Special Innovation

Effizienter Datenschutz

Informationstechnologie-Sicherheit für das 21. Jahrhundert muss nicht kompliziert sein: Eine Karte und ein Code ermöglichen Nutzern den Zugriff auf alle firmeninternen Anwendungen – vorausgesetzt, sie sind dazu berechtigt. Secure Identity Management bringt Unternehmen verbesserten Datenschutz und erhöhte Datensicherheit.

Sonja Gerstl

Klare Kompetenzverteilung: Nicht alle Mitarbeiter eines Unternehmens verfügen über uneingeschränkten Zugang zu heiklen Firmeninformationen. Ein effizienter Datenschutz verhindert unbefugte Zugriffe. Foto: Bilderbox.com

Firmennetzwerke sind mitunter äußerst komplexe Gebilde. Schließlich müssen Unternehmen mitilfe der Netzwerke in der Lage sein, Beziehungen zu recht unterschiedlichen Gruppen zu unterhalten oder zu verwalten. Mitarbeiter, Kunden und Geschäftspartner verlangen ein differenziertes Identitäts- und Zugriffsmanagement. Und das ist fürwahr keine einfache Aufgabe, der sich die Informationstechnologie (IT)-Abteilungen von Firmen zu stellen haben.

„Viele Unternehmen managen die Zutritts- und Zugriffsberechtigungen noch sehr undurchgängig. Dies birgt hohe Sicherheitsrisiken, vor allem im Hinblick auf die Informationssicherheit“, weiß Wilfried Pruschak, Geschäftsführer von Raiffeisen Informatik, um die Problematik Bescheid.

Überblick behalten

Denn meist ist es so, dass verschiedene Anwendungen und Systeme eine separate Verwaltung von Nutzern und deren Zugriffsrechten bedingen. Als Folge davon besitzen die Nutzer eines Netzwerks oftmals eine Vielzahl untereinander nicht abgestimmter, digitaler Identitäten und Berechtigungen für diverse Systeme, die sich nur noch unter einem enormen administrativen Aufwand überblicken lassen. Und das wiederum führt zu einem erhöhten Risiko von sogenanntem „Identitätsdiebstahl“ und unautorisierten Zugriffen. Auch die Einhaltung von gesetzlichen Vorschriften und Regularien (Compliance) ist unter solchen Voraussetzungen kaum möglich. Aufseiten von Raiffeisen Informatik setzt man daher bereits seit geraumer Zeit auf das sogenannte Secure Identity Management (SIM).

Über SIM ist ein einfacher Zugang zu allen Anwendungen und Systemen für autorisierte Benutzer möglich. Herzstück des Sicherheitssystems ist eine Smartcard mit Chip, die in Verbindung mit einem individuellen Zugangscode den einzelnen Nutzer dazu berechtigt, auf autorisierte Systeme zuzugreifen. Der Mitarbeiter erfährt seine Passwörter nicht, muss sie sich deshalb auch nicht merken und kann sie daher auch nicht mehr vergessen. Eine aufwendige Verwaltung durch den Helpdesk fällt somit ebenfalls flach. Verlässt der Mitarbeiter seinen Arbeitsplatz, zieht er die Karte aus dem Kartenleser, und alle Systeme oder Anwendungen sind automatisch vor unautorisierten Zugriffen geschützt.

Professioneller Schutz

„Secure Identity Management bietet einen einfachen Zugang für User, erhöht die Zeitersparnis in der Administration und die Sicherheit im Unternehmen. Es bietet dadurch mehr Effizienz bei firmeninternen Prozessabläufen. In Bezug auf IT-Sicherheit ist das sicherlich ein Thema der Zukunft. Wir haben SIM bereits im Einsatz und sind diesbezüglich Vorreiter auf dem österreichischen IT-Markt“, betont Pruschak.

Vor allem für die EDV-Abteilungen ist die einheitliche Administration über standardisierte Workflows eine wesentliche Erleichterung. Die Berechtigungsvergabe erfolgt funktionsbezogen über User-Rollen. Das bringt verbesserten Datenschutz und erhöhte Datensicherheit mit sich. Zudem profitiert das Unternehmen von der Protokollierung, Auswertung und Archivierung der Vergabe von Nutzer-Rechten. Konkret bedeutet das, dass jeder Nutzer während der gesamten Zeit seiner Betriebszugehörigkeit relativ einfach gemanagt werden kann. Die Zugriffsrechte werden dem jeweiligen Aufgabenbereich im Unternehmen angepasst – ändern sich Kompetenzen, kann auf Knopfdruck die Nutzeridentität im neuen Anforderungsprofil entsprechend modifiziert, aber auch vorübergehend außer Kraft gesetzt, widerrufen oder gar endgültig aufgehoben werden.

Die Kernfunktionalitäten von SIM bestehen aus einem „Identity Management“, einer „Single-Sign-on“-Lösung und einer Public Key Infrastructure. Identity Management bezeichnet dabei die Funktion, den „richtigen“ Mitarbeitern zur rechten Zeit den berechtigten, gesicherten Zugang zu Applikationen, Ressourcen und Daten des Unternehmens zu verschaffen. Kernstück der Sicherheitsinfrastruktur ist eine Public Key Infrastructure. Der Zugang erfolgt via Nutzer-Zertifikate mit zweifacher Authentifizierung – das heißt, der Nutzer benötigt Passwort und Karte. Die „Single-Sign-on“-Lösung schließlich verbessert die Bedienungsfreundlichkeit der IT-Systeme für Anwender: Eine einzige Anmeldung reicht für alle angebundenen Systeme.

www.r-it.at

Alexis Kahr: „Video nimmt an Bedeutung zu. Viele verbreiten Nachrichten nicht mehr per E-Mail, sondern mittels Video“, erklärt der Business Development Manager von Cisco Österreich.

Intelligent eingebunden

***economy:** Einer der Schwerpunkte, denen man sich bei Cisco im Jahr 2008 verstärkt widmen will, lautet „Collaboration“. Was genau planen Sie in diesem Zusammenhang?*

Alexis Kahr: „From Communication to Collaboration“ beschreibt sehr gut die Entwicklung in Richtung umfassender Zusammenarbeit intern als auch extern von und zwischen Organisationen. Die völlige Integration von Mobility, Unified Communication, Video, Applikationen sowie Geschäftsprozessen und das Angebot von verschiedensten neuen „Collaborative Tools“ eröffnet Unternehmen neue Möglichkeiten. Im Mittelpunkt steht der einzelne Kunde, der Mitarbeiter – also der Mensch. Cisco wird 2008 einige Innovationen auf den Markt bringen, die einen Meilenstein in Richtung Collaboration darstellen.

Ein weiteres großes Thema ist der Einsatz von Video-Kommunikation oder Unified Communications. Welche Neuerungen kommen hier auf uns zu?

2007 war für Cisco ein großer Erfolg für die Telepresence-Lösungen. Das Feedback unserer Kunden war überwältigend. Video wird in Unternehmen immer mehr an Bedeutung zunehmen. Viele verbreiten wichtige Nachrichten nicht mehr per E-Mail, sondern mittels Video. Schulungen und Informationen werden immer häufiger als Video on Demand verbreitet. 2008 wollen wir vollständige Integrationen dazu vorstellen. Das Endgerät wird immer flexibler – das heißt, Handy, PDA, Softphone, Internet-Telefon, WLAN und so fort sind voll eingebunden.

Ihre Prognose für 2008: Welche „Techniken“ oder „Services“ werden an Relevanz gewinnen, welche in der Versenkung verschwinden?

Intelligente Netzwerke rücken immer mehr ins Zentrum. Der „dumme“ Switch allein reicht nicht mehr aus, um die neuen Möglichkeiten zu unterstützen. Wir sehen auch einen ganz deutlichen Trend in Richtung Managed Services, wie zum Beispiel Managed Security. Gerade bei Klein- und Mittelbetrieben ist der Bedarf dafür unseres Erachtens sehr groß. *sog*

www.cisco.at

Zur Person

Alexis Kahr ist Business Development Manager bei Cisco Österreich. Foto: Cisco