Mit Identitäten Zugriffe regeln

07.10.2008, 11:41 | IT, New Media & Software

Pressemitteilung von: *all-about-security.de*
Presseagentur: *IT Kaktus*

Mit der Optimierung ihrer Geschäftsprozesse verfolgen Unternehmen hauptsächlich drei Ziele: Kosteneinsparungen, Sicherheit und Compliance gegenüber internen und externen Auflagen. Eine Möglichkeit, diese Vorhaben elegant miteinander zu verbinden, ist ein umfassendes Identity und Access-Management (IAM) – ein unverzichtbarer Eckpfeiler jeder modernen IT-Sicherheitsinfrastruktur.

Aschheim, 07. Oktober 2008 - Immer mehr Firmen gehen heute dazu über, Basisdaten zu ihren Mitarbeitern als virtuelle Identität abzuspeichern und zu verwalten. Auf dieser Basis können sie festgelegen, welche Rechte die einzelne Person bezüglich Anwendungen und Daten besitzt. Durch den zentralen Verwaltungsansatz von IAM lassen sich verlässliche Zugriffskontrollen auf alle Applikationen etablieren und unberechtigte Zugreifer sicher abwehren. Siemens IT Solutions and Services hat diesen Ansatz jüngst um eine physikalische Komponente erweitert: "Ein zentrales Rollenmodell regelt dabei nicht nur die IT-Zugriffe, sondern auch Zugänge zu Gebäuden und Anlagen – bei Bedarf mit biometrischen Systemen", erklärt Reinhard Bertram, verantwortlich für den Bereich Security bei Siemens IT Solutions and Services.

An Identifikation und Anmeldung schließt sich die Frage an: Auf welche Daten und Systeme darf die Person zugreifen und auf welche nicht? Die entsprechenden Rechte erteilt, verweigert oder entzieht das Siemens-Produkt "DirX" automatisch. Entscheidungsbasis sind die vorher individuell festgelegten Befugnisse und definierten Rollen, etwa Vertriebsleitung, Einkauf oder Projektmanager. Übernimmt ein Mitarbeiter eine neue Aufgabe im Unternehmen, werden die Zugriffsrechte sofort an seine neue Rolle angepasst. Die automatische Vergabe der Rechte steigert die Produktivität und senkt Fehlerquoten sowie die Kosten für Administration.

Zentrales Benutzermodell für Compliance und Sicherheit

Da alle Identitäten und Rechte immer eindeutig und auf dem aktuellsten Stand sind, lassen sich die international steigenden Compliance-Anforderungen einfach erfüllen. Bei Bedarf können Firmen lückenlos nachvollziehen, wer wann was wo geändert hat. "Gerade mit Blick auf rechtlich verbindliche Vorgaben kann dies dem Unternehmen erhebliche Schadensersatzzahlungen und den Geschäftsverantwortlichen gegebenenfalls noch härtere Folgen ersparen", betont Bertram.

Ein Beispiel für ein zentrales Benutzermodell ist die Public Key Infrastructure (PKI), die heute bereits bei vielen Behörden im Einsatz ist. Das System ermöglicht es, digitale Zertifikate auszustellen und zu verteilen. Es kann über Smartcards auch mit den Zugangsrechten zu Anwendungen und Gebäuden kombiniert werden. So hat Siemens IT Solutions and Services etwa die Mitarbeiter der Deutschen Rentenversicherung Bund sowie der Deutschen

Rentenversicherung Rheinland mit 60.000 Chipkarten ausgestattet. Damit können sich die Angestellten im elektronischen Schriftverkehr zweifelsfrei identifizieren, E-Mails verschlüsseln und Dokumente signieren. Doch die flexiblen Karten bieten noch mehr Funktionen: Neben der hochsicheren Zugangs- und Zugriffskontrolle lassen sich auch die Arbeitszeit automatisch erfassen, Parkschranken öffnen oder bargeldlos in der Kantine zahlen.

Auch die Bundesagentur für Arbeit hat sich für die Einführung einer PKI entschieden, um sichere elektronische Geschäftsprozesse zu gewährleisten. Der IT-Dienstleister hat dort ein Trust Center eingerichtet, das etwa mit einem Passamt vergleichbar, die Zertifikate und Schlüssel ausstellt, und versorgt die Mitarbeiter mit Chipkarten für qualifizierte Signaturen. Entscheidend für die sichere Verteilung der Schlüssel und damit der digitalen Identitäten ist die Public Key Infrastructure (PKI). So lassen sich zwingende verwaltungsrechtliche Vorgaben wie eine lückenlose Protokollierung bei Entscheidungs- und Aushandlungsprozessen einhalten.

Schlüssel für elektronische Signatur

Um elektronische Unterschriften zu erzeugen, benötigt der Benutzer ein Schlüsselpaar mit einem Public Key und einem Private Key. Diese bilden die Basis eines asymmetrischen Codierungsverfahrens: Der Besitzer signiert Dokumente mit seinem Private Key und der Eingabe einer PIN, die nur ihm bekannt ist. Der Empfänger kann mit dem Public Key, der allgemein bekannt gemacht wird, die Signatur prüfen. Derzeit ist die Speicherung auf einer Smart Card der einzig gesetzlich gangbare Weg, den privaten Schlüssel aufzubewahren.
Die Zuordnung der öffentlichen Schlüssel zu einer Person erfolgt durch Zertifikate – eine Art elektronisch beglaubigter Ausweis. Das Zertifikat ordnet der digitalen Identität bestimmte Eigenschaften wie E-Mail-Adresse, Name oder Anschrift zu und beglaubigt den öffentlichen Schlüssel. In einem Corporate Directory werden die Zertifikate verteilt. Je nach Ausführung lässt sich die Gültigkeit online via OCSP (Online Certificate Service Protocol) oder mittels aktueller Sperrlisten (Certificate Revocation Lists – CRL) steuern – etwa bei Verlust.

Weitere Informationen zum Thema Identity- & Access-Management bietet das IT-Security-Portal dem interessierten Leser in seinem Thema des Monats unter:

http://www.all-about-security.de/kolumnen/thema-des-monats/

Portrait

www.all-about-security.de ist ein branchenorientiertes, aber dennoch offenes IT-Security-Portal. Das Portal holt das oft verdrängte Thema der IT-Security schonungslos zurück in das Rampenlicht -unbequeme Fragen und die passenden Antworten inbegriffen. Für alle und über alle Betriebsgrößen hinweg.

News-ID: 248433 • Views: 1181 (Stand: 21.07.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/248433/Mit-Identitaeten-Zugriffe-regeln.html