Stolpersteine bei der Verwaltung von Kreditkartendaten

Cloakware Password Authority: zur Einhaltung von Vorschriften der Payment Card Industry

Frankfurt/Vienna (Virginia), 04. Juni 2009 – Cloakware, Hersteller von innovativen Sicherheitslösungen, hat die fünf häufigsten Fehler bei der Verwaltung von Kreditkartendaten identifiziert:

1. **Benutzung von Default Passwörtern der Hersteller**
   Default Passwörter werden voreingestellt vom Hersteller ausgeliefert. Via Internet können sich Hacker und eigene Mitarbeiter diese aber jederzeit problemlos beschaffen und so den Zugriff auf kritische Unternehmensdaten erlangen. Unternehmen sollten diese Passwörter nach der Installation daher ändern und regelmäßig aktualisieren.

2. **Ungesicherter Zugriff auf Kreditkartendaten**
   Oftmals werden Administratorpasswörter in Tabellenkalkulationen wie Excel verwaltet. Dies macht es nicht autorisierten Personen leicht, daran zu gelangen und sich somit Zugriff auf die Kreditkartendaten von Kunden zu verschaffen. Unternehmen sollten an dieser Stelle ein sicheres System für das Passwortmanagement privilegierter Nutzer einsetzen.

3. **Zu viele Rechte**
   Um die Verwaltung zu vereinfachen, neigen Unternehmen dazu, Rechte auf Datenbanken und Applikationen nicht granular genug zu vergeben. Um den Zugriff unbefugter Angestellter auf kritische Daten zu unterbinden, sollten Unternehmen hier zumindest gruppen- und rollenbasierende Rechte vergeben.

4. **Keine Nachvollziehbarkeit**
   Bei der gemeinsamen Nutzung von Passwörtern kann nie zweifelsfrei sichergestellt werden, wer tatsächlich auf ein System zugegriffen hat. Die Vergabe eindeutiger Identitäten löst dieses Problem, vergrößert aber gleichzeitig den Aufwand für die Verwaltung. Ein geeignetes Passwort-Managementsystems eliminiert diese Schwachstellen.

5. **Kein Monitoring**
   Auch eine einfache Berechtigungskontrolle reicht oft nicht aus. Unternehmen sollten den Zugriff auf alle relevanten Systeme daher aktiv überwachen. So wird die Dauer erfolgter Regelverstöße minimiert. Aktives Monitoring ist an dieser Stelle ein effizientes Mittel der Risikominimierung.

Aufgrund der Häufigkeit derartiger Problemfälle sollten Unternehmen geeignete Gegenmaßnahmen ergreifen. Password Authority, eine Sicherheitslösung von Cloakware, automatisiert und vereinfacht das Management von A2A (Application-to-Application)- und Administrator-Passwörtern in Unternehmen. Die zentralisierte und auf Richtlinien basierende Kontrolle sorgt für die Einhaltung aller maßgebenden Richtlinien (Compliance-Anforderungen) und regelt, wer auf kritische Systeme und Daten zugreifen darf. Zudem senkt die Automatisierung des Passwort-Managements die administrativen Kosten und eliminiert Ausfallzeiten, die üblicherweise mit der manuellen Änderung von A2A-Passwörtern einhergehen. Gleichzeitig verhindert sie sogar Systemausfälle, wie sie oftmals durch falsche oder fehlende sogenannte Credentials (Benutzername/Passwort) verursacht werden. Insofern spart Password Authority Zeit und Geld, während die Verfügbarkeit und der Leistungsumfang, die sogenannten Service Levels, gesteigert werden.

Lösungen von Cloakware unterstützen den Payment Card Industry Data Security Standard (PCI). Dabei handelt es sich um ein Regelwerk für den Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht. Der Standard wird von

allen wichtigen Kreditkartenorganisationen unterstützt.

Über Cloakware
Cloakware, ein Bereich von Irdeto und Teil der Naspers Group, ist Hersteller von innovativen Sicherheitslösungen. Cloakware´s patentierte Produkte bieten jenen umfassenden Schutz, den Behörden, Firmen und Endanwender benötigen, und schützen heute bereits über eine Milliarde Applikationen und Produkte der namhaftesten Unternehmen weltweit. Cloakware Password Authority unterstützt Organisationen bei der Einhaltung von Regularien wie GRC (Governance, Risk, Compliance), SOX und PCI. Der Hauptsitz von Cloakware ist Vienna (Virginia, USA). Das Unternehmen hat Niederlassungen in Ottawa, Kanada und regionale Vertriebsbüros in den USA und Europa. Mehr Informationen unter: http://datacenter.cloakware.com.

Über Digital Hands
Die Digital Hands GmbH unterstützt IT-Hersteller aus den Bereichen Security und Networking beim Aufbau von Vertrieb und Marketing in Europa. Das Service Portfolio reicht von Value Added Distribution über Marketing und PR bis zu technischem Support und Training. Mit erfahrenen, professionellen Mitarbeitern und Kontakten zu Channel Partnern und Endkunden in ganz Europa bietet Digital Hands schnelle Marktdurchdringung und Vertriebserfolg. www.digital-hands.eu

Mehr Informationen:
Cloakware
Keimstraße 9
D-63225 Langen

Thomas Fink
Marketing Director Central Europe
T: +49 6103 270 265
F: +49 6103 270 266
M: +49 163 6050350
E-Mail: thomas.fink@cloakware.com
URL: http://datacenter.cloakware.com

Pressekontakt:
Riba:BusinessTalk GmbH
Klostergut Besselich
56182 Urbar / Koblenz

Aki Blum
PR-Beratung
T: +49 261-963757-23
F: +49 261-963757-11
E-Mail: ablum@riba.eu
URL: www.riba.eu
URL: www.eprf.eu