

Banken und Versicherungen müssen sich für den PCI-Standard fit machen

Interviewpartner
Andre Muscat ist
Director Network
Security Products
bei GFI Software.

Bild: GFI Software



? Welche Anforderungen stellt der PCI-Sicherheitsstandard an Unternehmen?

Andre Muscat: Der von den wichtigsten Kreditkartenunternehmen ins Leben gerufene PCI DSS (Payment Card Industry Data Security Standard) ist ein strenges Regelwerk mit Sicherheitsanforderungen, die den weltweit wachsenden Missbrauch von Kreditkartendaten unterbinden sollen. Laut eines Berichts der US-Verbraucherschutzbehörde FTD (Federal Trade Commission) entfielen im Jahr 2006 allein 25 Prozent aller angezeigten Fälle von Identitätsdiebstahl auf den Kreditkartenbetrug.

Für Unternehmen, die im Zahlungsverkehr mit Kreditkartendaten arbeiten, bestehen in diesem Jahr zwei Fristen zur Umsetzung der PCI-Anforderungen. Für Händler mit mehr als sechs Millionen Kreditkartentransaktionen pro Jahr gilt der Stichtag 30. September 2007. Werden jährlich ein bis sechs Millionen Transaktionen durchgeführt, endet die Frist am 31. Dezember 2007.

Das PCI DSS-Regelwerk umfasst zwölf Sicherheitsanforderungen, die sich in sechs Kategorien einteilen lassen:

1. Einrichtung und Wartung eines geschützten Netzwerks,
2. Schutz von archivierten und zu übermittelnden Karteninhaberdaten,
3. Einrichtung eines Schwachstellen-Management-Systems,
4. Umsetzung effektiver Richtlinien zur Zugriffskontrolle,
5. regelmäßige Überwachung und Überprüfung der IT-Infrastruktur und
6. Formulierung und Durchsetzung einer Richtlinie zur Informationssicherheit.

Zum Erreichen der PCI-Compliance sind folgende drei Aspekte zu berücksichtigen:

Erstens sind alle Protokoll-daten sicher zu erfassen und vor Manipulationen geschützt zu speichern, damit Daten zu Sicherheitsanalysen herangezogen werden können. Zweitens müssen Unternehmen bei Sicherheits-Audits vor Ort anhand von verfügbaren Nachweisen über implementierte Schutzmaßnahmen belegen können, dass PCI-Compliance besteht. Und drittens müssen Systeme zur kontinuierlichen Überwachung von Datenzugriff und -verwendung implementiert sein, z. B. automatische Warnsysteme, die Administratoren bei kritischen Ereignissen umgehend benachrichtigen. Zudem muss die Erfassung und Speicherung von Protokoll-daten nachweisbar sein.

? Warum müssen Unternehmen die Anforderungen umsetzen und welche Konsequenzen sind bei Nichteinhaltung des Sicherheitsstandards zu erwarten?

Andre Muscat: Händlerbanken sollten aus eigenem Interesse darauf achten, dass Händler als Akzeptanzpartner mit dem PCI DSS vertraut sind und damit konform gehen. Für eine erfolgreiche und gesunde Geschäftsbeziehung zu Kreditkartenunternehmen müssen Banken daher sicherstellen, dass sich ihre Akzeptanzpartner hinreichend vor Datenverlust und -diebstahl schützen. Der PCI DSS erlaubt dabei die Beurteilung der implementierten Schutzmaßnahmen. Händler und Dienstleister sind wiederum dazu angehalten, gegenüber ihren Banken einen Nachweis zu erbringen, mit welchen Maßnahmen 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.

Firmen, die sich nicht an den PCI DSS halten, drohen schwerwiegende Konsequenzen. Kartenunternehmen können Händlerbanken mit empfindlichen Geldstrafen in sechsstelliger Höhe belegen, falls PCI-Sicherheitsvorschriften nicht eingehalten wurden. Akzeptanzpartner wiederum sind unter Umständen gegenüber Banken vertraglich verpflichtet, diese schadlos zu halten und für entstandene Schäden aufzukommen. Neben rechtlichen Konsequenzen und der Gefahr eines Imageverlusts droht Händlern sogar im

schlimmsten Fall, dass ihnen auch die Akzeptanz von Kreditkarten untersagt wird.

? Wie sorgen GFI EventsManager und GFI LANguard N.S.S. für die Einhaltung der IT-relevanten PCI-Anforderungen?

Andre Muscat: Einige Aufgaben zur Erfüllung der PCI-Anforderungen lassen sich mit Hilfe von Software-basierten Technologielösungen automatisieren. Um Unternehmen bei Umsetzung und Einhaltung der strengen Sicherheitsauflagen zu unterstützen, hat GFI vor Kurzem seine GFI PCI Suite veröffentlicht. Die GFI PCI Suite liefert eine zentrale Verwaltungskonsolle, über die Administratoren speziell für den PCI DSS erweiterte Versionen von GFI EventsManager und GFI LANguard N.S.S. einsetzen können. Beide Sicherheitslösungen sorgen für den Schutz von Netzwerken und bieten wichtige Unterstützung bei der Einhaltung der PCI-Vorgaben. GFI EventsManager fördert die Einhaltung des PCI DSS, indem Systemverantwortliche unter anderem zu für den Schutz von Kreditkartendaten relevanten Netzwerkeignissen umgehend informiert werden. GFI LANguard N.S.S. ermöglicht ein proaktives Aufspüren und Beheben von Netzwerkschwachstellen, um Sicherheitslücken rechtzeitig schließen zu können, bevor sie ausgenutzt werden. Mit der GFI PCI Suite wird zusätzlich zu den GFI-Lösungen für Ereignisprotokoll-Verwaltung und Schwachstellen-Management eine speziell für den PCI DSS erweiterte Reporting-Funktionalität verfügbar. So bietet das ReportPack von GFI EventsManager acht neue Berichte, die noch detailliertere Informationen zu PCI DSS-relevanten Aktivitäten von Netzwerkbenutzern und Netzwerkkomponenten liefern. Das GFI LANguard Network Security Scanner ReportPack unterstützt die Einhaltung des PCI DSS unter anderem mit einem neuen Bericht, der über den Status von im Netzwerk eingesetzten Anti-Virus-Lösungen informiert; neue Datenfilter erlauben zudem eine noch differenziertere Ausgabe von Berichtsinformationen.

! Vielen Dank
für das Gespräch!