

## ... PCI-KONFORMITÄT

Bis Ende Dezember 2007 müssen alle Unternehmen, die Zahlungen per Zahlkarte entgegennehmen, mit dem Payment Card Industry Data Security Standard (PCI DSS) konform sein. Der aus zunehmenden Sicherheitsverletzungen, durch die Kreditkarteninformationen tausender Kunden gestohlen oder gefährdet wurden, entstandene Standard wurde in Zusammenarbeit großer Kartenunternehmen, wie MasterCard und Visa, erstellt und enthält mehrere grundlegende Sicherheitsanforderungen.

Der Standard erfordert die Erstellung von Richtlinien und Ergreifung von Maßnahmen, um eine gesicherte Verwaltung von Kreditkartendaten und den kontrollierten Zugriff auf die Netzwerke zu gewährleisten, über die die Karteninformationen der Kunden gesendet werden. Die Nichteinhaltung der Anforderungen kann hohe Strafen und möglicherweise sogar den Ausschluss aus Kreditkartenprogrammen nach sich ziehen. Wenn Sie also Zahlungen per Kredit- oder Debitkarte entgegennehmen oder Informationen über Kreditkartentransaktionen erfassen, bearbeiten oder speichern, befolgen Sie diese einfachen Schritte, um die Sicherheitsaspekte der PCI-Kompatibilität zu erfüllen.



### 1 Erstellen und Verwalten eines sicheren Netzwerks

PCI-Anforderungen 1 und 2

Die Zugriffskontrolle auf das Netzwerk ist Grundvoraussetzung für die Sicherheit der Daten von Karteninhabern. Netzwerke und zentral verwaltete Firewalls sollten so konfiguriert werden, dass der gesamte eingehende und ausgehende Datenfluss gestoppt wird, der nicht für Geschäftszwecke erforderlich ist und die Sicherheit des Unternehmens gefährden könnte. Mithilfe von Network Access Control (NAC)-Lösungen können Sie dafür sorgen, dass Gastcomputer, z.B. von Geschäftspartnern, nur auf Ihr Netzwerk zugreifen, wenn sie eine vom Unternehmen genehmigte Firewall benutzen.

Außer der Kontrolle der Netzwerk- und Internetverbindungen müssen Sie auch die Sicherheit einzelner Computer in Betracht ziehen, in der Branche anerkannte optimierte Standards verwenden, um Systeme nach einem festgelegten ungenutzten Zeitraum zu sperren, und den sicheren Gebrauch von Kennwörtern durchsetzen. Stellen Sie sicher, dass wirkungsvolle Kennwörter benutzt und regelmäßig geändert werden und keine Wiederverwendung von Kennwörtern möglich ist. Mit NAC können Richtlinien erstellt und die Konformität mit mehreren Sicherheitsmaßnahmen abgeglichen werden. Außerdem kann Computern, die von den Richtlinien abweichen, der Zugriff auf unternehmenskritische Ressourcen verweigert werden.

### 2 Schutz von Karteninhaberdaten

PCI-Anforderungen 3 und 4

Nur befugten Personen sollte der Zugriff auf Kreditkartendaten gestattet werden und, wenn möglich, sollten Kreditkartennummern verkürzt dargestellt werden. Mindestens sollten jedoch Informationen auf der Festplatte verschlüsselt sein, damit Daten von Karteninhabern für den Fall eines Verlusts oder Diebstahls des Computers nicht lesbar sind. Sie sollten Richtlinien für die sichere Übertragung von Kreditkarteninformationen einführen. Nur verschlüsselte Daten sollten über ein offenes öffentliches Netzwerk per E-Mail versendet werden. Stellen Sie sicher, dass Ihre E-Mail-Gateway-Richtlinie darauf eingestellt ist, E-Mails zu blockieren, die unverschlüsselte Karteninhaberdaten enthalten.

Der Verlust vertraulicher Daten kann außerdem durch Deaktivierung bestimmter Ports verhindert werden, sodass z.B. keine drahtlosen Verbindungen oder der Einsatz von USB-Sticks und anderen Wechseldatenträgern zugelassen ist.

### 3 Programme zur Verwaltung von Schwachstellen

PCI-Anforderungen 5 und 6

Sie müssen auf allen Computern des Unternehmens Endpoint Security Software installieren, die regelmäßig aktualisiert wird. Durch die Erstellung einer soliden, zentral verwalteten Richtlinie für effektive zeitgesteuerte Überprüfungen und Überprüfungen bei Zugriff sowie die Verwaltung von Sicherheitspatches bei allen Entwicklungs-, Test- und Produktionssystemen sorgen Sie dafür, dass Sie den Überblick und die Kontrolle über das Netzwerk haben. Ihre Richtlinie sollte dafür sorgen, dass der Microsoft Patch Update-Dienst auf allen Windows-Geräten aktiviert ist. Wie bei der Verwendung von Firewalls sorgt eine NAC-Lösung dafür, dass Gastcomputer nur auf Ihr Netzwerk zugreifen können, wenn sie eine vom Unternehmen genehmigte aktuelle Virenschutzsoftware benutzen. Damit können Sie auch den Patch-Status von Computern überprüfen und die Computer in Quarantäne verschieben, die Ihrer Sicherheitsrichtlinie nicht entsprechen. Idealerweise sollte die Lösung ein Datafeed enthalten, das alle kritischen und wichtigen Patches erkennt und eine Inhaltsüberprüfung durchführt, damit nur Patches, die für den jeweiligen Computer relevant sind, überprüft werden. Der Web-Gateway muss außerdem in allen Vulnerability Management-Programmen enthalten sein, um zu verhindern, dass webbasierte Malware auf Endgeräte heruntergeladen wird.

## 4 Implementierung wirkungsvoller Zugriffssteuerungsmaßnahmen

PCI-Anforderungen 7, 8 und 9

Peer-to-Peer Remote-Zugriff-Software sollte blockiert werden, sofern sie nicht für Geschäftszwecke erforderlich ist, da sie ein unnötiges Risiko darstellt. Sollte sie *doch* zum Einsatz kommen, muss jeder Computer eindeutige Zugangsdaten verwenden und Verschlüsselung und andere Sicherheitsfunktionen müssen aktiviert sein. Wählen Sie eine Sicherheitslösung, die diese potenziell unerwünschten Anwendungen erkennen und deren Gebrauch durch unbefugte Anwender verhindern kann.

Verwenden Sie eine NAC-Lösung, um unbefugten Anwendern den Zugriff auf Computer sowie Server zu verweigern, auf denen sich Karteninhaberdaten befinden können. Verwenden Sie einen Mechanismus zur Durchsetzung, der entweder den Zugriff am Netzwerkschalter mit 802.1x sperrt oder den Anwender durch DHCP-Durchsetzung daran hindert, eine gültige IP-Adresse zu erhalten. Drahtloser Zugriff durch Gäste oder Geschäftspartner sollte eingeschränkt werden und alle Computer, die nicht mit Ihrer Network Access Control-Richtlinie übereinstimmen, sollten in Quarantäne verschoben werden. Alle Geräte und Medien, die Karteninhaberdaten enthalten, müssen direkt vor unbefugtem Zugriff geschützt werden.

## PCI DATA SECURITY STANDARD

- 1 Installieren und verwalten Sie eine Firewall zum Schutz von Karteninhaberdaten
- 2 Verwenden Sie keine Herstellerstandards für Kennwörter und andere Sicherheitsparameter
- 3 Schützen Sie gespeicherte Karteninhaberdaten
- 4 Verschlüsseln Sie die Übertragung von Karteninhaberdaten über offene öffentliche Netzwerke
- 5 Nutzen Sie Virenschutzsoftware und aktualisieren Sie sie regelmäßig
- 6 Entwickeln und setzen Sie sichere Systeme und Anwendungen ein
- 7 Beschränken Sie den Zugriff auf Karteninhaberdaten auf Befugte
- 8 Weisen Sie jeder Person mit Computerzugriff eine einmalige ID zu
- 9 Machen Sie Karteninhaberdaten nur Befugten zugänglich
- 10 Erfassen und überwachen Sie den gesamten Zugriff auf Netzwerkressourcen und Karteninhaberdaten
- 11 Testen Sie Sicherheitssysteme und -prozesse regelmäßig
- 12 Verwalten Sie eine spezielle Richtlinie für Informationssicherheit

## 5 Regelmäßige Überwachung und Test von Netzwerken

PCI-Anforderungen 10 und 11

Nach der Installation von Malwareschutz und Systemen zum Schutz vor Hackern und Zero-Day-Bedrohungen im Netzwerk und auf Endpoint-Computern ist es unbedingt erforderlich, dass Sie die Funktion dieser Maßnahmen testen. Außer einer ständigen Suche nach Schwachstellen in allen Systemen im Netzwerk sollten Sie außerdem *alle* Zugriffsversuche erfassen – sowohl erfolgreiche als auch fehlgeschlagene – und diese Aufzeichnungen mindestens drei Monate lang aufheben. Eine Endpoint Security-Lösung, die Host Intrusion Prevention und eine Network Access Control-Lösung integriert und sicherstellt, dass sie ordnungsgemäß installiert wurde, funktioniert und über den neuesten Schutz verfügt, hilft Ihnen dabei, dass Ihr Test zur Routine wird und nicht der Anfang eines langwierigen Reparaturprozesses.

## 6 Verwalten einer Richtlinie für Informationssicherheit

PCI-Anforderung 12

Für eine effektive Konformität mit PCI DSS müssen Sie über eine umfassende Informationssicherheitsrichtlinie zahlreiche Prozesse und Sicherheitsmaßnahmen für Mitarbeiter und Gäste erstellen und verwalten. Die Sicherheitsmaßnahmen in dieser Anleitung bilden eine gute Basis.

Sophos NAC Advanced und Sophos Enterprise Security and Control bieten Schutz, Automatisierung und Ausgereiftheit, um Ihr Unternehmen rund um die Uhr zu sichern. Mehr über Sophos Produkte erfahren Sie auf [www.sophos.de](http://www.sophos.de). Dort stehen auch Testversionen zum Download bereit.

Sophos ist ein weltweit führender Hersteller von IT-Lösungen im Bereich Security and Control. Wir bieten Unternehmen, dem Bildungswesen und Behörden umfassenden Schutz und Kontrolle. Sophos Lösungen schützen vor bekannter und unbekannter Malware, Spyware, Hackern, unerwünschten Anwendungen, Spam, Richtlinienmissbrauch und bieten umfassende Network Access Control (NAC). Unsere zuverlässigen, benutzerfreundlichen Produkte schützen über 100 Millionen Benutzer in mehr als 150 Ländern. Wir verfügen über mehr als 20 Jahre Erfahrung und ein globales Netzwerk aus Bedrohungsanalysecentern und können daher schnell auf neue Bedrohungen reagieren. Dadurch haben wir den höchsten Grad an Kundenzufriedenheit in der Branche erreicht. Sophos ist ein globales Unternehmen mit Hauptsitzen in Oxford, GB, und in Boston, USA.

Boston, USA • Mainz, Deutschland • Mailand, Italien • Oxford, GB • Paris, Frankreich  
Singapur • Sydney, Australien • Vancouver, Kanada • Yokohama, Japan

© Copyright 2007 Sophos GmbH. Alle Rechte vorbehalten. Alle hier aufgeführten Marken sind Eigentum der jeweiligen Inhaber.

fo/071025

**SOPHOS**  
secured.