Zugangssysteme verhindern IT-Pannen

Unternehmen versprechen sich viel von der Einbindung ihrer Wertschöpfungs-Prozesse in die IT-Umgebung. Damit das nicht auf Kosten der Sicherheit geht, sollten sie die Daten mit einem automatisierten und zentralisierten System verwalten und überwachen.

von Felix Weber

Schneller, besser, effizienter: das sind die Anforderungen, die viele Unternehmen an sich selbst stellen, um im hart umkämpften Markt bestehen zu können. Erreichen können sie dies, indem sie Mitarbeitende, Partner und Kunden in eine möglichst durchgängig IT-basierte Wertschöpfungskette einbinden. Mit einem solchen System gehen die Unternehmen allerdings Sicherheitsrisiken ein, die nicht unterschätzt werden dürfen: Plötzlich haben Unberechtigte Zugriff zu Anwendungen und Daten, die sie gar nichts angehen.

Um das zu verhindern, muss das Unternehmen den Systemzugang strikte einschränken. Die berechtigten Benutzer müssen klar definiert und mit den erforderlichen Schlüsseln ausgerüstet werden. Und, mindestens ebenso wichtig: Wenn sie die Berechtigung aus irgend einem Grund verlieren, müssen ihre Codes sofort ungültig gemacht werden. Bei den heute üblichen Sicherheitssystemen ist das erschreckend oft nicht der Fall: Nach einer Studie der Meta Group jedenfalls behält etwa jeder vierte ausgeschiedene Mitarbeiter mindestens ein unautorisiertes Zugriffsrecht. Dazu gehören neben Netzwerkberechtigungen auch Benutzerkennungen und Passwörter. Vor allem bei unfreiwilligen Abgängen kommt das praktisch einer Einladung zu Datenklau oder Sabotage gleich.

Identity Management automatisieren

Tatsächlich ist die Verwaltung und Kontrolle der ungezählten Zugriffe auf ein IT-System in der Praxis sehr schwierig – vor allem, wenn der Benutzerkreis auf Kunden, Prozesspartner und Lieferanten ausgeweitet wird. Die Sisyphus-Arbeit nimmt dann ein Ausmass an, das sich nur mit einem weitgehend automatisierten Management sauber und effizient bewältigen lässt. Die Lösung heisst «Secure Identity Management» (SIM); ihr Ziel ist die zentralisierte, Computer gestützte Administration sämtlicher Benutzerrechte.

Und das funktioniert wie folgt: Der Systemadministrator kann mit wenigen Eingaben festlegen, welche Mitarbeitenden auf welchen Kanälen (firmeninternes Netz, Mobilgerät etc.) auf welche Systemteile, Anwendungen und Daten zugreifen dürfen. Auf gleiche Art und Weise lassen sich individuelle Zugriffsrechte für Kunden, Partner und Lieferanten definieren.

Die Umsetzung dieser Vorgaben erfolgt dann automatisch: Eine SIM-Komponente namens «Provisioning Manager» registriert die entsprechenden Listen, generiert Passwörter und richtet die Zugänge ein – quer durch die ganze IT-Umgebung des Unternehmens. Wobei automatisch sichergestellt wird, dass jeder Anwender nur eine Identität braucht – selbst wenn er Berechtigung für ganz verschiedene Anwendungen hat. Eine andere Komponente, der so genannte «Password Manager», sorgt dafür, dass die zugelassenen Benutzer ihre Zugangs-Codes jederzeit selbst ändern können, ohne damit ein Chaos anzurichten.

Allein schon dies ist eine riesige Hilfe: Die Zeitersparnis beim Registrieren und Verwalten der Zugänge gegenüber herkömmlichen Security-Systemen ist enorm. Lücken und Doppelspurigkeiten sind praktisch ausgeschlossen, alles ist säuberlich protokolliert und jederzeit nachvollziehbar. Ein weiterer grosser Gewinn von SIM ist, dass man damit auch das Streichen von Berechtigungen im Griff hat: Scheidet ein Mitarbeiter aus oder fällt ein Kunde weg, so genügen wenige Administrator-Mausklicks, um dessen Zugangsrechte lückenlos zu löschen. Damit wird das Sicherheitsrisiko von nicht mehr erwünschten Access-Rechten effizient minimiert.

Kritische Erfolgsfaktoren

Was braucht es denn für eine erfolgreiche Einführung von Secure Identity Management? Die wichtigste Voraussetzung für die Zusammenführung und Zentralisierung von unternehmensweit eingesetzten Systemen ist fundiertes Integrationswissen. Zwar können SIM-Lösungen bei modernen Betriebssystemen, Datenbanken und Messaging-Systemen in der Regel problemlos eingebunden werden. Bei vielen anderen Anwendungen ist das aber bedeutend schwieriger. Hier ist fast ausnahmslos eine individuelle Integration nötig, die entsprechendes Fachwissen verlangt. Und längst nicht alle IT-Ausrüster haben dafür geschultes Personal.

Sehr oft hapert es auch bei den Schnittstellen: Viele sind nicht standardisiert und zudem schlecht dokumentiert. Oder – noch schlimmer – überhaupt nicht vorhanden. In solchen Fällen können die Vorteile von Secure Identity Management (siehe Kasten) höchstens teilweise genutzt werden.

Da fast niemand «auf der grünen Wiese» beginnt, ist auch eine kluge Integration bestehender Sicherheitslösungen in das neu einzuführende SIM-System gefragt. Häufig sind die Benutzerlegitimationen nicht nur an verschiedenen Orten gespeichert, sondern werden auch dezentral verwaltet (zum Beispiel im Personaldepartement, in der IT-Abteilung usw.). Die Integrationsaufgabe beginnt also

mit der Analyse des Ist-Zustands. Nach dem Ausarbeiten eines geeigneten Lösungskonzepts geht es um die Wahl der entsprechenden Bausteine, aus denen sich ein effizient funktionierendes Gesamtsystem zusammensetzen lässt.
Diese Schritte sind alles andere als trivial und verlangen vom Realisator viel Know-how und Erfahrung. Es ist aber nicht bloss eine Frage der Technik – zu einer praxistauglichen Lösung gehört auch eine gute Organisation. Dazu ein Beispiel: Für die meisten Anwender ist das Einloggen ins System ein lästiger Vorgang. Also muss man dafür sorgen, dass sie damit auf Anhieb zurecht kommen. Und dass sie auch wissen, an wen sie sich in Problemfällen (vergessener PIN-Code etc.) wenden können. Vor allem aber müssen die Systembetreiber für diese heiklen Fälle gerüstet sein – nicht nur technisch, sondern auch organisatorisch. Denn bei Pannen im IT-Bereich sind wegen der hohen Integration oft weite Bereiche, wenn nicht gar das ganze Unternehmen betroffen. Neben geeigneter Software sind daher auch Mitarbeiter gefragt, die im Falle eines Falles rasch und sicher reagieren können. ◆

SECURE IDENTITY MANAGEMENT: WENIG AUFWAND, VIEL NUTZEN

Identitätsmanagement gehört zu den grossen Trends in der IT-Branche. Kein Wunder, denn Fachleute behaupten, dass sich mit Secure Identity Management (SIM) innerhalb eines einzigen Jahres ein Return on Investment von 40 Prozent erzielen lasse. Marktforscher wie Frost & Sullivan schätzen das jährliche Wachstum der jungen Technologie in Europa auf 27 Prozent und erwarten 2006 ein Marktvolumen von gut 800 Mio. Dollar.
Ob diese optimistischen Zahlen auch tatsächlich zutreffen, muss sich natürlich erst weisen. Tatsache ist jedenfalls, dass gute SIM-Lösungen den Unternehmen eine ganze Reihe von kostenreduzierenden Vorteilen bringen:

- **Vereinfachung der Benutzerverwaltung**
  SIM verwaltet zentral die Profile und Accounts sämtlicher zugangsberechtigter Anwender.
- **Teilweise Automation beim Erstellen und Löschen von Anwender-Accounts**
  SIM generiert für jede Anwender-Kategorie systematisch neue Accounts.
- **Passwort-Management**
  SIM erlaubt den Anwendern, ihre Profile und Passwörter zu ändern und synchronisiert letztere mit allen betroffenen Applikationen.
- **Single Sign-on**
  SIM verschafft dem Anwender mit einem einzigen Login Zugang zu allen erlaubten Applikationen.
- **Aktives Risikomanagement**
  SIM minimiert das Risiko, dass ein Benutzer – egal, ob Mitarbeiter, Lieferant oder Kunde – unberechtigt Zugriff auf Programme oder Daten erhält.
- **Professioneller Auftritt bei allen Benutzern**
  SIM sorgt dafür, dass sowohl interne wie externe Anwender das Unternehmen einheitlich wahrnehmen.
- **Effizienteres CRM und Data Mining**
  SIM ermöglicht mit seinem zentralen Managementsystem für die Benutzer-Identitäten und Zugriffe, verschiedene Datenbanken untereinander zu korrelieren – eine spürbare Hilfe für CRM und Data Mining.
- **Kürzere Entwicklungszeiten**
  SIM zentralisiert die Benutzerverwaltung und Rechtevergabe sämtlicher Unternehmens-Applikationen. Die entsprechenden Sicherheitsroutinen müssen daher nur einmal programmiert werden. *(fw)*

KRYPTOLOGEN WOLLEN RAUBKOPIERER STOPPEN

180 europäische Forscher und Entwickler haben sich zum «Ecrypt»-Netzwerk, einem Projekt zur Sicherung von Multimediadaten (Digital Rights Management), zusammengeschlossen. Die Forscher wollen Methoden entwickeln, um Musik, Bilder und Videos mit zusätzlichen Schutzmechanismen zu versehen. Damit sollen Manipulationen erkannt und Raubkopien verhindert und aufgespürt werden können.

SPAM-SHREDDER GEGEN WERBE-E-MAILS

Der US-amerikanische Sicherheitsspezialist Webroot hat ein neues Werkzeug für die Unterdrückung unerwünschter E-Mail-Nachrichten präsentiert. Der «Spam-Shredder» arbeitet mit allen POP3-Clients zusammen, untersucht E-Mail-Konten in Outlook, Outlook-Express und Eudora und konfiguriert sie für eine effektive Spam-Abwehr. Darüber hinaus «merkt sich» der Häcksler die Auswahlkriterien seines Users.

SICHERHEITS-SUITE GEGEN DATENKLAU

Die deutsche Softwareschmiede Digitronic hat eine neue Kollektion von Sicherheitskomponenten präsentiert, die Zugriffsschutz mit Datensicherheit kombiniert. Die Authention Safety Suite 2.0 besteht aus fünf Einzellösungen, die durch ihr Zusammenspiel einen kompletten Schutzschild um Windows 2000 und Windows XP entfalten sollen.

SASSER SCHLÜPFT DURCH OFFENE PC-PORTS

Der Sicherheitsspezialist Symantec warnt vor dem neuen Internetwurm «W32-Sasser», der sich ohne Aktion des Anwenders verbreitet. Allein die Verbindung zum Internet reicht aus, um dem Schädling Tür und Tor zu öffnen. Das Schadprogramm infiziert Computer, die noch nicht die Sicherheitslücke LSASS (Local Security Authority Subsystem Service) in Windows XP, 2000 und 2003 Server geschlossen haben. *(ICT/Agenturen)*