



# MANAGEMENT-SOFTWARE HILFT BEI EINHALTUNG DES PCI-STANDARDS

Brian Patch und Greg Naderi

*Version 1.1 des Payment Card Industry Data Security Standard verlangt strengere Durchsetzung von Sicherheitsrichtlinien bei Handelsunternehmen, Banken und Service-Providern.*

## **INHALT**

**Die Auswirkungen von Identitätsdiebstahl 2**

**Der Payment Card Industry Data Security Standard – PCI DSS 3**

**Das „digitale Dutzend“: die PCI-Regeln verstehen 4**

**Kosten-Nutzen-Analyse 5**

**Der „Geltungsbereich“ des PCI-Standards 6**

**Mängel und Herausforderungen: die „Top Ten“ der wichtigsten Verstöße gegen PCI-Regeln 7**

**SonicWALL und der PCI-Standard 7**

**SonicWALL GMS: solides Fundament für PCI-Compliance 8**

**Zusammenfassung 10**

## Überblick

Die Einhaltung des Payment Card Industry Data Security Standard – kurz PCI DSS oder PCI – erfordert ausgeprägtes Expertenwissen bezüglich der Anforderungen an Datenaufbewahrung und Verschlüsselung, Integration einzelner Geräte sowie Vorgaben für Logging und Reporting in verteilten Netzwerken. Das preisgekrönte SonicWALL Global Management System (GMS) hilft Unternehmen dabei, die strikten Anforderungen des PCI-Standards in diesen Bereichen einzuhalten. Zu diesem Zweck ermöglicht die Software u. a. die zentrale Festlegung und Durchsetzung von Sicherheitsregeln und Policies in verteilten Umgebungen, die Echtzeitüberwachung von Systemen sowie das rückwirkende („historische“) Reporting für Installationen aller Größenordnungen.

## Die Auswirkungen von Identitätsdiebstahl

Der Diebstahl von Konto- und Kreditkarteninformationen, auch bekannt als *identity theft*, hat sich in den vergangenen Jahren zu einem milliardenschweren Geschäftsfeld entwickelt, das Berufskriminellen weltweit inzwischen deutlich mehr Geld einbringt als klassische Raubdelikte. Nach jüngsten Berichten der US-Handelsschutzbehörde *Federal Trade Commission* (FTC) fielen allein 2005 rund 8,3 Millionen Amerikaner entsprechenden Delikten zum Opfer<sup>1</sup>; der Gesamtschaden summierte sich dabei auf geschätzte 15,6 Milliarden Dollar. Noch prekärer ist die Lage nach den aktuelleren Angaben des u. a. vom US-Justizministerium gesponserten *Identity Theft Resource Center* (ITRC): Ihnen zufolge beläuft sich allein die Zahl der in diesem Jahr gestohlenen, verlorenen oder sonstwie abhanden gekommenen Datensätze auf 19,6 Millionen (Stichtag: 29.07.2008)<sup>2</sup>, wobei allerdings zu berücksichtigen ist, dass hier auch Angaben zur Sozialversicherung und medizinische Unterlagen einbezogen werden. Kaum besser stellt sich die Situation in Deutschland und Europa dar: So weist die im Mai vom Bundesinnenministerium vorgelegte *Polizeiliche Kriminalstatistik 2007* insgesamt 5927 Fälle der Fälschung von Zahlungskarten, Schecks und Wechseln und 4829 Fälle des Ausspähens von Daten aus<sup>3</sup> – beide Male ein sattes Plus von mehr als 60 Prozent gegenüber dem Vorjahr. Das britische Innenministerium veranschlagte den Gesamtschaden für die Wirtschaft des Vereinigten Königreichs 2005 auf 2,16 Milliarden Euro. Und die Europäische Kommission wiederum bezifferte vergangenen April die Ausfälle durch „Zahlungskartenbetrug“ im Einheitlichen Euro-Zahlungsverkehrsraum (Single Euro Payments Area – SEPA) auf eine Billion Euro jährlich<sup>4</sup>. Die Statistiken belegen eindrucksvoll, was IT-Sicherheitsexperten seit langem beklagen: Identitätsdiebstahl und speziell der Missbrauch von Konto- und Kreditkarteninformationen sind zu einem globalen Problem geworden.

Die o. g. FTC-Studie zeigte ferner, dass im Berichtsjahr 3,7 Prozent der knapp 5000 Befragten in der einen oder anderen Form Opfer eines Identitätsdiebstahls wurden – das entspricht hochgerechnet jedem 27. US-Haushalt. Der dabei entstandene Verlust belief sich auf durchschnittlich 1882 Dollar (rund 1200 Euro). In 85 Prozent der Fälle kaperten die Datendiebe dabei bestehende Geschäftsverbindungen, bevorzugt mit Banken und Kreditkartenunternehmen; 17 Prozent der Betroffenen berichteten darüber hinaus, dass in ihrem Namen neue Konten eröffnet bzw. neue Dienstleistungs-, Kredit- und Versicherungsverträge abgeschlossen wurden. Andere Formen des Missbrauchs umfassten u. a. das Erschleichen staatlicher Finanzhilfen. Etwa 40 Prozent der Opfer stellten binnen einer Woche fest, dass Kriminelle ihre Daten nutzten, der Rest brauchte teilweise deutlich länger (bis zu sechs Monaten). Interessant ist darüber hinaus der zur Klärung der Probleme benötigte Zeitaufwand: Dieser belief sich in 23 Prozent der Fälle auf weniger als 24 Stunden, knapp 16 Prozent der Befragten hatten zwischen sieben und 30 Tagen damit zu tun, und elf Prozent benötigten drei Monate oder länger. Gut ein Fünftel der Teilnehmer (21 Prozent) kämpfte auch während der Befragung noch mit den Folgen der Datenverluste. Schwerer als die so entstandenen und immer noch entstehenden Schäden wiegt eigentlich nur die Tatsache, dass diese durch eine

---

<sup>1</sup> Vgl. dazu: Federal Trade Commission – 2006 Identity Theft Survey Report, S. 4; online unter: <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>

<sup>2</sup> Vgl. dazu: 2008 ITRC Breach Report, S. 123; online unter: <http://idtheftmostwanted.org/ITRC%20Breach%20Report%202008.pdf>

<sup>3</sup> Vgl. dazu: Bundesministerium des Innern, Polizeiliche Kriminalstatistik 2007, S. 9; online unter: [http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/Polizeiliche\\_Kriminalstatistik\\_2007\\_de\\_templateld=raw,property=publicationFile.pdf/Polizeiliche\\_Kriminalstatistik\\_2007\\_de.pdf](http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/Polizeiliche_Kriminalstatistik_2007_de_templateld=raw,property=publicationFile.pdf/Polizeiliche_Kriminalstatistik_2007_de.pdf)

<sup>4</sup> Vgl. dazu: Commission Staff Working Document – Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004–2007 EU Action Plan, S. 6; online unter: [http://ec.europa.eu/internal\\_market/payments/docs/fraud/implementation\\_report\\_en.pdf](http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf)

ausreichende Absicherung der für die Datenübermittlung genutzten technischen Systeme und Netzwerke hätten vermeiden bzw. wenigstens deutlich vermindern lassen.

## **Der Payment Card Industry Data Security Standard – PCI DSS**

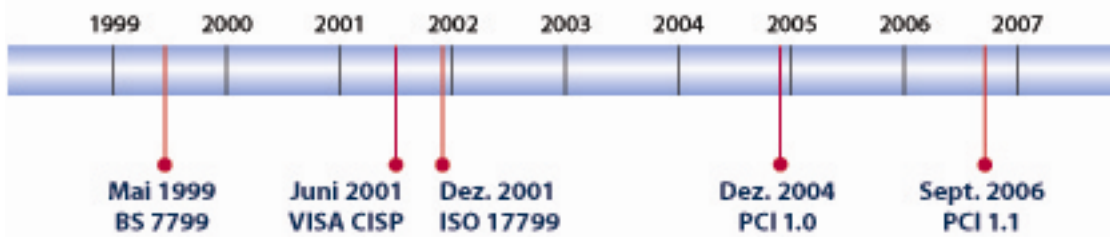
Der PCI DSS, PCI-Standard oder ganz kurz PCI entstand 2004 aus dem *Visa Cardholder Information Security Program* (CISP), welches das gleichnamige Kreditkartenunternehmen im Juni 2001 vorgelegt hatte. Ziel des PCI DSS war, einen offenen Standard zum Schutz der Daten von Kreditkarteninhabern zu schaffen, der allen Handelsunternehmen zugänglich sein sollte. Entwickelt von den vier größten der Branche – *American Express, Discover, MasterCard* und *Visa* –, sollte er darüber hinaus allen Kunden die Gewissheit vermitteln, dass ihre Daten sicher wären, wann immer sie in einem Kaufhaus, Restaurant oder Hotel mit ihrer Karte bezahlen. Heute gilt dieser Standard bei jeder Transaktion, die eine Weitergabe der Kreditkartennummer (*Primary Account Number* – PAN) erfordert, und regelt, wie die einschlägigen Informationen gesichert aufzubewahren, zu verarbeiten und zu übermitteln sind. Alle Handels- und Dienstleistungsunternehmen, die Kreditkarten akzeptieren, sind zur Einhaltung des PCI verpflichtet; bei Zuwiderhandlungen drohen befristete Sperren, Geldstrafen oder sogar Kündigung des Vertrages.

Doch nicht bloß diese Auflagen sind streng: Nach Meinung vieler Experten enthält der PCI-Standard in seiner aktuellen Version 1.1 schlicht die umfassendsten aller zurzeit existierenden Datenschutzvorschriften, neben denen selbst die auch bei europäischen Unternehmen gefürchteten Vorgaben des *Sarbanes-Oxley Act* verblassen. Aus europäischer Sicht bietet sich wohl am ehesten ein Vergleich mit dem EU-weit gültigen EMV-Standard für Debitkarten (EC- bzw. Maestro-Karten) an. Die Grundlagen des PCI DSS wiederum setzen auf den Vorgaben des international anerkannten Datenschutz- und Informationssicherheitsstandards ISO/IEC 17799 (seit Sommer vergangenen Jahres: ISO/IEC 27002:2005) auf, der seinerseits auf dem British Standard 7799 basierte. Die Vorgaben des PCI erstrecken sich im Einzelnen auf folgende Bereiche:

- Sicherheitsrichtlinien;
- Organisation von System- und Netzwerkressourcen;
- Bewertung und Überwachung informationsverarbeitender Systeme;
- Personal- und physische Sicherheit;
- Kommunikations- und Produktionsmanagement;
- Zugriffskontrolle;
- Systementwicklung und -pflege;
- Kontinuitätsmanagement/Aufrechterhaltung des Geschäftsbetriebs im Krisenfall;
- Compliance.

Der PCI gibt somit einen Satz von Standards und Verfahrensregeln vor, die über System- und Netzwerkgrenzen hinweg gelten. Anders ausgedrückt: Er legt fest, welche Anforderungen die Kreditkartenunternehmen an den Umgang mit den Daten der Karteninhaber stellen, wie sie Handels- und Dienstleistungsunternehmen einstufen und wie sie deren Anstrengungen zur Einhaltung des Standards bewerten. Händler, Dienstleister sowie eventuell zwischengeschaltete Daten verarbeitende Unternehmen sind für den Schutz der Kundeninformationen verantwortlich und dürfen z. B. bestimmte Datentypen weder auf den eigenen Systemen vorhalten noch zum gleichen Zweck an Dritte weitergeben. Sie haften außerdem für alle Schäden, die durch einen möglichen Datendiebstahl oder -verlust bzw. die Nichteinhaltung des Standards entstehen. Trotz dieser strengen Auflagen qualifiziert selbst die „wortgetreue“ Einhaltung des Standards ein Unternehmen nicht automatisch für die Zertifizierung durch eine der großen Kreditkartengesellschaften: Diese unterstützen zwar gemeinsam die im PCI festgelegten Prüf- und Auditierungsregeln, stellen aber nach wie vor ihre eigenen Zertifikate und Zulassungen aus.

## Entwicklung der Sicherheitsstandards



### Das „digitale Dutzend“: die PCI-Regeln verstehen

Der PCI-Standard beruht auf sechs fundamentalen Prinzipien<sup>5</sup>:

- Einrichtung und Unterhaltung eines sicheren Netzwerks;
- Schutz von Karteninhaberdaten/Kundeninformationen;
- Einhaltung eines Programms zur Abwehr von Sicherheitsrisiken;
- Implementierung strikter Zugriffsregeln;
- regelmäßige Überwachung und Prüfung von Netzwerken;
- Einhaltung unternehmensweiter Informationssicherheitsrichtlinien.



Diese Prinzipien werden weiterhin in zwölf zentrale Anforderungen aufgeschlüsselt, die auch als das „digitale Dutzend“ bekannt sind:

1. Einrichtung und Betrieb einer Firewall zum Schutz von Karteninhaberdaten;
2. keine Verwendung der Standardwerte des Hersteller für Systemkennwörter und andere Sicherheitsparameter;

<sup>5</sup> Quelle: PCI Security Standards Council: Payment Card Industry (PCI) Data Security Standard, Version 1.1, Release: September, 2006; online unter: [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)

3. Schutz gespeicherter Kundendaten; Verzicht auf die überflüssige Speicherung von Karten- und Transaktionsdaten;
4. Verschlüsselung der Karteninhaberdaten und anderer sensibler Informationen bei Übertragung über öffentliche Netzwerke;
5. Verwendung und regelmäßige Wartung/regelmäßiges Upgrade sicherer Systeme und Anwendungen sowie von Schutzprogrammen (z. B. AV-Software);
6. Entwicklung und Betrieb sicherer Systeme und Anwendungen;
7. Beschränkung des Zugriffs auf Karteninhaberdaten auf das für Transaktionen erforderliche Mindestmaß;
8. Zuweisung einer eindeutigen ID/Kennung zu jeder Person mit Computerzugriff;
9. Einschränkung des physischen Zugangs zu Karteninhaberdaten;
10. Nachverfolgung und Überwachung sämtlicher Zugriffe auf Netzwerkressourcen und Karteninhaberdaten;
11. regelmäßige Tests von Sicherheitssystemen und -prozessen;
12. Einführung und Durchsetzung strenger Sicherheitsprinzipien und -maßnahmen.

Auf diesem hohen Niveau lässt sich der PCI-Standard vergleichsweise intuitiv einhalten. Die Grundprinzipien und zentralen Anforderungen bilden eine Art allgemeingültiger Rahmenrichtlinie zur Einführung anerkannter Sicherheitsmaßnahmen, die sinnvollerweise nicht nur im Umgang mit Kreditkarteninformationen, sondern mit allen geschäftskritischen Daten gelten sollten.

### **Kosten-Nutzen-Analyse**

Einrichtung und Erhalt sicherer IT-Netzwerke kosten Geld, das ist aus der alltäglichen Praxis bekannt. Leider dient genau diese Feststellung, verbunden mit der Frage nach dem wirtschaftlichen Nutzen der Aktion, in vielen Fällen als Gegenargument gegen den Aufbau entsprechender Infrastrukturen. Im Fall der Nichteinhaltung des PCI-Standards lässt sich zumindest die Frage nach den daraus resultierenden finanziellen Nachteilen schlüssig beantworten. Wenn Karteninhaberdaten, die von einem Handelsunternehmen oder einem damit betrauten Dienstleister verwaltet werden, verloren gehen oder publik werden, tragen die Verantwortlichen folgende Kosten:

- Geldbußen bis zu einer Höhe von 500.000 Dollar (325.000 Euro) – der Betrag liegt im Ermessen des Kartenausstellers;
- alle durch den Missbrauch der Karteninhaberdaten/Kreditkartennummern entstandenen Schäden, vom Tag des Datenverlustes an;
- alle Kosten für die Wieder- bzw. Neuausgabe von Karten an die geschädigten Inhaber;
- alle Kosten für eventuelle weitergehende Maßnahmen wie forensische Untersuchungen des IT-Equipments zur Entdeckung bzw. Verhütung weiterer Schäden, zusätzliche Überwachung von Systemen usw. – über den Umfang der Maßnahmen entscheidet die betroffene Kreditkartengesellschaft.

Ferner drohen höhere Versicherungsprämien für den Schutz gegen Schäden durch Nichteinhaltung von Sicherheits-, Datenschutz- und Serviceregeln; außerdem Zivilklagen, deren Kosten sich nicht vorhersagen lassen.

Aufbau und Betrieb sicherer Netzwerke nach PCI-Standard dienen aber nicht bloß der Abwehr solcher wirtschaftlichen Nachteile. Vielmehr haben sie auch darüber hinaus einen ökonomischen Sinn, da sie zu einer insgesamt verlässlicheren, auf die Geschäftserfordernisse zugeschnittenen IT-Infrastruktur mit besserem Service, erhöhter Verlässlichkeit und insgesamt reduzierten Sicherheitsrisiken führen. Daraus wiederum resultieren größeres Kundenvertrauen und eine verbesserte Kundenbindung, vereinfachte Prüfverfahren und effizientere Kostenkontrollen.

### **Der „Geltungsbereich“ des PCI-Standards**

Zur Einhaltung des PCI-Standards sind theoretisch alle Unternehmen verpflichtet, die Kundeninformationen und Daten von Kreditkarteninhabern verarbeiten.<sup>6</sup> Das schließt im Besonderen folgende Gruppen ein:

- E-Commerce-Anbieter bzw. Betreiber von Online-Shops und -Handelsplattformen;

---

<sup>6</sup> Da der PCI relativ jung ist, steht seine Einführung bzw. Umsetzung in den Unternehmen noch am Anfang. Interessenten könnten auf die Vorlage der für Oktober angekündigten Version 1.2 des Standards warten wollen.

- Handelsunternehmen (z. B. Kauf- und Versandhäuser, Fachgeschäfte) und Dienstleister (z. B. Hotels, Restaurants, Fluggesellschaften, Autovermieter) aus der „realen“ Welt, die eine Zahlung per Kreditkarte akzeptieren – unabhängig davon, ob Waren per Post oder telefonisch bestellt bzw. die Beträge am *Point of Sale* abgebucht werden;
- Dienstleister, die Kreditkartentransaktionen abwickeln;
- DV-Unternehmen, die Transaktions- und Kundeninformationen übermitteln (*Transaction Processing Partners*, TPP);
- Application Service Provider bzw. Hosting-Unternehmen, die Online-Speicher anbieten (im PCI-Sprachgebrauch so genannte *Data Storage Entities* – DSE);
- Mitgliedsunternehmen des PCI Security Standards Council, vor allem die Kreditkartengesellschaften selbst in ihrer Eigenschaft als Dienstleister für den Finanz- und Bankensektor.

Da gerade Kreditkarteninformationen – wie gezeigt – ein bevorzugtes Ziel von Datendieben darstellen, sind alle Unternehmen, die zu einer der genannten Gruppen zählen, verstärkten Angriffen ausgesetzt. Aus ihrer Sicht benennt der PCI-Standard die grundlegenden Anforderungen und Regeln für den Schutz der Karteninhaberdaten. Um zu verstehen, welche Parteien diese Regeln und Anforderungen erfüllen müssen, wollen wir einmal eine Kreditkartenzahlung einer ganzheitlichen Betrachtung unterziehen. Jede an diesem Prozess teilnehmende Organisation wird als Mitglied bezeichnet und einer der drei folgenden Gruppen zugeordnet:

- **Aussteller:** Mitgliedsbanken und -finanzdienstleister, die Kreditkarten an Unternehmen oder Privatpersonen ausgeben;
- **Acquirer:** Mitgliedsbanken und -finanzdienstleister, die Handels- und Dienstleistungsunternehmen „anwerben“ und bei der Transaktionsabwicklung unterstützen (im Deutschen vielleicht am Treffendsten als „**Betreuer**“ zu bezeichnen);
- **Service Provider:** alle Unternehmen, die im Auftrag von PCI-Mitgliedsunternehmen, Ausstellern und Betreuern Karteninhaber- und Transaktionsdaten verarbeiten, speichern oder übermitteln.

Die Kreditkartengesellschaften haben die Verantwortung für unterschiedliche Bereiche der von diesen Unternehmen gemeinsam genutzten Sicherheitsarchitektur untereinander aufgeteilt. So ist etwa *Visa* dafür zuständig, geeignete IT-Dienstleister zu finden, die ein PCI-Assessment vornehmen und Unternehmen bei der Einführung standardkonformer Prozesse und Infrastrukturen beraten können, ferner für die Aus- und Fortbildung sowie die Zertifizierung der zuständigen Mitarbeiter sowie dafür, dass die einmal erworbene Befähigung erhalten bleibt bzw. in regelmäßigen Abständen erneuert wird. Die Aufgabe von *MasterCard* wiederum besteht darin, IT-Dienstleister zu finden und zu qualifizieren, welche die ab einem Jahresumsatz von 10.000 Dollar fälligen, regelmäßigen vierteljährlichen Überprüfungen von Handelsunternehmen und Dienstleistern – das sog. *PCI Compliance Scanning* - abwickeln.<sup>7</sup>

Je nach Transaktionsvolumen, bevorzugten Zahlungswegen/-methoden und potenziellem Datenverlustrisiko weist PCI DSS den an einer Zahlung beteiligten Unternehmen eines von vier Compliance-Leveln zu, also eine Sicherheitsstufe, der sie genügen müssen:

- **Level 1:** Hierzu zählen alle Unternehmen, die entweder mehr als sechs Millionen Transaktionen pro Jahr abwickeln, unabhängig von Zahlungsweg und -methode, sowie alle anderen Unternehmen, die nach Meinung einer Kreditkartengesellschaft dafür qualifiziert sind. Um PCI zu genügen, müssen alle Level-1-Unternehmen eine jährliche Vor-Ort-Überprüfung mit Hilfe eines zertifizierten Dienstleisters (sog. *Qualified Data Security Company* – QDSC), wahlweise ein internes Audit, vornehmen; zusätzlich ist das o. g. vierteljährliche Scanning durch einen ASV vorgeschrieben.
- **Level 2:** Hierzu zählen alle Unternehmen, die zwischen einer und sechs Millionen Transaktionen pro Jahr abwickeln, ebenfalls unabhängig von Zahlungsweg und -methode. Im Gegensatz zur höchsten Kategorie reicht bei Level-2-Unternehmen eine jährliche interne Überprüfung anhand eines Standardfragebogens aus, hinzu kommen die ASV-Scans.

<sup>7</sup> Im PCI-Duktus heißen diese Dienstleister *Approved PCI Compliance Scanning Vendors* oder kurz ASVs. Eine Liste mit international zugelassenen ASVs findet sich online unter [https://www.pcisecuritystandards.org/pdfs/asv\\_report.html](https://www.pcisecuritystandards.org/pdfs/asv_report.html); für Interessenten aus dem deutschen Sprachraum bietet sich u. a. ein Besuch der Website „PCI Consultants.de“ (<http://pci2.aitigo.de/>) der IT Future AG mit Sitz in Frankfurt am Main an.

- **Level 3:** Dieser Kategorie gehören alle Unternehmen an, die zwischen 20.000 und einer Million Online-Transaktionen einleiten und ausführen (also Buchungs- oder Bestellvorgänge, bei denen Karteninhaberdaten per Internet übermittelt werden). Für sie gelten die gleichen Anforderungen wie für Level-2-Unternehmen.
- **Level 4:** Zu dieser Gruppe zählen alle Unternehmen, die weniger als 20.000 Online-Transaktionen (also Buchungs- oder Bestellvorgänge, bei denen Karteninhaberdaten per Internet übermittelt werden) vornehmen, sowie alle anderen Unternehmen, die bis zu einer Million Kartenzahlungen abwickeln, unabhängig von Zahlungsweg und -methode.

Unternehmen, die im Jahr vor der Einstufung Opfer einer Hackerattacke wurden und dabei Daten verloren haben, können jeweils der nächsthöheren Sicherheitsstufe zugeschlagen werden.

Service Provider teilt PCI einer der drei folgenden Kategorien zu:

- **Level 1:** Dieser Gruppe gehören alle sog. *VisaNet Processors* an (also Provider, die Kartentransaktionen für *Visa* abwickeln, unabhängig von ihrer PCI-Mitgliedschaft); außerdem alle *Payment Gateways*, d. h. Provider, die als Vermittler zwischen zwei Stellen innerhalb des *Visa*-Netzwerks auftreten. Alle Angehörigen dieser Gruppe müssen sich einmal jährlich einer Vor-Ort-Überprüfung durch eine QSDC sowie alle drei Monate einem Netzwerk-Scan durch einen ASV unterziehen.
- **Level 2:** Dieser Gruppe unterfallen alle Service Provider, die nicht zur ersten Kategorie zählen und mindestens eine Million Transaktionen pro Jahr abwickeln bzw. Daten von mindestens einer Million Kunden speichern. Es gelten die gleichen Kontrollvorgaben wie bei Level 1.
- **Level 3:** Hierzu zählen alle Service Provider, die nicht zur ersten Gruppe gehören und deren Transaktionsaufkommen bzw. Datenbankgröße die Million unterschreitet. Anstelle einer QSDC-Prüfung erfolgt bei ihnen einmal jährlich ein internes Audit anhand eines Standardfragebogens; der vierteljährliche ASV-Scan ist auch hier Pflicht.

### **Mängel und Herausforderungen: die „Top Ten“ der wichtigsten Verstöße gegen PCI-Regeln**

Bei den bisher vorgenommenen PCI-Audits haben sich folgende Punkte als häufigste Fehlerquellen erwiesen, die eine Zertifizierung der geprüften Unternehmen verhinderten:

- unzulässige Speicherung von Daten wie PIN, Kreditkarten-Prüfnummer (CVV2) etc.;
- nicht gepatchte bzw. unzureichend gewartete Systeme;
- Verwendung von Standardeinstellungen und -passwörtern der Hardwarehersteller;
- unsichere Web-Anwendungen (z. B. offen für SQL-Injection-Angriffe);
- überflüssige und verwundbare Dienste und Server;
- schwache Verschlüsselung und fehlende Benutzerauthentifizierung;
- fehlender oder unzureichender Schutz bei Verarbeitung der im Magnetstreifen gespeicherten Kundeninformationen (sog. *Track Data*);
- fehlerhaftes Change Management;
- unzureichende Audits und fehlende Durchsetzung von Sicherheits- und Passwortregeln;
- fehlende Absicherung von Mobilgeräten und Drahtlosnetzwerken.

### **SonicWALL und der PCI-Standard**

Als Anbieter von Security-Lösungen war SonicWALL daran interessiert herauszufinden, ob zwei Software-Produkte des Hauses den Sicherheitsanforderungen der Kreditkartengesellschaften genügen: zum einen die Management-Plattform *Global Management System* (SonicWALL GMS), zum anderen das Betriebssystem SonicOS in der Standard- ebenso wie in der Enhanced-Version, das auf den Network Security Appliances der Modellreihen TZ, PRO und NSA läuft. Zu diesem Zweck wurde standardkonform ein unabhängiger, zertifizierter Gutachter (PCI Qualified Security Assessor – QSA) mit der Prüfung beauftragt. Das Ergebnis zeigt, dass SonicWALL-Lösungen bei entsprechender Konfiguration und Implementierung die Anforderungen des PCI-Standards erfüllen.

Um die Umsetzung solcher IT-Projekte zu erleichtern und ihren Rollout zu beschleunigen, hat SonicWALL darüber hinaus einen dreibändigen *Implementation Guide* vorgelegt, der die wichtigsten Installations- und Konfigurationseinstellungen in SonicWALL GMS und SonicOS erläutert. Auch diese Konfigurationsvorgaben wurden von einem unabhängigen Gutachter geprüft und freigegeben.

## SonicWALL GMS und PCI: Welche Anforderungen sind abgedeckt?

Einrichtung und Unterhaltung eines sicheren Netzwerks	
Anforderung 1	Einrichtung und Betrieb einer Firewall zum Schutz von Karteninhaberdaten
Anforderung 2	Keine Verwendung der Standardwerte des Herstellers für Systemkennwörter und andere Sicherheitsparameter
Schutz von Karteninhaberdaten/Kundeninformationen	
Anforderung 3	Schutz gespeicherter Kundendaten; Verzicht auf die überflüssige Speicherung von Karten- und Transaktionsdaten
Anforderung 4	Verschlüsselung der Karteninhaberdaten und anderer sensibler Informationen bei Übertragung über öffentliche Netzwerke
Einhaltung eines Programms zur Abwehr von Sicherheitsrisiken	
Anforderung 5	Verwendung und regelmäßige Wartung/regelmäßiges Upgrade sicherer Systeme und Anwendungen sowie von Schutzprogrammen (z. B. AV-Software)
Anforderung 6	Entwicklung und Betrieb sicherer Systeme und Anwendungen
Implementierung strikter Zugriffsregeln	
Anforderung 7	Beschränkung des Zugriffs auf Karteninhaberdaten auf das für Transaktionen erforderliche Mindestmaß
Anforderung 8	Zuweisung einer eindeutigen ID/Kennung zu jeder Person mit Computerzugriff
Anforderung 9	Einschränkung des physischen Zugangs zu Karteninhaberdaten <sup>1</sup>
Regelmäßige Überwachung und Prüfung von Netzwerken	
Anforderung 10	Nachverfolgung und Überwachung sämtlicher Zugriffe auf Netzwerkressourcen und Karteninhaberdaten
Anforderung 11	Regelmäßige Tests von Sicherheitssystemen und -prozessen
Einhaltung unternehmensweiter Informationssicherheitsrichtlinien	
Anforderung 12	Einführung und Durchsetzung strenger Sicherheitsprinzipien und -maßnahmen

■ Die in diesem Text erwähnten SonicWALL-Lösungen unterstützen alle rot hinterlegten Anforderungen.

<sup>1</sup> Gilt für CDP-Systeme mit einer vor Ort installierten Appliance oder mit Offsite-Backup-Services, bei denen Primary Account Numbers (PAN) gespeichert werden.

<sup>2</sup> Bei Verwendung starker Codierschlüssel und Sicherheitsprotokolle, wie sie von SonicWALL unterstützt werden, ist dies in erster Linie eine Konfigurationsfrage.

### SonicWALL GMS: solides Fundament für PCI-Compliance

Die preisgekrönte Management-Software SonicWALL GMS ermöglicht die zentralisierte Verwaltung von Sicherheitsregeln in verteilten Umgebungen nebst einem zentralen, auf PCI-Erfordernisse zugeschnittenen Reporting und unterstützt Redundanz/Hochverfügbarkeit sowie Load Balancing. Sicherheitsvorgaben werden zentral erstellt und ihre Einhaltung in Echtzeit überwacht, zudem lassen sich jederzeit Prüf- und Nutzungsberichte erstellen – alles über eine einzige Schnittstelle. Auf diese Weise bietet GMS ein umfassendes Fundament für die Einführung des PCI-konformer Regularien und somit die PCI-Compliance.

Überdies hat SonicWALL GMS in der neuesten Edition um einige wichtige Komponenten erweitert, die die Einhaltung von Version 1.1 des PCI-Standards verbessern sollen. Insbesondere lässt sich das zentralisierte Management und Reporting nun auch auf die Network Security (NSA)-, SSL-VPN- und Continuous Data Protection (CDP)-Appliances ausdehnen. Administratoren können alle Appliances über ein einheitliches Interface konfigurieren, ihnen Aufgaben zuweisen und Berichte abrufen – in kleinen Installationen mit maximal zehn Geräten ebenso wie in großen mit mehreren tausend. Das spart Arbeitszeit bei der Einführung PCI-konformer Regelwerke. Unabhängig vom jeweiligen Compliance-Projekt bietet GMS damit vier wichtige Kernfunktionen, die jeder Sicherheitsarchitektur

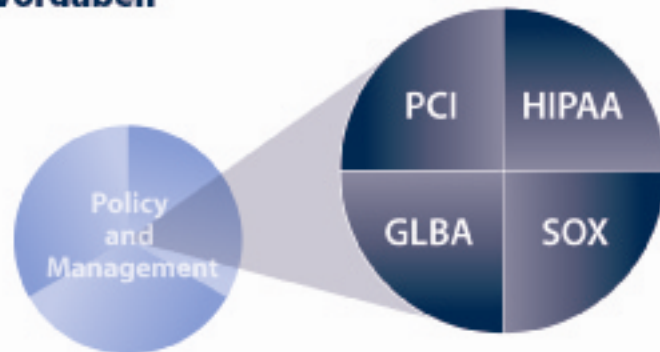
zugute kommen: zentrale Verwaltung, strenge Zugriffskontrollen, umfassende Protokollierung sowie die Möglichkeit, dynamisch und flexibel auf Sicherheitsrisiken zu reagieren.

GMS hat sich als hochgradig effektives Werkzeug erwiesen, das Unternehmen erlaubt, eine ganze Reihe von PCI-Regeln umzusetzen und damit das Bestehen der einschlägigen Auditverfahren beträchtlich erleichtert.

## GMS unterstützt zuverlässig die Einhaltung von Compliance-Voraben

### GMS bietet Policy- und Management-Funktionen:

- zentralisierte Verwaltung (verschlüsselt und authentifiziert)
- strenge Zugriffskontrolle (Lesen, Schreiben, etc.)
- umfassende Audit-Trails (Überwachung, Reporting, Anmeldung)
- dynamisches Vulnerability Management (UTM-Abos)



Im Folgenden geben wir einige Beispiele für Vorgaben des PCI DSS, die sich mit SonicWALL GMS besonders effektiv erfüllen lassen:

- **Passwortschutz auf Admin-Ebene:** Nach jeder Neuinstallation fordert das System den Administrator beim ersten Login auf, das Passwort für seinen Account zu ändern.
- **Passwortschutz auf User-Ebene:** Unabhängig von der Gruppenzugehörigkeit erscheint bei jedem ersten Login ein Prompt mit der Aufforderung, das Account-Passwort zu ändern.
- **Zeitlich begrenzte Accounts:** Mit Hilfe eines Kalenders kann der Administrator ein Verfalls- bzw. Löschdatum für Accounts mit begrenzter Laufzeit festlegen – auf Ebene der Gruppen wie der einzelnen User.
- **Nicht genutzte Accounts:** Die GMS-Benutzeroberfläche bietet zwei Werkzeuge für das automatische Löschen inaktiver Accounts.
- **Zeitgesteuerte Zugriffsbegrenzung:** GMS ermöglicht Administratoren, User-Zugriffe auf bestimmte Tageszeiten und Wochentage zu begrenzen.
- **Regelmäßige Passwortänderung:** GMS enthält einen Mechanismus, der User dazu zwingt, ihr Login-Passwort nach 90 Tagen bzw. einer individuell festgelegten Frist zu wechseln.
- **Passwortlänge und verwendete Zeichen:** GMS stellt sicher, dass alle Passwörter mindestens sieben Zeichen umfassen und sowohl Buchstaben als auch Zahlen enthalten, was größtmöglichen Schutz gegen alle Standardattacken bietet.
- **Erneuerung/Austausch von Passwörtern:** Ein weiterer GMS-Mechanismus sorgt dafür, dass sich jedes neu gewählte Passwort von jedem der vier vorangegangenen unterscheidet.
- **Zugriffssperre nach gescheitertem Login:** GMS sperrt jeden Account nach sechs oder weniger gescheiterten Login-Versuchen für 30 Minuten.

Diese Funktionen bieten Schutz gegen Fehlkonfigurationen sowie Flüchtigkeitsfehler bei der Festlegung von Account-/User-Berechtigungen, der Datenbankverschlüsselung und der Durchsetzung starker Authentifizierungs- und Verschlüsselungsverfahren für Remote-Systeme. Administratoren können jedes einzelne Feature an die individuellen Anforderungen ihres Unternehmens anpassen. Um zu gewährleisten, dass Erweiterungen und Verbesserungen des Standards möglichst schnell in die genannten Sicherheitsplattformen eingehen, arbeitet SonicWALL überdies eng mit den Kartengesellschaften und dem *PCI Security Standards Council* zusammen.

GMS bietet außerdem umfangreiche, stabile Berichtsfunktionen, darunter:

- zusammenfassende Reports zur Web-Nutzung, die u. a. Aufschluss darüber geben, wie viel HTTP-Traffic einzelne SonicWALL-Appliances an einem vorgegebenen Tag stündlich verarbeitet haben;

- Überblicke über die verarbeitete/übertragene Datenmenge pro Gerät;
- *Intrusion Prevention Reports*, die alle Einbruchsversuche über einen vordefinierten Zeitraum auflisten;
- Berichte zur Zahl und Art der wichtigsten Virusattacken, die gegen einzelne Appliances oder über diese erfolgten;
- *Attack Summary Reports*, die Zahl und Art aller Attacken auflisten, die gegen einzelne Appliances oder über diese erfolgten.

Die Automatisierung dieser Berichtsfunktionen ist eine der größten Herausforderungen bei der Einführung jedwedes gesetzlichen oder Branchenstandards bzw. darauf basierender Sicherheitsregeln. Zurzeit setzen viele Unternehmen dabei immer noch auf manuelle Verfahren, doch in der Automatisierung liegt der Schlüssel für eine wirklich umfassende Compliance.

## **Zusammenfassung**

PCI DSS ist die Antwort der Kreditkartenanbieter auf eine Form der Kriminalität, der sich alle Branchen ohne Ansehen der jeweils geltenden Regularien stellen müssen. Der Standard legt anerkannte Verfahren zur Erhöhung der Netzwerksicherheit fest, die in allen Umgebungen gelten sollten – nicht bloß bei Groß- und Einzelhändlern oder Dienstleistern, die Kreditkartendaten verarbeiten. Seine Einhaltung verspricht einen geschäftlichen Nutzen, der über die Vermeidung empfindlicher Geldbußen weit hinausgeht.

Das SonicWALL Global Management System (SonicWALL GMS) bietet eine solide Grundlage, um den PCI-Standard einzuhalten und entsprechende Audits zu bestehen. GMS fasst die Aufgaben des Netzwerk- und Sicherheitsmanagements in einer zentralen Steuerkonsole/Steuerungseinheit zusammen, mit deren Hilfe sich ein verteiltes Netzwerk von jedem beliebigen Ort aus zentral verwalten und überwachen lässt. Auf diese Weise kann der Administrator regeln für Netzwerkdienste und -sicherheit festlegen, einführen und durchsetzen, die entweder für einen Standort oder für tausende verteilter SonicWALL-Appliances gelten. Ausgereifte Werkzeuge für den Aufbau und die Konfiguration von VPNs helfen Unternehmen dabei, den normalerweise damit verbundenen Arbeitsaufwand, die Komplexität der Aufgabe sowie die notwendigen Investitionen gering zu halten. Dienstleistungsunternehmen erhalten mit GMS die Möglichkeit, für eine Vielzahl von Kunden maßgeschneiderte Sicherheitsprofile festzulegen.

SonicWALL GMS und SonicWALL-Appliances, die unter der Standard- oder der erweiterten Version des Betriebssystems SonicOS laufen, wurden von einem unabhängigen Gutachter (PCI Qualified Security Assessor – QSA) geprüft und akzeptiert. Damit ist sichergestellt, dass sie sich als technische Kontrollkomponente für alle Netzwerke eignen, in denen der PCI-Standard gelten soll.

## **Über SonicWALL**

SonicWALL, Inc. wurde 1991 gegründet und entwickelt seitdem Internet-Sicherheitslösungen für Unternehmen und Organisationen in aller Welt. Zum Produktportfolio gehören u. a. Schutz- und Filterprogramme für E-Mail-Systeme, VPN-Appliances, Content-Filter sowie Lösungen für Continuous Data Protection (CDP) und das regelbasierte Netzwerk-Management. SonicWALL ist einer der führenden Anbieter im KMU-Markt; seine Produkte werden aber auch in größeren Unternehmen, bei Behörden, im Einzelhandel, im Gesundheitswesen oder bei ISPs eingesetzt.