Lücke oder eine einzige nicht aktivierte Schutzmaßnahme, um das gesamte System zu kompromittieren. Dennoch müssen alle eingesetzten Komponenten eine PCI-Kompatibilität aufweisen, um innerhalb eines PCI-konformen Netzwerk eingesetzt zu werden. Das angestrebte Ziel ist die PCI-Konformität in einer sogenannten „end-to-end"-Form, also auf dem gesamten Datenweg zwischen Point-of-Sale und Kartenbetreiber.

Planung von PCI-konformen IT-Systemen

Auch wenn verschiedene Teil-Komponenten einer Infrastruktur scheinbar nichts mit Kartenzahlung zu tun haben, genügt den Angreifern eine beliebige, ungeschützte Stelle, um in das gesamte System einzubrechen. Es ist daher notwendig, bei der Planung der verwendeten Rechnernetze eine langfristige und skalierbare Lösung anzustreben, in der einzelne Komponenten austauschbar bleiben, ohne das Gesamtsystem zu gefährden.

Darüber hinaus spielt eine Erfüllung des Standards nur zum Zeitpunkt eines Angriffs eine Rolle, nicht danach oder davor. Es gilt also eine zeitlich permanente Lösung mit entsprechenden Maßnahmen zu wählen, und diese auch nachvollziehbar zu machen. Die Unternehmen müssen nach einem Angriff selber nachweisen, dass sie den Standard erfüllt haben.

Daraus ergibt sich ein Satz von Anforderungen an die Umsetzung des PCI DSS: Die angestrebte Lösung sollte modular aufgebaut sein und sich zentral verwalten, warten und überwachen lassen. Darüberhinaus muss es möglich sein, auch zeitlich zurückliegende Ereignisse untersuchen zu können, es muss also eine lückenlose Protokollierung erfolgen.

Die 12 Forderungen des PCI-Standards

Der PCI DSS umfasst konkret 12 Forderungen:

1. Das Einrichten einer Firewall
2. Das sofortige Ändern aller Werks-Passwörter und andere Sicherheits-relevante Parameter auf eigene, sichere Werte
3. Schutz der gespeicherten Daten
4. Verschlüsselung der Datenübertragung über offene Netze
5. Virenschutz
6. Die Pflege und Entwicklung sicherer Systeme und Anwendungen
7. Es sollten nur notwendige Datenzugriffe erfolgen, „need-to-know"-Basis
8. Jeder Benutzer des Netzwerkes muss eindeutig identifizierbar sein
9. Ein physischer Zugangs-Schutz
10. Eine umfassende Protokollierung aller Zugriffe auf Kartendaten
11. Eine regelmäßige Überprüfung aller Sicherheiteinrichtungen
12. Das Erstellen einer IT-Sicherheitsstrategie (Policy) und deren Einhaltung

Die letzte Forderung hat dabei eine besondere Bedeutung, da sich alle anderen Punkte hieraus direkt ableiten lassen. Die hier geforderte IT-Sicherheitsstrategie muss das gesamte System betreffen und alle restlichen Punkte abdecken. Dabei genügt es nicht, PCI-kompatible Hardware und Software einzusetzen, die IT-Sicherheitspolicy muss auch das Verhalten der Mitarbeiter einbeziehen, alle restlichen Forderungen des PCI DSS abdecken und so jede mögliche Angriffsstelle im System schließen.

Einzelne Geräte und Software müssen zwar den Anforderungen des PCI DSS entsprechen, können aber nur

LANCOM™ Whitepaper
PCI-Compliance

innerhalb eines Gesamtsystems, dass die Anforderungen erfüllt, ihren Teil zur angestrebten PCI-Compliance beitragen.

Netzwerkkomponenten müssen PCI-Konformität unterstützen

Ein Teil der Forderungen des PCI-Standards muss von den verwendeten Netzwerkkomponenten (z. B. Router und Switches) erfüllt werden, z.B. durch die Einrichtung von geeigneten Firewalls und die Verschlüsselung der Daten (z.B. VPN im WAN).

Mit diesen Funktionen stellen die Netzwerkkomponenten allerdings nur bestimmte Sicherheitsfunktionen für andere Dienste der Netzwerkstruktur bereit. Ein wesentlicher Aspekt zur Erfüllung der PCI-Anforderungen ist die Kontrolle über den Zugang zu den Netzwerkkomponenten selbst: wenn sich ein Angreifer Zugang zu einem Router oder Switch verschafft, kann er durch Änderungen der Konfiguration evtl. die anderen Sicherheitsmaßnahmen ausschalten und so das gesamte IT-System kompromittieren.

Um die Netzwerk-Hardware vor unberechtigten Zugriff zu schützen und so die PCI-Compliance zu erreichen, müssen die verwendeten Komponenten ein „Triple-A"-Verfahren unterstützen. „Triple A" steht für Authentifizierung, Autorisierung und Accounting.

- Mit der Authentifizierung wird der Benutzer erkannt. So wird sichergestellt, dass nur eindeutig identifizierte Benutzer einen Zugang zu den Netzwerkkomponenten erhalten (Punkt 8 der PCI-Anforderungen).
- Über die Funktion der Autorisierung werden dem Benutzer seine speziellen Rechte zugewiesen.
- Mit dem Accounting werden alle Aktionen des Benutzers aufgezeichnet. So kann auch im Nachhinein jederzeit geprüft werden, ob zu einem bestimmten Zeitpunkt das IT-System PCI-konform war.

Nur wenn die verwendeten Netzwerkkomponenten die Funktionen Authentifizierung, Autorisierung und Accounting unterstützen, können sie in einem PCI-konformen Netzwerk eingesetzt werden.

Ein mögliches Triple-A-System ist „TACACS+". Im Vergleich zum weit verbreiteten RADIUS bietet TACACS+ den Vorteil, dass die drei Einzelbereiche Authentifizierung, Autorisierung und Accounting auf getrennten Komponenten ausgeführt werden können. So kann z.B. die Verwaltung der Benutzerkonten zur Authentifizierung auf einem Server, die Protokollierung der Aktivitäten (Accounting) aber auf einem anderen Server erfolgen. Zudem bietet TACACS+ eine bessere Verschlüsselung der übertragenen Informationen.

LANCOM-Geräte ermöglichen systemweite PCI-Compliance

Mit der Unterstützung von TACACS+ stellen die LANCOM-Geräte sicher, dass nur eindeutig authentifizierte Benutzer Zugang zur Konfiguration der Geräte erhalten. Mit einer geeigneten Einstellungen der Benutzerrechte (Authorisierung) wird sichergestellt, dass die Benutzer nur nachvollziehbare Änderungen vornehmen dürfen, die vom Accounting-Server protokolliert werden können. Konkret werden dabei z.B. die Funktionen gesperrt, mit denen eine vollständige Gerätekonfiguration in das Gerät geschrieben werden kann, wie es bei der Nutzung von LANconfig üblich ist. Solange diese Funktion erlaubt ist, wäre ansonsten eine nicht protokollierbare Änderung der Konfiguration möglich, was einer PCI-Compliance widersprechen würde.

Auch mit weiteren Sicherheitsfunktionen zum Schutz der Konfiguration bei Diebstahl der Geräte unterstützen Router und Switches von LANCOM Systems den Aufbau einer PCI-konformen IT-Infrastruktur.

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de

LANCOM Systems