

Sicherheitspanne bei Fannie Mae exemplarisch

Cloakware empfiehlt Richtlinien zum Management privilegierter Passworte

Frankfurt/Vienna (Virginia), 31. März 2009 – Konzerne sollten ihre bisherige Sicherheitspolitik für privilegierte Accounts überdenken. Wie ein aktueller Vorfall bei der Hypothekenbank Fannie Mae zeigt, sind vor allem die Kontrollen von Passwörtern und damit verbundenen Privilegien häufig verbesserungswürdig.

Die aktuell angespannte wirtschaftliche Lage führt dazu, dass die Daten von Firmen wachsender Gefahr ausgesetzt sind. Durch Stellenabbau, Umstrukturierungen und Übernahmen entstehen Lücken in der IT-Security. Diese werden von unzufriedenen Mitarbeitern, Geschäftspartnern oder externen Saboteuren gezielt gesucht und ausgenutzt. Firmen drohen dadurch der Verlust wertvoller Daten, negative juristische Folgen, finanzieller Schaden und ein beschädigtes Image. Dieses kann auf Grund der wirtschaftlich angespannten Situation weitaus gravierende Folgen verursachen als üblich. Ereignisse also, die sich Unternehmen heute nicht mehr "leisten" können.

Der große amerikanische Finanzdienstleister Fannie Mae musste kürzlich einen derartigen Vorfall zugestehen. Durch Zufall hatte das interne IT-Team einen Wurm entdeckt, der Millionen von Hypothekeneintragungen gelöscht und den Zugriff auf das System für eine Woche unterbunden hätte. Ein früherer Mitarbeiter hatte den Wurm eingeschleust. Solche Vorfälle lassen sich vermeiden. Cloakware empfiehlt Firmen drei Maßnahmen, um derartige Einbrüche wesentlich zu erschweren und die internen Daten besser abzusichern.

Erstens sollten IT-Verantwortliche dokumentieren, wer auf privilegierte Informationen zugreifen darf. In einem zweiten Schritt sollten sie angemessene Regelungen erlassen und umsetzen, die sensible Daten vor unautorisiertem Zugriff schützen. Schließlich sollten sie die Zugriffs- und Sicherheitsregeln regelmäßig an die aktuelle Situation anpassen und ihre Wirksamkeit überwachen. Beachten Unternehmen diese einfachen Grundsätze, verbessern sie die Kontrolle über die Zugriffe auf wichtige Datenbestände bereits entscheidend.

"Vor allem für Firmen, die ihre Organisation verkleinern oder umstrukturieren, ist es entscheidend, Unternehmenswerte zu sichern und den Zugriff auf wesentliche Informationen zu schützen", betont David Canellos, President und Chief Operating Officer von Cloakware. "Dabei sind es oft Insider, denen man blind vertraut, von denen die größte Gefahr ausgeht, sofern ihre Zugriffe unkontrolliert bleiben."

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 Consumer 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: www.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 Vertriebs Erfolg. 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