

Implementierung des PCI DSS leicht gemacht

Hinweise zur Umsetzung des Payment Card Industry Data Security Standard (PCI DSS)

Die weltweit wichtigsten Kreditkartenunternehmen versuchen mit Hilfe neuer Maßnahmen, den wachsenden Missbrauch von Kreditkartendaten zu unterbinden. Durch die Einführung der strengen Sicherheitsvorgaben des PCI DSS sollen Karteninhaber wie Unternehmen noch besser vor Betrug und Identitätsdiebstahl geschützt werden. Das neue Regelwerk ist ab Ende 2007 für Unternehmen, die im Zahlungsverkehr mit Kreditkartendaten arbeiten, verbindlich. Wird der neue Standard nicht umgesetzt, kann die Akzeptanz von Kreditkartendaten untersagt werden. Darüber hinaus drohen empfindliche Strafen in sechsstelliger Höhe, wenn Daten verloren gehen oder gestohlen werden. In diesem White Paper werden die Anforderungen zur Erfüllung des PCI DSS erläutert, welche Auswirkungen seine Nichtumsetzung hat und wie effektives Ereignisprotokoll- und Schwachstellen-Management einen bedeutenden Beitrag zur PCI DSS-Compliance leisten.

Einführung

Kreditkarten sind ein gängiges Zahlungsmittel, das vor allem beim Einkauf im Internet immer beliebter wird. Allein in den USA waren im Jahr 2004 1,3 Mrd. Kreditkarten im Umlauf. 76 Prozent aller Amerikaner besitzen mindestens eine Kreditkarte. Der Einzelhandel in den USA verzeichnete im vierten Quartal 2006 E-Commerce-Umsätze in Höhe von 33,9 Mrd. Dollar – eine Steigerung von 25 Prozent gegenüber dem Vergleichszeitraum des Vorjahres.

Doch wo Licht ist, ist auch Schatten: Mit 25 Prozent nimmt der Kreditkartenbetrug den größten Anteil an den im Jahr 2006 verzeichneten Fällen von Identitätsdiebstahl ein, durch den Finanzinstituten und Unternehmen Verluste in Höhe von mehr als 48 Mrd. US-Dollar entstanden. Privatpersonen mussten einen Schaden in Höhe von 5 Mrd. US-Dollar hinnehmen. Identitätsdiebstahl hat sich somit zu einem Problem entwickelt, das sich auf die gesamte Gesellschaft auswirkt. Auch die Zahl der Betrugsfälle im E-Commerce nimmt weiter zu. Nach einer siebenprozentigen Steigerung gegenüber dem Jahr 2005 lag der Schaden im Jahr 2006 bereits bei 3 Mrd. US-Dollar.

Mit diesem White Paper sollen die Folgen des Diebstahls der Daten von Kreditkarteninhabern näher betrachtet und folgende wesentliche Fragen beantwortet werden:

- Worum handelt es sich beim PCI-Regelwerk?
- Warum ist PCI-Compliance für Ihr Unternehmen von Bedeutung?
- Welche Konsequenzen sind bei Nichteinhaltung des Sicherheitsstandards zu erwarten?
- Welche Lösungen sorgen für PCI-Compliance?

Kreditkartendaten in Gefahr: aktuelle Diebstahl- und Betrugsfälle

- 18. Februar 2005 – Die Bank of America gibt den Verlust von mehr als 1,2 Millionen Kundendaten bekannt. Es gebe jedoch keine Hinweise, dass die Daten in die Hände von Kriminellen gelangten, so die Bank.
- Juni 2005 – Gegen den US-Dienstleister CardSystems, der für Händler Zahlungen mit Kreditkartendaten abwickelt, wird Klage erhoben, die persönlichen Daten von rund 40 Millionen Kunden nicht hinreichend geschützt zu haben. Die durch den Diebstahl betroffenen Kreditkartenunternehmen VISA und American Express beenden ihre Geschäftsbeziehung mit CardSystems und untersagen dem Unternehmen die weitere Verarbeitung ihrer Kartendaten. Die Folge: CardSystems gerät in finanzielle Schwierigkeiten und wird aufgekauft.
- 9. Februar 2006 – Unbekannte US-Einzelhändler, mutmaßlich OfficeMax und andere Händler, haben Kontodaten von geschätzt rund 200.000 amerikanischen Debit-Karten öffentlich zugänglich gemacht. Betroffen sind Konten von Händlerbanken und Finanzdienstleistern in den ganzen USA, wie von der CitiBank und Wells Fargo.
- 31. Januar 2006 – Die US-Tageszeitungen Boston Globe und The Worcester Telegram & Gazette sorgen für eine besondere Art von Enthüllung, als sie die Kreditkartendaten von über 240.000 Abonnenten mit ihren Zeitungspaketen ausliefern. Die sensiblen Informationen sind auf Papier gedruckt, das wiederverwendet wurde, um die druckfrischen Ausgaben einzuwickeln.
- 12. Januar 2007 – MoneyGram, Dienstleister für internationale Geldüberweisungen, muss eingestehen, dass Unbekannte sich über das Internet Zugriff auf einen Firmen-Server verschafft haben. Zugänglich wurden dadurch Daten von etwa 79.000 Rechnungszahlern, darunter Name, Anschrift, Telefonnummer und in einigen Fällen sogar Kontonummern.
- 17. Januar 2007 – Die Kaufhauskette TJX Companies Inc. gibt öffentlich bekannt, dass sein Datenverarbeitungssystem für Kreditkartendaten gehackt wurde. Im bisher unrühmlichsten Fall von Datenschutzverletzung werden ganze 45,7 Millionen Kreditkarten-Datensätze und über 455.000 Kundenunterlagen zur Warenrückgabe (samt Kundenname und Führerscheindaten) gestohlen.

Opfer von Datendiebstahl werden längst nicht mehr nur bedeutende Online-Händler. Die öffentlich bekannt gemachten Fälle erregen wegen ihres Ausmaßes großes Aufsehen, doch stellen Experten für Finanzbetrug einen wachsenden Anstieg bei Angriffen auf kleine kommerzielle Websites fest. Teilweise gelingt es Kriminellen, über die Website laufende kreditkartenrelevante Transaktionen in Echtzeit abzuschöpfen, um so an gültige Kartennummern zu gelangen – und dann zu Lasten des Opfers auf Einkaufstour zu gehen. Bei kleineren Online-Händlern ist oftmals kein großer Kundenstamm betroffen, dennoch sind sie als "weiche Ziele", die leichter zu schädigen sind, beliebt. Fehler in der Software des Online-Shops oder ein allzu großes Vertrauen in externe Dienstleister, die mit dem Website-Schutz beauftragt sind, vereinfachen die Angriffe.

Cybercrime und die lauenden Gefahren durch Identitätsdiebstahl wirken sich negativ auf das Kunden- und Konsumentenvertrauen aus und bewirken, dass dem E-Commerce immer noch mit großem Misstrauen begegnet wird. Der Schutz von Informations- und Datenverarbeitungssystemen im Rahmen der Computer-Sicherheit steht daher zurecht im öffentlichen Interesse.

Das Regelwerk der Payment Card Industry (PCI)

Das Regelwerk der PCI zum Schutz von Kreditkartendaten wurde von den Kreditkartenfirmen American Express, Discover Financial Services, JCB, MasterCard Worldwide und VISA International erstellt. Vor dem Jahr 2004 hatte jedes dieser Unternehmen eigene Sicherheitsvorschriften – für Händler, die verschiedene Karten akzeptieren, bedeutete dies häufig einen erheblichen Aufwand an Verwaltungsarbeit. Mit der Einführung des PCI DSS wurde ein von allen beteiligten Kreditkartenfirmen getragener, einheitlicher Sicherheitsstandard mit Anforderungen ins Leben gerufen, die für die gesamte Kartenzahlungsbranche gelten (Kartenmodelle privater Anbieter ausgenommen). Der PCI DSS gilt für Kreditkartentransaktionen im Einzelhandel sowie per Post, Telefon und E-Commerce.

Das PCI DSS-Regelwerk

Das PCI DSS-Regelwerk zum Schutz von Kreditkartendaten umfasst zwölf Sicherheitsanforderungen (von VISA als "Digitales Dutzend" bezeichnet), die in sechs Kategorien eingeteilt sind:

PCI DSS
Einrichtung und Wartung eines geschützten Netzwerks
Anforderung 1: Einrichtung und Wartung einer Firewall zum Schutz der Daten von Kreditkarteninhabern Anforderung 2: Änderung der von Herstellern vorgegebenen Standardpasswörter und Sicherheitseinstellungen
Schutz der Daten von Kreditkarteninhabern
Anforderung 3: Schutz der gespeicherten Daten von Kreditkarteninhabern Anforderung 4: Verschlüsselte Übertragung der Daten von Kreditkarteninhabern in öffentlichen Netzwerken
Einrichtung eines Schwachstellen-Management-Systems
Anforderung 5: Einsatz und regelmäßige Aktualisierung von Virenschutzlösungen Anforderung 6: Entwicklung und Verwendung sicherer Systeme und Anwendungen
Umsetzung effektiver Richtlinien zur Zugriffskontrolle
Anforderung 7: Einschränkung des Zugriffs auf Kreditkartendaten nach dem Grundsatz "Kenntnis, nur wenn nötig". Anforderung 8: Zuweisung einer eindeutigen Benutzerkennung an jede Person mit Zugang zum Computersystem Anforderung 9: Einschränkung des physikalischen Zugriffs auf Daten von Kreditkarteninhabern
Regelmäßige Überwachung und Überprüfung des Netzwerks
Anforderung 10: Protokollierung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen und Daten von Kreditkarteninhabern Anforderung 11: Regelmäßige Überprüfung von Sicherheitssystemen und -abläufen
Formulierung und Durchsetzung einer Richtlinie zur Informationssicherheit
Anforderung 12: Einrichtung einer Unternehmensrichtlinie mit Vorgaben zur Informationssicherheit für Mitarbeiter und Vertragspartner

Tabelle 1: Das PCI DSS-Regelwerk

Die Umsetzung dieser Anforderungen kann zusammengefasst in drei Hauptbereichen erfolgen:

- **Erfassung und Speicherung:** Sichere Erfassung und fälschungssichere Speicherung aller Protokoll Daten als Vorbereitung für Sicherheitsanalysen.
- **Reporting:** Berichterstellung und -vorlage zum sofortigen Compliance-Nachweis im Fall einer Auditierung vor Ort und Nachweis über implementierte Maßnahmen zum Datenschutz.
- **Überwachung und Benachrichtigung:** Einsatz von Systemen zur kontinuierlichen Überwachung von Datenzugriff und -verwendung mit automatischem Versand von Warnungen an Administratoren: Bei Problemen wird sofort eine Benachrichtigung verschickt,

um rasche Gegenmaßnahmen zu ermöglichen. Protokolldaten sind ebenfalls zu berücksichtigen – die Erfassung und Speicherung von Protokolldaten muss nachweisbar sein.

PCI DSS-Kategorisierung von Händlern und Dienstleistern

Zur Einhaltung des PCI DSS verpflichtete Händler und Dienstleister werden abhängig von der in einem Zwölfmonatszeitraum abgewickelten Zahl von Kreditkartentransaktionen in unterschiedliche Kategorien eingestuft. Die nachfolgenden Tabellen 2 und 3 informieren über die einzelnen Kategorien und Compliance-Anforderungen für Händler und Dienstleister.

Autorisierte **Händler** sind dazu befugt, Kreditkarten zur Zahlung von Waren und Dienstleistungen zu akzeptieren. Händler aus beispielsweise folgenden Branchen müssen die Vorgaben des PCI DSS einhalten:

- Online-Handel, z. B. Internet-Buchhändler
- Einzelhandel, z. B. Kaufhausketten
- Bildungseinrichtungen, z. B. Universitäten
- Gesundheitswesen, z. B. Krankenhäuser
- Hotel- und Gaststättengewerbe sowie Freizeitbranche
- Energieversorgung, z. B. Tankstellenbetreiber
- Finanzunternehmen, z. B. Banken und Versicherungen

HÄNDLERKATEGORIEN	
DEFINITION DER HÄNDLERKATEGORIE*	EINHALTUNG DER PCI DSS-COMPLIANCE
Kategorie 1	
<ul style="list-style-type: none"> • Händler, deren verwaltete Kreditkartendaten kompromittiert wurden • Händler mit jährlich mehr als sechs Millionen Kreditkartentransaktionen über alle Verkaufskanäle, darunter auch E-Commerce 	Jährliche PCI-Sicherheitsauditierung vor Ort und vierteljährliche Sicherheits-Scans des Netzwerks
Kategorie 2	
<ul style="list-style-type: none"> • Händler mit 1-6 Millionen Kreditkartentransaktionen/Jahr 	Jährliche Beantwortung eines PCI-Fragebogens und vierteljährliche Netzwerk-Sicherheits-Scans
Kategorie 3	
<ul style="list-style-type: none"> • Händler mit 20.000 bis 1.000.000 Million E-Commerce-Kreditkartentransaktionen/Jahr 	Jährliche Beantwortung eines PCI-Fragebogens und vierteljährliche Netzwerk-Sicherheits-Scans
Kategorie 4**	
<ul style="list-style-type: none"> • Alle anderen Händler 	Jährliche Beantwortung eines PCI-Fragebogens und jährlicher Netzwerk-Sicherheits-Scan

Tabelle 2: Händlerkategorien

* Definition der Händlerkategorien gemäß Vorgaben von VISA USA

** Zur Einhaltung der Vorschriften des PCI DSS müssen alle Händler externe Netzwerk-Scans durchführen lassen. Händlerbanken fordern von Kategorie 4-Händlern ggf. die Vorlage der Scan-Berichte und/oder Fragebögen.

Zu den **Dienstleistern** zählen Organisationen, die Daten von Kreditkarteninhabern im Auftrag von Mitgliedern eines Kartenverbands, Händlern oder anderen Dienstleistern verarbeiten, speichern oder weiterleiten. Unter anderem müssen folgende Dienstleister die Vorgaben des PCI DSS einhalten:

- Payment-Gateways*
- Host-Provider im E-Commerce
- Managed-Service-Provider
- Auskunfteien
- Backup-Management-Unternehmen
- Datenvernichter

DEFINITION DER DIENSTLEISTER-KATEGORIE (EXEMPLARISCH)	MASSNAHMEN ZUR PCI DSS-COMPLIANCE
Kategorie 1	
Alle von Händlerbanken und Händlern beauftragten Datenverarbeiter von Kreditkartenzahlungen und Payment-Gateways	Jährliche PCI-Sicherheitsauditierung vor Ort und vierteljährliche Sicherheits-Scans des Netzwerks
Kategorie 2	
Jeder nicht zur Kategorie 1 zählende Dienstleister, der jährlich mehr als 1 Million Kreditkartenkonten/-transaktionen speichert, verarbeitet oder übermittelt.	Jährliche PCI-Sicherheitsauditierung vor Ort und vierteljährliche Sicherheits-Scans des Netzwerks
Kategorie 3	
Jeder nicht zur Kategorie 1 zählende Dienstleister, der jährlich weniger als 1 Million Kreditkartenkonten/-transaktionen speichert, verarbeitet oder übermittelt.	Jährliche Beantwortung eines PCI-Fragebogens und vierteljährliche Sicherheits-Scans des Netzwerks

Tabelle 3: Dienstleister-Kategorien

* Als Payment-Gateway wird ein bei Zahlungsvorgängen als Schnittstelle fungierender Auftraggeber oder Dienstleister bezeichnet, der Daten von Kreditkarteninhabern speichert, verarbeitet und/oder übermittelt (z. B. PayPal). Der Payment-Gateway unterstützt Transaktionen (wie Zahlungsautorisierung oder Zahlung) zwischen Händlern und Verarbeitungssystemen für Zahlungsvorgänge (z. B. VisaNet). Händler können Zahlungen direkt mit dem Verarbeitungssystem oder über einen Payment-Gateway abwickeln.

Strenge Compliance-Fristen

Große Kreditkartenunternehmen fordern Händler nachdrücklich dazu auf, den PCI DSS umzusetzen. Verschiedene verbindliche Zielvorgaben sollen für eine fristgerechte Implementierung des PCI DSS sorgen – werden diese Vorgaben nicht eingehalten, drohen empfindliche Strafen.

Zu den wichtigsten durch VISA USA gesetzten Fristen zählen:

- 31. März 2007 – Datum, bis zu dem Händler der Kategorie 1 und 2 belegen müssen, dass sie die vollständige Kartenummer, Daten der Magnetstreifen Spuren, Kartenverifizierungscode (CVV2) und PIN-Nummer nicht speichern.
- 30. September 2007 – Datum, bis zu dem alle Händler der Kategorie 1 den PCI DSS vollständig umgesetzt haben müssen.
- 31. Dezember 2007 – Datum, bis zu dem alle Händler der Kategorie 2 den PCI DSS vollständig umgesetzt haben müssen.

Compliance-Fristen sind je nach Kreditkartenunternehmen und Land verschieden. Händler und Dienstleister sollten sich daher mit Händlerbanken oder Kartenunternehmen in Verbindung setzen, um Informationen zu dem für sie verbindlichen Datum zu erfragen.

Warum ist PCI-Compliance für Ihr Unternehmen von Bedeutung?

PCI DSS hat seinen Ursprung in den USA, gilt jedoch weltweit für jede Organisation, die mit Kreditkartendaten arbeitet. Diese Tatsache ist vielfach noch unbekannt. Beispielsweise ist es in der australischen Bankbranche durch die unzureichende Aufklärung über neue Compliance-Maßnahmen allein im Jahr 2006 zu fünf Verstößen gegen den PCI DSS gekommen.

Händlerbanken sollten aus eigenem Interesse darauf achten, dass Händler den PCI DSS kennen und damit konform gehen. Das Vertrauen zwischen Kreditkartenunternehmen und Händlern wird hauptsächlich durch Händlerbanken aufgebaut. Treten jedoch Missstände oder Sicherheitsdefizite bei Händlern auf, werden zuerst die Banken für Probleme zur Verantwortung gezogen. Für eine dauerhaft erfolgreiche Geschäftsbeziehung zu Kreditkartenunternehmen müssen Händlerbanken somit dafür Sorge tragen, dass ihre Händler geschützt sind und Maßnahmen zur Sicherung von Kreditkartendaten korrekt implementiert haben.

Von Händlern und Dienstleistern wird ein regelmäßiger Nachweis darüber erwartet, wie sie die Vorgaben des PCI DSS einhalten. Schwierigkeiten aufgrund von fehlender Compliance lassen sich dadurch rechtzeitig erkennen, und Händler bestätigen das in sie gesetzte Vertrauen der Händlerbanken.

Welche Konsequenzen sind bei Nichteinhaltung des Sicherheitsstandards zu erwarten?

Kreditkartenunternehmen können ihre Händlerbanken mit empfindlichen Strafen belegen, sollten Händler die Sicherheitsvorschriften der PCI nicht eingehalten haben. Händler wiederum sind unter Umständen gegenüber den Banken vertraglich verpflichtet, diese von schadlos zu halten und für Schäden aufzukommen. Die Konventionalstrafe kann bis zu 500.000 US-Dollar pro Missbrauchsfall betragen, wenn Daten aufgrund der Nichteinhaltung von Sicherheitsstandards kompromittiert wurden. Im schlimmsten Fall kann Händlern zudem die Akzeptanz von Kreditkarten untersagt werden.

Unternehmen, die eine Kompromittierung der von ihnen verwalteten Kreditkartendaten feststellen, sind dazu verpflichtet, Anzeige zu erstatten und potenziell betroffenen Kunden kostenfreie Hilfe beim Kontoschutz zu gewähren.

Neben Strafzahlungen gibt es jedoch Konsequenzen, die ebenso schwer wiegen: Der Verlust von Kartendaten, ob durch Nachlässigkeit oder Diebstahl, kann zu Klagen durch Karteninhaber führen. Eine öffentliche Berichterstattung schlägt sich dann möglicherweise wiederum in Umsatzeinbußen nieder.

Welche Lösungen zur Einhaltung der PCI-Anforderungen bietet GFI?

Die Einhaltung einiger PCI-Anforderungen lässt sich mit Hilfe von Software-Lösungen automatisieren. Sie überwachen, ob PCI DSS-Compliance gewährleistet ist und warnen bei sicherheitskritischen Ereignissen im Zusammenhang mit Kreditkartendaten. GFI bietet mehrere Tools, die Unternehmen bei dieser Aufgabe unterstützen:

GFI EventsManager, GFI LANguard Network Security Scanner (N.S.S.) und GFI EndPointSecurity, drei mehrfach ausgezeichnete Netzwerksicherheitslösungen. Funktionen zur Auditierung, Überwachung, Berichterstellung und Benachrichtigung helfen Ihnen bei der Umsetzung mehrerer Aspekte von neun der zwölf PCI-Anforderungen, wie die nachfolgende Tabelle 4 verdeutlicht.

ANFORDERUNGEN DES PCI DSS			
	GFI EventsManager	GFI LANguard N.S.S.	GFI EndPointSecurity
1. Einrichtung und Wartung einer Firewall zum Schutz der Daten von Kreditkarteninhabern	•	•	
2. Änderung der von Herstellern vorgegebenen Standardpasswörter und Sicherheitseinstellungen	•	•	
3. Schutz der gespeicherten Daten von Kreditkarteninhabern	•		•
4. Verschlüsselte Übertragung der Daten von Kreditkarteninhabern in öffentlichen Netzwerken			
5. Einsatz und regelmäßige Aktualisierung von Virenschutzlösungen		•	
6. Entwicklung und Verwendung sicherer Systeme und Anwendungen		•	
7. Einschränkung des Zugriffs auf Kreditkartendaten nach dem Grundsatz "Kenntnis, nur wenn nötig".	•		
8. Zuweisung einer eindeutigen Benutzerkennung an jede Person mit Zugang zum Computersystem	•	•	
9. Einschränkung des physikalischen Zugriffs auf Daten von Karteninhabern			
10. Protokollierung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen und Daten von Kreditkarteninhabern	•	•	
11. Regelmäßige Überprüfung von Sicherheitssystemen und -abläufen	•	•	•
12. Einrichtung einer Unternehmensrichtlinie mit Vorgaben zur Informationssicherheit für Mitarbeiter und Vertragspartner			

Tabelle 4: Anforderungen des PCI DSS

GFI EventsManager

Die Analyse von Ereignisdaten ist in Anforderung 10 der obigen Tabelle 4 festgelegt. Ungeachtet ihrer Branche sollten Organisationen die Überwachung von Ereignissen generell in den Netzwerk-Sicherheitsschutz aufnehmen.

Ereignisdaten können in normalen Netzwerken an den unterschiedlichsten Orten zu finden sein, sind sehr umfangreich und lassen zudem an Verständlichkeit wünschen. Tools zur Ereignisanalyse sind zwar bereits im Lieferumfang der meisten Betriebssysteme enthalten, doch lassen ihre in Umfang und Leistung begrenzten Funktionen zur Ereignisanzeige und -filterung nur sehr rudimentäre Untersuchungen zu. Administratoren fehlt zudem die Möglichkeit, sich bei kritischen oder speziellen Sicherheitsereignissen wie dem unautorisierten Zugriff auf Kreditkartendaten warnen zu lassen.

Als umfassende Verwaltungslösung für Ereignisprotokolle schafft GFI EventsManager Abhilfe. Ereignisse können zentral gesichert werden, und die Ereigniserfassung lässt sich automatisieren. Warnungen sowie detaillierte Analyseberichte informieren zudem über den aktuellen Sicherheitsstatus. Integrierte Regelsätze verarbeiten und klassifizieren von GFI EventsManager erfasste Ereignisse und sorgen dafür, dass Warnungen ausgegeben oder Aktionen eingeleitet werden. Einer der bereits mitgelieferten Regelsätze zielt insbesondere auf die Ereignisklassifizierung wie von der PCI gefordert ab. Der integrierte Events-Browser unterstützt darüber hinaus die Ereignisanalyse, die benutzerdefinierbar auch für spezifische Ereignisse erfolgen kann.

Mit GFI EventsManager können Unternehmen dafür sorgen, dass sämtliche Ereignisse mit Bezug zu Kreditkartendaten fortlaufend überwacht werden. Weitere Informationen und eine kostenfreie Testversion des Produkts stehen zur Verfügung unter <http://www.gfisoftware.de/de/eventsmanager/>.

GFI LANguard Network Security Scanner

Das Schwachstellen-Management spielt eine große Rolle bei Anforderungen 5 und 6 (siehe Tabelle 4 oben). Schwachstellen müssen jedoch auch in verschiedenen anderen Anforderungsbereichen aufgespürt werden können.

Mit GFI LANguard Network Security Scanner (N.S.S.) stehen die drei Stützpfeiler des Schwachstellen-Managements – Sicherheits-Scans, Patch-Management und Netzwerk-Audits – in einer integrierten Lösung zur Verfügung. Die Sicherheitslösung überprüft das gesamte Netzwerk auf über 15.000 Schwachstellen, zeigt sämtliche potenziellen Sicherheitsbedrohungen an und stattet Administratoren mit wichtigen Tools zur schnellen Bewertung und Behebung ermittelter Schwachstellen aus.

Systemverantwortliche stehen tagtäglich vor demselben großen Problem: Sicherheitsrelevante Aufgaben wie Schwachstellen-Scans, Patch-Management und Netzwerk-Audits müssen oft getrennt voneinander mit unterschiedlichen Lösungen bewältigt werden. Diese sind nicht nur

aufwendig zu installieren, erlernen und verwalten, auch die genaue Lokalisierung und Analyse der aufgespürten Probleme nimmt vielfach sehr viel Zeit in Anspruch. Zur eigentlichen Beseitigung der Gefahren kann es dann bereits zu spät sein. Dank der umfassenden Integration und leistungsfähigen Reporting-Funktionalität von GFI LANguard N.S.S. erhalten Administratoren die Möglichkeit, schneller und effektiver auf Schwachstellen zu reagieren.

Mit GFI LANguard N.S.S. können Unternehmen sicherstellen, dass die Netzwerkumgebung, in der Daten von Karteninhabern verwaltet werden, zuverlässig geschützt ist. Weitere Informationen und eine kostenfreie Testversion des Produkts stehen bereit unter <http://www.gfisoftware.de/de/lannetscan/>.

GFI EndPointSecurity

Der Schutz gespeicherter Daten von Kreditkarteninhabern muss sichergestellt sein, so die wichtige Anforderung 3 des PCI DSS (siehe Tabelle 4 oben). Unternehmen müssen daher unterschiedlichste Vorkehrungen treffen, dass vertrauliche Informationen keinesfalls in die falschen Hände geraten können.

Mobile Massenspeicher wie USB-Speichersticks haben in jüngerer Zeit immer mehr an Beliebtheit gewonnen. Sie lassen sich leicht und schnell mit Computern verbinden, besitzen eine große Speicherkapazität für Daten aller Art und passen aufgrund ihrer Kompaktheit sogar in jede Hemdtasche. Diese Eigenschaften können leicht für den Diebstahl von Daten und somit auch Kreditkarteninformationen missbraucht werden. Ohne entsprechende Schutzmaßnahmen lassen sich Inhalte im Handumdrehen und unbemerkt kopieren.

GFI EndPointSecurity schützt die Integrität von Daten und verhindert den unautorisierten Dateiaustausch über tragbare Speichermedien. Die Sicherheitslösung gestattet oder blockiert den Zugriff auf mobile Massenspeicher und erlaubt es darüber hinaus, lokalen oder Active Directory-basierten Benutzern/Gruppen gerätespezifischen Vollzugriff oder lediglich Leserechte zu erteilen. Die Verwendung sämtlicher an Netzwerkrechner angeschlossener mobiler Geräte lässt sich zudem mit Datum und Uhrzeit sowie der Angabe zum Gerätebenutzer protokollieren.

Mit GFI EndPointSecurity erhalten Unternehmen die Möglichkeit, sich vor der Übertragung von kreditkartenrelevanten Daten auf unerlaubte Speichermedien zu schützen. Weitere Informationen und eine kostenfreie Testversion des Produkts stehen zur Verfügung unter <http://www.gfisoftware.de/de/endpointsecurity/>.

GFI ReportCenter

GFI ReportCenter ist ein zentralisiertes Reporting-Framework und ermöglicht es, aus Daten, die von GFI EventsManager, GFI LANguard N.S.S. und GFI ReportCenter erfasst wurden, zahlreiche Arten von Berichten erstellen zu lassen. Für die drei GFI-Lösungen für Netzwerksicherheit stehen entsprechende ReportPack-Berichtmodule zur Verfügung, die nahtlos mit dem GFI ReportCenter-Framework integriert sind.

Zahlreiche vorkonfigurierte Berichte bieten grafisch aufbereitete Informationen für einen fundierten, anschaulichen Überblick über die Sicherheit des Netzwerks. Verwaltungsfunktionen zur Berichterstellung nach Zeitplan, zum Export und zum automatischen Berichtversand per E-Mail sorgen dafür, dass relevante Daten an Entscheidungsträger weitergeleitet werden. Nicht zuletzt lässt sich anhand der Berichte die Effektivität unternehmensinterner Vorgaben zur PCI-Compliance leicht überprüfen. Weitere Informationen und eine kostenfreie Download-Version des Produkts stehen zur Verfügung unter <http://www.gfisoftware.de/de/reportcenter/>.

Förderung der PCI-Compliance

Es liegt im eigenen Interesse der mit Kreditkartendaten arbeitenden Organisationen, die Richtlinien des PCI DSS einzuhalten. Ebenso haben Banken darauf zu achten, dass Händler mit den Regeln konform gehen.

Um die PCI-Compliance ihrer Händler zu fördern, ist beispielsweise vorstellbar, dass Banken bei Abschluss eines Akzeptanzpartner-Vertrags Lizenzen der Netzwerksicherheitslösungen von GFI kostengünstiger oder gratis anbieten. Zusätzliche von Seiten der Bank angebotene Services wie die Unterstützung der Händler mit technischem Know-how zu den GFI-Lösungen können das Angebot abrunden – zum Vorteil beider Vertragspartner. Händler hätten die Gewissheit, die Anforderungen des PCI DSS in weiten Teilen zu erfüllen und würden zudem vom Leistungsumfang der GFI-Lösungen profitieren, der weit über die Sicherheitsanforderungen der Kreditkartenunternehmen hinausgeht. Banken könnten sich ihrerseits gegenüber den Kreditkartenfirmen absichern, da bei ihren Händlern umfangreiche Maßnahmen zur Einhaltung des PCI-Sicherheitsstandards implementiert wären.

Zusammenfassung

Für Unternehmen besteht fortwährend das Risiko, Opfer von Datenverlust oder -diebstahl zu werden. Vertragsstrafen, Rechtsverfahren und negative Berichterstattung sind nur einige Konsequenzen, die bei der Kompromittierung von Daten drohen. Vor allem die daraus resultierenden Geschäftseinbußen können verheerend sein. Organisationen, die mit Kreditkartendaten arbeiten, sollten sich daher die Umsetzung der PCI DSS-Anforderungen zur dringlichsten Aufgabe machen.

Mit dem GFI-Produktportfolio für Netzwerksicherheit, das Ereignisprotokoll- und Schwachstellen-Management, Sicherheits-Scans und Endpunkt-Sicherheit bietet, ist bereits ein großer Schritt in Richtung PCI DSS-Compliance getan.

Über GFI Software

GFI Software bietet als führender Software-Hersteller eine umfassende Auswahl an Netzwerksicherheits-, Inhaltssicherheits- und Kommunikationslösungen aus einer Hand, um Administratoren einen reibungslosen Netzwerkbetrieb zu ermöglichen. Mit seiner mehrfach ausgezeichneten Technologie, einer konsequenten Preisstrategie und der Ausrichtung an den Anforderungen kleiner und mittlerer Unternehmen erfüllt GFI höchste Ansprüche an Effizienz und Produktivität. Das Unternehmen wurde 1992 gegründet und ist mit Niederlassungen auf Malta, in London, Raleigh, Hongkong, Adelaide sowie auf Hamburg vertreten und betreut über 200.000 Installationen weltweit. GFI bietet seine Lösungen über ein weltweites Netz von mehr als 10.000 Channel-Partnern an und ist Microsoft Gold Certified Partner. Weitere Informationen stehen zum Abruf bereit unter <http://www.gfisoftware.de>.

Quellenangaben

CreditCards.com (2006) *Credit Card Industry Facts and Personal Debt Statistics*, abrufbar unter: <http://www.creditcards.com/statistics/statistics.php> (zuletzt eingesehen am 29. Dezember 2006).

U.S. Census Bureau (2006) *Quarterly retail e-commerce sales 2nd quarter 2006*, abrufbar unter: <http://www.census.gov/mrts/www/data/html/06Q2.html> (zuletzt eingesehen am 29. Dezember 2006).

Federal Trade Commission (2006) *Consumer Fraud and Identity Theft Complaint Data January – December 2005*.

United States Postal Service *Identity Theft: Stealing Your Name and Your Money*, abrufbar unter: <http://www.usps.com/postalinspectors/IDtheft2.htm> (zuletzt eingesehen am 29. Dezember).

Bednarz A. (2006) *Online merchants will lose \$3 billion to fraud in 2006*, Network World, Inc., abrufbar unter: <http://www.networkworld.com/news/2006/111406-online-merchants-fraud.html?nlhtsec=1113securityalert2> (zuletzt eingesehen am 29. Dezember 2006).

Marlin S. (2005) *Customer Data Losses Blamed On Merchants And Software*, CMP Media LLC, abrufbar unter: <http://www.informationweek.com/showArticle.jhtml?articleID=161601930> (zuletzt eingesehen am 29. Dezember 2006).

Ward M. (2005) *Web shops face tighter security*, BBC, abrufbar unter: <http://news.bbc.co.uk/2/hi/technology/4449759.stm> (zuletzt eingesehen am 29. Dezember 2006).

Evers J. (2005) *Credit card breach exposes 40 million accounts*, CNET Networks, Inc., abrufbar unter: http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029_3-5751886.html (zuletzt eingesehen am 29. Dezember 2006).

Extended Retail Solutions (2006) *Fighting spyware and retail identity theft*, GDS Publishing Ltd., abrufbar unter: <http://www.extendedretail.com/pastissue/article.asp?art=25770&issue=147> (zuletzt eingesehen am 29. Dezember 2006).

Schneier B. (2005) *Schneier on Security: Visa and Amex Drop CardSystems*, Schneier.com, abrufbar unter: http://www.schneier.com/blog/archives/2005/07/visa_and_amex_d.html (zuletzt eingesehen am 29. Dezember 2006).

Harris Interactive (2005) *Global Consumer Attitudes and Behaviors Toward Data Security*, Visa International.

Krebs B. (2006) *ID Thieves Turn Sights on Smaller E-Businesses*, The Washington Post,

abrufbar unter: <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html> (zuletzt eingesehen am 29. Dezember 2006).

Cybertrust (2006) *PCI Merchant & Service Provider Levels*, abrufbar unter: http://www.cybertrust.com/solutions/compliance_governance/pci_compliance/pci_levels/ (zuletzt eingesehen am 29. Dezember 2006).

MasterCard *Merchant Levels Defined*, abrufbar unter: http://www.mastercard.com/us/sdp/merchants/merchant_levels.html (zuletzt eingesehen am 29. Dezember 2006).

Pauli D. (2006) *Australian Compliance Confusion Leads to Security Breaches*, CXO Media Inc., abrufbar unter: http://www2.csoonline.com/blog_view.html?CID=25049 (zuletzt eingesehen am 29. Dezember 2006).

Wells Fargo *Merchant Services - Payment Card Industry (PCI) Data Security Standards FAQs*, abrufbar unter: <https://www.wellsfargo.com/biz/help/merchant/faqs/pci#Q24> (zuletzt eingesehen am 29. Dezember 2006).

PCI Security Standards Council (2006) *Payment Card Industry (PCI) Data Security Standard (Version 1.1)*, abrufbar unter: https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

© 2007. GFI Software. Alle Rechte vorbehalten. Die in diesem Dokument aufgeführten Informationen geben den von GFI Software zum Zeitpunkt der Veröffentlichung vertretenen Standpunkt zum Thema dieses White Papers wieder. Modifizierungen aufgrund von veränderten Marktbedingungen sind vorbehalten. Die in diesem Dokument präsentierten Informationen stellen keine Verpflichtung seitens GFI Software dar, und für ihre Genauigkeit wird nach dem Datum der Veröffentlichung keine Garantie übernommen. Die Angaben in diesem White Paper dienen nur der allgemeinen Information. GFI Software übernimmt keine ausdrückliche oder stillschweigende Haftung für die in diesem Dokument präsentierten Informationen. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor und die zugehörigen Produktlogos sind eingetragene Marken oder Marken von GFI Software in den Vereinigten Staaten und/oder anderen Ländern. Alle hier aufgeführten Produkte und Firmennamen sind Marken der jeweiligen Eigentümer.