

Statement of the Month – Novell Identity & Security

Düsseldorf im August 2007

Neuer Kreditkarten-Sicherheitsstandard erhöht Kaufspaß

Endlich Urlaub - die Sonne lacht, die Stimmung steigt und der Geldbeutel sitzt lockerer. Am einfachsten lässt es sich natürlich mit der Kreditkarte zahlen, mit dem entscheidenden Vorteil, dass man nicht immer gleich sieht, wie viel schon ausgegeben wurde. So lässt sich der Urlaub noch entspannter genießen. Wenn die Daten in falsche Hände geraten und jemand anderes auf eigene Kosten Urlaub macht, kann das die Freude schnell trüben - Die zunehmende Komplexität der IT-Umgebungen sorgt jedoch für immer mehr Schwachstellen. Zum Glück für den Konsumenten gibt es hier neue Richtlinien. Seit dem 30. Juni 2007 ist für alle Vertragspartner der Kreditkartenunternehmen der so genannte "Payment Card Industry Data Security Standard" (PCI-DSS) verpflichtend. Marina Walser, Director Identity & Security Management, Novell Central Europe, erläutert, wie Unternehmen diese Standards mittels Identitätsmanagement umsetzen können und wie das Bezahlen "mit dem guten Namen" dadurch sicherer wird.

Die Gefahren, die das Bezahlen mit der Kreditkarte für den Konsumenten, wie aber auch für den Händler oder Dienstleister mit sich bringt, sind nicht zu unterschätzen. Ein unbekannter Hacker hat zum Beispiel 300.000 Kreditkartennummern gestohlen, die beim Unternehmen CD Universe gespeichert waren und 25.000 davon auf einer Website veröffentlicht, nachdem der Händler sich weigerte, 100.000 US-Dollar "Lösegeld" für die Daten zu bezahlen. Beispiele dieser Art gibt es viele, die Betrugsfälle gehen in die Millionen. Daher haben sich die Sicherheitsexperten der Kreditkartenunternehmen zusammengesetzt und eine gemeinsame Lösung entwickelt. Jedes Unternehmen, das mit Kreditkarten-Daten umgeht, sie überträgt oder speichert, muss eine Reihe von Sicherheits-Richtlinien zum Schutz der Daten einhalten. Im anderen Fall sind hohe Schadensersatzzahlungen und erhöhte Transaktionsgebühren zu leisten. Es handelt sich nicht um einen gesetzlichen, sondern um einen privaten Standard, der aber nichtsdestotrotz verpflichtend ist.

Die aktuellen Richtlinien entstanden in ihrer heutigen Form innerhalb von nur wenigen Jahren: 2001 hatte Visa das so genannte Carholder Information Security Program (CISP) ins Leben gerufen. Dieses erste Programm seiner Art verlangte von Händlern und Dienstleistern die Einhaltung von ganz spezifischen Datenschutz-Anforderungen. Einige Jahre später schlossen sich Visa, MasterCard, American Express, Discover, Diner*s Club und JCB zusammen und führten den Payment Card Industry Data Security Standard ein, eine aktualisierte und umfassende Version des Standards, der im Juni 2005 für alle Händler und Dienstleister verbindlich wurde. Im September 2006 wurde der Standard erneut aktualisiert und enthält seitdem rund 160 Anforderungen, die seit Ende Juni 2007 verpflichtend sind. Dabei handelt es sich keineswegs um reines Papierwerk. Allein im Jahr 2006 hat Visa im Gesamtwert von 4,6 Millionen Dollar Klagen gegen Händler eingereicht, die sich nicht an die Standards gehalten haben. Das sind rund 35 Prozent mehr als im Jahr davor.

Die Strafen haben es ohnehin in sich: Sie reichen von 50.000 USD pro Tag für Nichteinhalten der Compliance-Richtlinien bis zu 500.000 USD für einen Vorfall, bei dem Daten entwendet wurden. Und in diesen sauren Apfel müssen alle Unternehmen beißen. Es ist ein Trugschluss, zu glauben, dass zum Beispiel nur Händler verpflichtet sind, diese Standards einzuhalten. Auch Dienstleister und jedes andere Unternehmen, das Daten über Kreditkartenhalter speichert, verwendet oder überträgt, kann haftbar gemacht werden, wenn die Regeln nicht eingehalten werden. Es gibt auch keine halbe Lösung, alle Unternehmen müssen zu 100 Prozent die Compliance-Anforderungen einhalten. Der Standard ist nicht nur ein Ziel, das zu erreichen lohnt, sondern ein Muss. Bisher haben die Kreditkartenfirmen zwar kaum Kontrollen in Deutschland durchgeführt, sondern sich vorrangig auf die USA konzentriert; das kann sich aber bald ändern.

Die Händler müssen daher rasch handeln, wenn sie es nicht schon längst getan haben. Die Risiken und möglichen Kosten sind einfach zu hoch. Das Ganze hat nur einen Haken: Nur sehr wenige Unternehmen verfügen über die nötige IT-Infrastruktur und die Ressourcen, um die ehrgeizigen und weitreichenden Anforderungen schnell umzusetzen. Bis zu 20 Prozent der Händler sind heute immer noch nicht auf einer Linie (compliant) mit dem Standard. Manche Unternehmen entscheiden sich für eine einfache Lösung, die aber meist wenig ausgereift und von Dauer ist. Wesentlich Erfolg versprechender und langfristiger ist ein sorgfältig geplanter strategischer Ansatz, von dem auch andere IT Bereiche profitieren. Die 160 Richtlinien lassen sich - je nach Sichtweise - zum Beispiel in sechs Kontrollziele zusammenfassen:

Aufbau und Unterhaltung eines sicheren Netzwerkes

Die Daten von Karteninhabern müssen gegenüber externen Zugriffen geschützt werden. Grundlage dafür ist

eine sichere Infrastruktur mit Firewalls und Überwachungs-Systemen. Viele Unternehmen haben zwar Firewalls im Einsatz, aber oftmals sind diese mangelhaft konfiguriert und werden nur selten überprüft, so dass sie viele Schwachstellen aufweisen.

Lösungen, die Identitäten managen, Zugriffsrechte kontrollieren und sich in Firewalls einbinden lassen, reduzieren die Zeit und den Aufwand, der sonst zur Wartung der Schutzwälle notwendig ist. Der neue PCI Standard schreibt vor, dass eine funktionstüchtige Firewall die Daten schützt und dass keine voreingestellten Passwörter oder anderen Sicherheitsparameter verwendet werden.

Schutz der Kreditkartendaten

Falls ein Hacker oder ein interner Mitarbeiter doch einmal Zugriff auf geschlossene Bereiche erlangen sollte, ist es wichtig, dass die Daten durch Verschlüsselung, automatische Vernichtung oder weitere Zugriffsbeschränkungen dennoch geschützt sind. Ohne Identitätsmanagement lassen sich solche Prozesse und Funktionalitäten nur schwer und vor allem kostspielig abbilden. Insgesamt soll das Speichern von Daten der Kreditinhaber ohnehin auf ein Minimum reduziert werden.

Wenn vertrauliche Informationen weitergeleitet werden, müssen diese immer verschlüsselt sein.

Unterhaltung eines Programms zu Abwehr von Schwächen

Viele Viren werden geschrieben, um vertrauliche Daten auszukundschaften. Die Anwendungen im Unternehmen müssen dagegenhalten und dafür sind sie oft nicht gerüstet. Der PCI Standard zwingt die Händler und Dienstleister Maßnahmen zu ergreifen, um potentielle Schwachstellen zu identifizieren und auszumerzen. Dafür müssen die Systeme immer auf dem neuesten Stand sein. Gleichzeitig müssen alle, die diese Updates einpflegen, kontrollierten und isolierten Zugriff auf die jeweiligen Systeme erhalten. Andernfalls entsteht gleich hier eine entscheidende Sicherheitslücke.

Implementierung starker Zugriffs-Kontrollmechanismen

Die Daten von Kreditkartenhaltern darf nur der einsehen, der sie tatsächlich benötigt. Dies klingt selbstverständlich, ist es aber meistens nicht. Am sichersten ist es, den Zugriff von vornherein für alle zu sperren und dann vereinzelte Ausnahmen zuzulassen. Automatisierte Lösungen liefern hier den besten Ansatz. Zusätzlich muss jeder Person, die Zugriff auf einen Computer hat, eine eindeutige Identität zugeordnet werden. Nur so kann Missbrauch vorgebeugt werden. Viele Einzelhändler haben eine großes Netz an Nutzern, Systemen, Datenbanken und Anwendungen, die über eine zentrale Lösung verwaltet werden müssen. Auch der physische Zugriff muss natürlich kontrolliert werden. Am besten lässt sich das über so genannte Token, also Zugangskarten, realisieren.

Regelmäßige Überwachung und Tests der Netzwerke

Der neue Standard erfordert, dass jeder Zugriff auf Systeme, die mit den sensiblen Kartendaten agieren, überwacht und aufgezeichnet wird. Das geht bis hinunter auf die untersten Ebenen. Damit ist sichergestellt, dass es der IT-Abteilung nicht langweilig wird - es sein denn, eine automatisierte Lösung, die Zugriffsüberwachung, Alarm und Reports eng verknüpft, ist im Einsatz.

Einsatz einer Regel für Datensicherheit

Ganze 40 Einzelregeln fallen unter das Ziel, eine Richtlinie für Datensicherheit aufzustellen. Darin enthalten sind jährliche Prozesse, um die Gefahren und Schwachstellen zu identifizieren, jährliche Risiko- sssessments, tägliche Sicherheitsprozeduren und vieles mehr.

Die meisten dieser Ziele drehen sich um das Konzept eines eingeschränkten, kontrollierten Zugriffs. Es darf nur der, der wirklich befugt ist, auf die Daten von Kreditkartenhaltern zugreifen. Jede Lösung muss daher ausgeprägte Funktionalitäten zur Verwaltung von Identitäten mit sich bringen und eng mit Zugriffskontrolle und Überwachungsmöglichkeiten verknüpft sein. Ohne ein stabiles Set automatisierter Werkzeuge für Identitäts- und Zugriffsmanagement ist die Einhaltung der PCI Standards praktisch unmöglich. Andererseits schützt eine Identitätsmanagement-Lösung dann auch alle anderen sensiblen Daten im Unternehmen, regelt den Zugriff und bindet Geschäftspartner und Kunden verlässlich und kontrolliert ein. Neben den 160 Fliegen des PCI Standards, sind das also noch ein paar mehr, die sich mit einer Klappe erledigen lassen.

Die Kreditkartenunternehmen sind zufrieden, die Händler müssen keine Betrugsfälle oder Strafen fürchten und für den Kunden macht Bezahlen mit der Kreditkarte wieder Spaß - wovon dann alle Parteien profitieren - zumindest so lange bis die nächste Kreditkartenabrechnung ins Haus flattert.

Über Novell

Novell, Inc. (Nasdaq: NOVL) bietet Infrastruktur-Software für das Open Enterprise an. Novell ist eines der führenden Unternehmen bei unternehmensweiten Betriebssystemen für Unternehmen auf Basis von Linux und Open Source sowie bei Sicherheits- und System Management Services, die benötigt werden, um heterogene IT-Umgebungen zu betreiben. Novell unterstützt seine Kunden dabei, Kosten, Komplexität und Risiken zu reduzieren, damit sie sich auf Innovation und Wachstum konzentrieren können. Das Unternehmen mit Hauptsitz in Waltham, Massachusetts (USA), beschäftigt weltweit rund 4.700 Mitarbeiter. Seit 1986 ist Novell durch die Novell GmbH in Düsseldorf auch auf dem deutschen Markt vertreten. Von diesem Standort aus werden Vertrieb und Marketing für Deutschland, Österreich und die Schweiz koordiniert - Niederlassungen befinden sich in Berlin, Frankfurt, München, Nürnberg, Wien, Zürich und Genf. Weitere ausführliche Informationen über Novell Lösungen, Produkte und Services stehen im Internet zur Verfügung unter www.novell.com oder www.novell.de.

Pressekontakt:

Lars Basche
Text 100 Public Relations
Tel: +49 - (0)89 - 99 83 70-33
E-Mail: novell@text100.de

Ihre Ansprechpartnerin bei Novell:
Ulrike Beringer
PR Manager Novell Central Europe
Tel: +49 - (0)89 - 206002118
E-Mail: uberinger@novell.com