

PCI DSS-Compliance durch automatisiertes Schwachstellen-Management

Netzwerksicherheit und PCI DSS-Compliance in der Praxis

Mit diesem White Paper werden die Herausforderungen bei der Bewältigung von Netzwerk-Sicherheitsrisiken im Rahmen des Schwachstellen-Managements erläutert. Erfahren Sie, wie eine automatisierte Verwaltung von Schwachstellen im Netzwerk dazu beiträgt, branchenspezifische Sicherheitsstandards wie den PCI DSS (Payment Card Industry Data Security Standard) einzuhalten und zudem Sicherheitsprobleme proaktiv erkennen lässt.

Einführung

Das zum Risiko-Management zählende Schwachstellen-Management befasst sich mit Gefahren im Zusammenhang mit dem E-Commerce und Informationssystemen. Aufgaben des Schwachstellen-Managements sind die regelmäßige Überwachung von Hardware- und Software-Komponenten der IT-Infrastruktur sowie das Aufspüren von Schwachstellen und deren Behebung. Viele IT-Experten sehen den hierfür zu betreibenden inhaltlichen wie zeitlichen Aufwand jedoch als sehr belastend an. Die Folge: Dieser Bereich des Sicherheits-schutzes wird sträflich vernachlässigt.

Das Netzwerkschwachstellen-Management hat jedoch längst nicht mehr einen freiwilligen Charakter: Gesetzliche Richtlinien und Branchenstandards wie der PCI DSS (Payment Card Industry Data Security Standard) verpflichten zur regelmäßigen Kontrollen und Sicherheits-nachweisen – bei Nichteinhaltung der Vorgaben drohen schwerwiegende Konsequenzen.

Dieses White Paper erläutert, warum effektives Schwachstellen-Management dringend erforderlich ist. Es befasst sich mit den dabei zu bewältigenden Herausforderungen und erklärt, wie IT-Experten mit Hilfe automatisierter Prozesse Sicherheitslücken schließen, Kosten optimieren und zusätzliche Unterstützung bei der Einhaltung des PCI DSS erhalten.

Einführung	2
Was ist der PCI DSS?	2
Was bedeutet Schwachstellen-Management?	3
Wie spiegelt sich das Schwachstellen-Management im PCI DSS wider?	4
Herausforderungen des Schwachstellen-Managements	5
GFI LANguard Network Security Scanner	8
Zusammenfassung	8
Über GFI	9

Was ist der PCI DSS?

Der PCI DSS (Payment Card Industry Data Security Standard) besteht aus einer Zusammenstellung verbindlicher Regeln, mit denen IT-Sicherheitsstrukturen in Unternehmen, die mit Kredit- und Debitkartendaten arbeiten, gestärkt werden sollen. Ziel des PCI DSS ist es, dem Finanzbetrug einen Riegel vorzuschieben. Folgende drei Gründe, die den Missbrauch von Kartendaten fördern, haben zur Aufstellung des Sicherheitsstandards geführt:

1. Die wachsende Akzeptanz des E-Commerce, der nicht nur geografische Grenzen aufhebt, sondern in vielen Fällen auch lokale Gesetze und Richtlinien zu Schutzmaßnahmen.
2. Die große Verbreitung des „Plastikgelds“, das Kunden Einkäufe jeder Art erlaubt.

3. Die Nichtbeachtung von Best-Practice-Richtlinien zur Datensicherheit durch Unternehmen – Karteninformationen werden ungeschützt gespeichert und/oder verarbeitet.

Um den Kredit- und Debitkartenbetrug einzudämmen und Kartentransaktionen sicherer zu machen, haben die fünf größten Kartenunternehmen Visa International, MasterCard Worldwide, American Express, JCB und Discover Financial Services den PCI DSS als Rahmenwerk mit Sicherheitsanforderungen aufgestellt. Unternehmen jeder Größe, die Kartendaten verarbeiten, ob im Einzelhandel, bei postalischen oder telefonischen Bestellungen oder im E-Commerce, müssen die PCI DSS-Vorgaben beachten.

Was bedeutet Schwachstellen-Management?

Neu entdeckte Sicherheitsschwachstellen in Software-Lösungen führen dazu, dass Hersteller fortwährend Reparatur-Patches veröffentlichen müssen, mit denen die Lücken behoben werden. Administratoren haben dafür zu sorgen, dass solche Sicherheits-Updates auch für ihr Netzwerk eingespielt werden – eine anstrengende Aufgabe angesichts der Vielzahl von Aktualisierungen. Infolgedessen können viele Systemverantwortliche ihrer Aufgabe nicht mehr sorgfältig genug nachkommen. Diese Vernachlässigung machen sich Hacker zunutze und schleusen Würmer und Viren durch die Sicherheitslücken nicht gepatchter Systeme.

Einer dieser berüchtigten Schädlinge ist der Wurm „Mytob“, der in unterschiedlichster Form auftritt. Obwohl Mytob sich über hinlänglich bekannte Schwachstellen verbreitet, für die seit August 2004 ein Sicherheits-Update bereitsteht, ist er immer noch aktiv: In den Top 20 der von Viruslist.com gepflegten Liste aktiver Schädlinge nimmt er standhaft den siebten Rang ein (Viruslist.com, [Virus Top 20](#), [Stand April 2007](#)).

Aber auch zielgerichtete Angriffe stellen eine wachsende Bedrohung der Business-Continuity dar und müssen von Administratoren in Abwehrstrategien einbezogen werden. Angreifer, die genau wissen, in welchen Bereichen der IT-Umgebung eines Unternehmens Sicherheits-Updates fehlen, können durch diese Lücken Schadsoftware einschleusen, die ihnen Zugang zum Netzwerk verschafft. Bei solchen an die individuellen Schwachstellen eines Unternehmens angepassten Angriffen vergeht oftmals viel Zeit bis zur Entdeckung – Auswirkungen sind dann bereits spürbar, und für Gegenmaßnahmen ist es vielfach zu spät.

Häufig wird Netzwerksicherheit fälschlicherweise nur mit (fehlenden) Patches und anderen Sicherheitsaktualisierungen in Verbindung gebracht. Netzwerksicherheit umfasst jedoch einen weitaus größeren Bereich, bedingt durch die Vielzahl an Angriffsmöglichkeiten und Schwächen, denen Rechnung getragen werden muss. Mangel an erforderlicher Sorgfaltspflicht oder menschliche Fehler sind eigene Kategorien von Schwachstellen, die ebenfalls unmittelbar zu schwerwiegenden Sicherheitsverletzungen beitragen können. In diesem Zusammenhang stellen sich Fragen wie: Wieso werden vom Hersteller vorgegebene Passwörter für systemkritische Dienste nicht geändert? Warum werden Lösungen zur netzwerkweiten Abwehr von Viren und anderer Malware nicht mit aktuellen Signaturen auf dem neuesten Stand gehalten?

Wieso können tragbare Speichermedien, die sich für den Diebstahl vertraulicher Daten, das Einschleppen gefährlicher Viren, die Übertragung von Raubkopien, die Installation von P2P-Software und vieles mehr missbrauchen lassen, auch weiterhin unkontrolliert in Firmennetzwerken verwendet werden?

Eine Lösung dieser Probleme, die tägliche Geschäftsabläufe beeinträchtigen und zahlreiche rechtliche Folgen nach sich ziehen, bietet das Schwachstellen-Management. Es stellt die Sicherheit des unternehmensspezifischen Netzwerks aus unterschiedlichen Perspektiven und unter Berücksichtigung verschiedener Angriffsmethoden auf die Probe. Schwächen werden aufgespürt, klassifiziert und angemessen beseitigt. Das Schwachstellen-Management findet sich in jedweder Form von Sorgfaltspflicht im Rahmen der Netzwerksicherheit wieder – ein Grund, warum das Sicherheitsgremium der Kartenverbände, der PCI Security Standards Council, es zur zentralen Voraussetzung für PCI DSS-Compliance gemacht hat.

Wie spiegelt sich das Schwachstellen-Management im PCI DSS wider?

Sicherheit ist nach Maßgabe des PCI DSS nur so zuverlässig wie das schwächste Glied aller Schutzmaßnahmen. Mit dem PCI DSS sollen folgende Ziele erreicht werden:

- Einrichtung und Betrieb eines geschützten Netzwerks
- Schutz von aufbewahrten und übermittelten Karteninhaberdaten
- Einrichtung und Betrieb eines Schwachstellen-Management-Systems
- Umsetzung effektiver Richtlinien zur Zugriffskontrolle
- Regelmäßige Überwachung und Überprüfung der IT-Infrastruktur
- Formulierung und Durchsetzung einer Richtlinie zur Informationssicherheit

Der PCI DSS gibt zur Umsetzung dieser Ziele 12 Sicherheitsanforderungen vor, die von Systemadministratoren mit einem entsprechenden Nachweis realisiert werden müssen. Anforderung 1 gibt beispielsweise vor, dass zum Schutz von Karteninhaberdaten vor Angriffen von außen Firewalls installiert und gepflegt werden müssen. Für Systemverantwortliche bedeutet dies, dass sie ihre Netzwerke scannen, die Firewall-Installation und -Konfiguration überprüfen und Einstellungen so abstimmen müssen, dass die Netzwerksicherheit nicht gefährdet ist. Mit Anforderung 6 des PCI DSS wird wiederum der Aufbau und Betrieb sicherer Systeme und Anwendungen vorgeschrieben – eine Aufgabe des Schwachstellen-Managements, bei der es darauf ankommt, dass alle Netzwerkkomponenten mit aktuellen Sicherheits-Patches der Hersteller auf dem neuesten Stand gehalten werden.

Das Schwachstellen-Management ist für alle 12 Anforderungen des PCI DSS relevant. Es umfasst mehr als bloße Schutzmaßnahmen zur Netzwerksicherheit und betrifft sämtliche Bestandteile und Bereiche der IT-Infrastruktur, die mit der Speicherung, Verarbeitung oder Übertragung von Daten zu Zahlungskarten verbunden sind. Hierzu zählen:

- Zentrale Komponenten der Netzwerksicherheit wie Firewalls, Router, Intrusion-Prevention-Systeme (IPS) und Intrusion-Detection-Systeme (IDS).
- Netzwerkbereiche wie Demilitarisierte Zonen (DMZ)
- Server und Geschäftssysteme, die DNS-Dienste hosten oder NTP-, SMTP/POP3/IMAP- und andere E-Mail-Dienste sowie Authentifizierungsverfahren, Active Directory-Richtlinien, Web- und Datenbank-Server u. Ä.
- Interne Anwendungen oder solche mit Web-Zugang, ob standardmäßige oder individuell konzipierte Software

Herausforderungen des Schwachstellen-Managements

Werden für die oben erwähnten Sicherheitsbereiche des Netzwerks keine zuverlässigen Verfahren zum Schwachstellen-Management eingesetzt, verstoßen Unternehmen gegen den PCI DSS und setzen sich unternehmensinternen wie auch externen Gefahren aus. Bei Sicherheitsverletzungen sind jedoch nicht nur Konsequenzen aufgrund der Nichteinhaltung des PCI DSS zu befürchten. Unternehmen riskieren auch, gesetzlichen Vorschriften zuwiderzuhandeln, in den USA beispielsweise denen der US-amerikanischen Verbraucherschutzbehörde FTC (Federal Trade Commission). Daher sind zusätzliche Strafzahlungen und weitere Rechtsfolgen zu erwarten.

Obwohl das Schwachstellen-Management gesetzlich und branchenspezifisch vorgeschrieben ist, wird es von IT-Profis als lästig empfunden, zumal die sich wiederholenden, vielfach manuell zu erledigenden Aufgaben sehr anfällig für Fehler sind. Sämtliche Hardware- und Software-Komponenten des Unternehmensnetzwerks müssen überprüft und Daten zentral konsolidiert und gesichert werden. Zudem sind die erfassten Informationen zu analysieren und entsprechende Gegenmaßnahmen einzuleiten, sofern erforderlich. Diese anspruchsvolle Aufgabe ist nur mit Hilfe automatisierter Abläufe zu bewältigen. Dank einer Automatisierung des Schwachstellen-Managements können sich Systemverantwortliche den folgenden Herausforderungen leichter stellen:

Herausforderung 1 – Durchführung tausender Sicherheits-Checks auf jedem einzelnen Computer

Bestes Beispiel für die Notwendigkeit des Schwachstellen-Managements lieferte die weltweit in den Medien verbreitete [Sicherheitsverletzung beim US-Einzelhändler TJX](#). Laut Vizepräsident und Senior Fellow John Pescatore vom IT-Analysten Gartner wäre der Diebstahl von über 45 Millionen Datensätzen zu Kredit- und Debitkarten mit Hilfe eines Schwachstellen-Scans des Netzwerks, der die Gefahren im Handumdrehen deutlich aufgezeigt hätte, leicht zu verhindern gewesen (Quelle: [SCMagazine.com](#)). Vom Cyber-Crime sind jedoch nicht nur große Unternehmen betroffen. In einer Rede vor dem britischen Oberhaus im November 2006 anlässlich einer Veranstaltung zur IT-Sicherheit wies der ehemalige Sicherheitsberater der US-Regierung, Howard Schmidt, mit Nachdruck auf die Anfälligkeit von Unternehmen jeder Größe

hin: „Kleine und mittelgroße Firmen sollten nicht glauben, dass sie vor Angriffen verschont bleiben, nur weil klein sind. Überall, wo es etwas zu holen gibt, werden Angreifer auch ihr Glück versuchen.“ ([CNET News.com](http://CNETNews.com)). Ein Fall aus den USA verdeutlicht diese Mahnung nur zu gut: Am 4. Februar 2007 war die Website von „Johnny’s Selected Seeds“, einer relativ kleinen, nur 100 Mitarbeiter zählenden Saatgut-Firma in Winslow, Maine, Ziel eines Hacker-Angriffs: Über 11.500 Datensätze zu Kredit-/Debitkarten wurden gestohlen (Quelle: MaineToday.com). Erst zwei Wochen später, nachdem Kunden auf den Missbrauch ihrer Kreditkartendaten aufmerksam gemacht hatten, realisierte das Unternehmen den Datenabfluss. Eine professionell gesteuerte Sicherheitsüberwachung hätte die beschriebenen Schäden vermeiden können. Mit automatisierten Schwachstellen-Scans ist eine konsistente Überwachung gewährleistet, menschliche Fehler lassen sich verhindern. Auch können Sicherheitslücken leichter aufgespürt und Gefahren rechtzeitig erkannt werden.

Herausforderung 2 – Unterschiedlicher Schutz unzähliger Daten auf zu vielen Computern

Im März 2007 gelang es einem Subunternehmer der Dai Nippon Printing Corporation, fast neun Millionen vertrauliche Datensätze des bedeutenden japanischen Druckereiunternehmens zu entwenden, darunter auch Kreditkartennummern (Quelle: DarkReading.com). Der Diebstahl erfolgte firmenintern über mobile Speichermedien. Sicherheitsüberprüfungen, so verdeutlicht dieser Vorfall, müssen über den Rahmen üblicher Kontrollen hinausgehen, um auch Gefahren abwehren zu können, die sich mit normalen Schwachstellendefinitionen allein nicht erkennen lassen. Hochleistungslösungen zum Schwachstellen-Management sind in der Lage, mit einer erschöpfenden Anzahl an Überwachungsmöglichkeiten unerwünschte und sicherheitsgefährdende Hard- und Software aufzuspüren, die eine potenzielle Bedrohung für die Netzwerkintegrität darstellt. Diese Informationen sind auf anderem Weg nur mit sehr großem Aufwand zu gewinnen.

Herausforderung 3 – Patch-Management: Wer nicht am Ball bleibt, verliert

Dass Administratoren mit dem Patch-Management überfordert sein können, ist nicht verwunderlich: Im Jahr 2006 wurden von Microsoft allein 104 Sicherheits-Updates der Kategorie „kritisch“ veröffentlicht. Lösungen, mit denen die Verwaltung von Patches automatisiert wird, sorgen dafür, dass fehlende Sicherheitsaktualisierungen zeitnah und ohne manuelles Eingreifen abgerufen werden. Sie stellen darüber hinaus sicher, dass die Bereitstellung auf den einzelnen Computern ebenfalls selbsttätig erfolgt. Neben dieser „Push“-Funktionalität können Updates per Rollback-Funktion zudem wieder rückgängig gemacht werden, falls Stabilitätsprobleme dies erforderlich machen sollten.

Herausforderung 4 – Begrenzter Funktionsumfang von Standard-Tools zum Schwachstellen-Management

Ein typischer Fall für eine in ihren Funktionen eingeschränkte Lösung zum Schwachstellen-Management sind die Microsoft Windows Server Update Services (WSUS). Mit ihnen können zwar fehlende Microsoft-Updates abgerufen werden, doch Schwachstellen-Scans, Netzwerk-Audits und Berichterstellung stehen nicht zur Verfügung. Dieses Funktionsdefizit muss mit zusätzlichen Lösungen behoben werden. Hier zeigt sich eine weitere Herausforderung für Systemverantwortliche: Sämtliche Ergebnisse der einzelnen Spezialanwendungen sind aufeinander abzustimmen, um zuverlässige Aussagen zum Sicherheitsstatus zu erhalten. Es liegt am Administrator, Ergebnisse händisch zu konsolidieren. Doch damit nicht genug: Vielfach sind keine ausgeprägten Reporting-Funktionen vorhanden, sodass Administratoren weitere Zeit damit verbringen müssen, Berichte manuell, oft per Copy-and-Paste, zusammenzustellen.

Herausforderung 5 – Aufwändiger Nachweis über die Einhaltung von Sicherheitsstandards

Den Nachweis über die korrekte Einhaltung von Sicherheitsstandards liefert ein umfassendes Reporting, das mit aussagekräftigen Berichten die implementierten Verfahren zum Schwachstellen-Management belegt. Der Umfang der Berichterstellung und die erforderliche Archivierung von Reports führt jedoch zu zusätzlichen Problemen. Auch hier unterstützen automatisierte Abläufe die Arbeit von Administratoren ungemein, indem Berichte nach einem festen Zeitplan erstellt und ohne Zutun des Systemverantwortlichen beispielsweise allen Entscheidungsträgern zugestellt werden. Compliance-Vorgaben können leichter eingehalten und Workflows verschlankt werden.

Automatisierung ist somit ein wichtiges, jedoch nicht das einzige Leistungsmerkmal, das eine umfassende Lösung für Schwachstellen-Management aufweisen muss, damit sich typische Herausforderungen an die Sicherheit meistern lassen. Für eine zuverlässige Absicherung des Firmennetzwerks sind weitere Funktionalitäten von Bedeutung, mit denen sich eine noch größere Anzahl an Schwachstellen erkennen lässt: eine komplette, erprobte Schwachstellen-Datenbank und die nahtlose Integration verschiedener Kontrollverfahren für unterschiedliche Sicherheitsbereiche. Neben der Automatisierung ist Systemadministratoren auch an einer Lösung gelegen, mit der sich das Schwachstellen-Management in ihren täglichen Arbeitsablauf einbinden lässt, ohne bestehende Workflows zu beeinträchtigen. All diese Anforderungen erfüllt GFI LANguard Network Security Scanner (N.S.S.).

GFI LANguard Network Security Scanner

GFI LANguard Network Security Scanner (N.S.S.) unterstützt Administratoren mit einer zentralen Konsole beim Aufspüren, Bewerten und Beheben von Sicherheitslücken im Netzwerk. Die mehrfach ausgezeichnete und OVAL-zertifizierte Lösung überprüft heterogene Netzwerke mit leistungsfähigen Schwachstellen-Scans und System-Audits, bietet umfassendes Patch-Management und liefert dank der ReportPack-Berichterstellung zielgerichtet aufbereitete Sicherheitsinformationen in kompakter Form.

GFI LANguard N.S.S. ist auch im Lieferumfang der GFI PCI Suite enthalten und wurde für das Lösungspaket an die Anforderungen des PCI DSS angepasst. Zur Suite zählen zudem GFI EventsManager für umfassendes Ereignisprotokoll-Management und eine Auswahl an PCI DSS-spezifischen Berichten. Weitere Informationen zu GFI LANguard N.S.S. und zur GFI PCI Suite sowie zum Thema „PCI DSS-Compliance mit Lösungen von GFI“ erhalten Sie hier: <http://www.gfisoftware.de/de/pci/>.

Zusammenfassung

IT-Experten können sich den Aufgaben des Schwachstellen-Managements, die mit der Einhaltung von Sorgfaltspflichten und dem PCI DSS untrennbar verbunden sind, nicht entziehen. Netzwerkadministratoren kann das Aufspüren von Netzwerkschwachstellen jedoch bedeutend vereinfacht werden. Moderne Lösungen wie GFI LANguard N.S.S. sorgen mit automatisierten Funktionen für Erleichterung und erlauben wichtige Sicherheitsüberprüfungen mit geringstmöglichem Aufwand – bei optimierten Kosten und niedrigerer Fehleranfälligkeit.

Über GFI

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>.

© 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.

