Special Innovation

Sicherheit durch Identifikation

Chipkartenbasierte Zugangssysteme ermöglichen klare Rollenvergabe und sparen Zeit.

Ernst Brandstetter

Schutz für sensible Daten durch Chipkarten-Identifikation. Damit wird vermieden, dass es zu unterschiedlichen Rechteverteilungen in verschiedenen Systemen kommt. Zudem bleibt der Überblick über die Berechtigungen stets voll erhalten. Foto: Thiel Logistik

In großen Unternehmen geht es oft lustig zu, was die Computersicherheit betrifft: Passwörter werden einfach oder mehrfach verwendet, vergessen, notiert, verlegt, und oft weiß niemand mehr, wer Zugang haben darf oder nicht. Denn auch bei Benutzer-Accounts herrscht gerne Chaos, es gibt Dubletten, Sperren werden vergessen oder verschlampt, und die Benutzerstammdaten in unterschiedlichen Systemen sind nicht standardisiert. Eine Dokumentation über Änderungen ist meist nicht vorhanden oder hoffnungslos veraltet.

Der größte Schaden nach einem Sicherheitsvorfall in IT-Systemen liegt für Unternehmen im Verlust geschäftskritischer Daten, erklärten 82 Prozent der Befragten einer unter 100 IT-Experten erhobenen Untersuchung der deutschen Nationalen Initiative für Internet-Sicherheit (Nifis e.V.). Danach folgen der Ausfall produktiver Systeme (72 Prozent) und finanzielle Schäden, wobei 66 Prozent hier „teilweise“ und nur 14 Prozent mit einem klaren „Ja“ zustimmen. 63 Prozent der Unternehmen hatten im vergangenen Jahr Probleme mit der Informationssicherheit zu bewältigen.

Hinter dem Verlust geschäftskritischer Daten folgt an zweiter Stelle mit 72 Prozent der Stimmen die lange Ausfallzeit produktiver Systeme. Ein Ausfall der Produktivsysteme hat für die meisten Unternehmen weitreichende Konsequenzen, wenn dadurch Produktion oder Absatz nicht möglich sind. Mehr als die Hälfte der Fachleute (52 Prozent) sieht darüber hinaus im Imageverlust ein besonderes Problem. Wenn ein Sicherheitsvorfall in der Öffentlichkeit bekannt wird, kann der Folgeschaden infolge von Kündigungen seitens bestehender Kunden und fehlender neuer Geschäftsabschlüsse sogar liquiditätsbedrohend sein, so das Ergebnis der Umfrage.

Die Lösung sei ein professionelles Secure Identity Management (SIM), erklärt der Geschäftsführer der Raiffeisen Informatik Wilfried Pruschak. Eine Karte und ein Passwort ermöglichen dann den gesicherten, berechtigten Zugang zu allen firmeninternen Anwendungen. Das wird besonders bei sicherheitsrelevanten Bereichen oder bei Gefahr von unberechtigten Datenzugriffen immer wichtiger.

„Der Zugriff zu unternehmenskritischen Daten muss koordiniert, kontrolliert sowie gesichert ablaufen“, erklärt Pruschak, der aus Erfahrung weiß, dass „viele Unternehmen die Zutritts- und Zugriffsberechtigungen noch sehr undurchgängig managen.“ Das aber birgt hohe Sicherheitsrisiken, vor allem im Hinblick auf Informationssicherheit. Secure Identity Management von Raiffeisen Informatik steuert die Berechtigungen über eine einzige Karte mit Chip und in Verbindung mit einem Code. Damit können sich User auf allen Systemen, für die sie berechtigt sind, einloggen. Man muss sich dann auch nicht mehr für jede Applikation erneut anmelden. Verlässt man den Arbeitsplatz, wird die Karte aus dem Lesegerät entfernt, und alle Systeme sind automatisch vor fremdem Zugriff geschützt. Pruschak: „Das bringt zusätzliche Zeitersparnis in der Administration sowie Sicherheit im Unternehmen und bietet dadurch mehr Effizienz.“

Einfache Handhabung

Die einheitliche Administration derartiger Karten über standardisierte Workflows erleichtert zudem die User-Administration erheblich. Die Berechtigungsvergabe erfolgt funktionsbezogen über User-Rollen. Darüber hinaus profitiert das Unternehmen von der Protokollierung, Auswertung sowie Archivierung der Vergabe von User-Rechten und ist von diversen Routinetätigkeiten wie etwa dem Passwortrücksetzen entlastet. Für alle Typen von Mitarbeitern können bestimmte Rollen festgelegt werden, die zentral verwaltet werden.

Info

- **Secure Identity Management (SIM).** Die Kernfunktionalitäten von SIM bestehen aus Identity Management, einer Single-Sign-on-Lösung und Publik Key Infrastructure. Die SIM-Lösung vereinfacht Benutzerverwaltungsprozesse erheblich und dient als zentrales System für benutzerrelevante Daten. So werden einerseits Kosteneinsparungen in der Administration erzielt, andererseits der Sicherheitsstandard auf aktuellem Stand gehalten.

- **Identity Management (IM).** IM ermöglicht den richtigen Personen zur rechten Zeit den gesicherten Zugang zu Applikationen, Ressourcen und Daten.

- **Public Key Infrastructure (PKI).** Als Kern der Sicherheitsinfrastruktur kommt PKI zum Einsatz. Sie ermöglicht mittels User-Zertifikaten eine Authentifizierung über die Karte und zusätzlich über ein Passwort. Weiters bietet dieses System die Basis für die Bereitstellung von Zertifikaten, welche für Sicherheitsfunktionen wie Vertraulichkeit, Integrität und Nicht-Abstreitbarkeit von diversen Applikationen genutzt wird.

- **Single-Sign-on.** Mit einem Log-in können alle Systeme genützt werden, zu denen man zugangsberechtigt ist. Das verbessert die Bedienungsfreundlichkeit der IT-Systeme für Anwender, weil sich Mitarbeiter für alle angebundenen Systeme nur einmal authentifizieren/anmelden müssen.

Steckbrief

Wilfried Pruschak ist Geschäftsführer der Raiffeisen Informatik GmbH.
Foto: Raiffeisen