Die Sicherheitsrisiken für Unternehmen und Organisationen sind vielfältig und ebenso vielfältig sind die Antworten. Dies führt dazu, dass über die Jahre eine Reihe von Insellösungen für Zugangskontrolle, Identifikation, Rechtevergabe und Provisioning zusammenkommen. Mehrfache Datenhaltung und fehlende Transparenz machen die Administration dieser Einzelsysteme ineffizient und fehleranfällig. Die Konsolidierung zu einem einheitlichen Identity- und Access-Management (IAM) verspricht nicht nur eine erhebliche Reduzierung der Administrationskosten und einen höheren Komfort für die Anwender, sondern auch mehr Sicherheit und Transparenz.

IDENTITY UND ACCESS-MANAGEMENT

Sicherheitskonzepte konsolidieren

Gegen den administrativen Wildwuchs bei der Sicherheit

Eine Vielzahl einzeln geregelter Zugangsberechtigungen, Log-ins für verschiedene IT-Systeme und dazu noch unterschiedliche Zugriffsrechte über das lokale Netzwerk oder Internetverbindungen – das ist die Praxis in deutschen Unternehmen. Mitarbeiterfluktuation, Reorganisationen oder die temporäre Beschäftigung externer Dienstleister erzeugen einen enormen Administrationsaufwand in den IT-Abteilungen. Umgekehrt beschweren sich die Fachabteilungen und Mitarbeiter, dass ihre Arbeit durch lückenhafte Zugriffsberechtigungen und aufwändige Autorisierungsprozesse immer wieder behindert wird. Zunehmend schwerer wiegt darüber hinaus die Compliance-Problematik: Die Frage, was der „Mitarbeiter Müller" denn aktuell darf, lässt sich nur durch die aufwändige Recherche nach allen Einzelberechtigungen beantworten. Dabei wäre es im Sinne nachvollziehbarer Sicherheitsprotokolle wichtig, auf einen Blick feststellen zu können, wer welche Räume betreten darf und wer auf welche Daten und Applikationen tatsächlich Zugriff hat.

IAM als lohnenswertes Projekt verstehen

Ironischerweise nimmt gerade in gut gesicherten Unternehmen der Administrationsaufwand kritische Ausmaße an. Organisationen, die in einzelnen Bereichen, wie dem Werkschutz, dem Datenschutz, im Netzwerk oder dem mobilen externen IT-Zugang bereits hochentwickelte, aber voneinander unabhängige Sicherheitslösungen betreiben, stehen beispielsweise in der Gefahr, dass einzelne Zugangsberechtigungen


© pn_photo/Fotolia.com

übersehen werden und beim Ausscheiden eines Mitarbeiters weiterbestehen. Eine solche Situation verlangt nach einem durchgängigen Identity- und Access-Management-System (IAM). Ein solches integriert alle physischen und elektronischen Zugangsberechtigungen der Mitarbeiter und ermöglicht deren einheitliche, geregelte und nachvollziehbare Verwaltung.

Die IAM-Praxis zeigt: Die „perfekte" Lösung ist dabei nicht auf einen Schlag zu haben. Vielmehr müssen Planung und Durchführung von IAM-Projekten einer sorgfältig nach Prioritäten geordneten Roadmap folgen. So analysieren IAM-Spezialisten, wie die Nürnberger Peak Solution, die Unternehmen vor dem Projektstart mittels eines Reifegradmodells. Dabei wird untersucht, wie weit die Prozesse und verwendeten Technologien für Identifizierung und Zugangskontrolle bereits beschrieben und nutzbringend integriert sind. Auf dieser Basis lässt sich dann zum einen feststellen, wo es Sicherheitslücken gibt, die mit hoher Priorität geschlossen werden müssen. Zum anderen lassen sich aber auch Prozesse identifizieren, die soweit ausgereift sind, dass man im Weiteren auf ihnen aufbauen kann.

Perspektivwechsel: Wer braucht welche Rechte?

IAM-Projekte beginnen mit einem Perspektivenwechsel. Statt von der einzelnen Applikation oder der klassischen Perimeter-Sicherheit auszugehen, wird der Anwender in den Mittelpunkt gerückt. Dazu identifiziert man verschiedene Anwendungsfälle (Use Cases), um daraus abzuleiten, welche Sicherheitsanforderungen es überhaupt gibt, wo die Verantwortlichkeiten liegen, wer beteiligt ist und welches Ergebnis erreicht werden soll. Diese Anwendungsfälle werden ausgiebig und möglichst exakt beschrieben, Verbindungen zwischen den Use Cases transparent gemacht.

Mit diesen Use-Case-Beschreibungen als grafische Darstellungen schafft man eine verständliche Diskussionsgrundlage für alle Fachabteilungen und die Instanzen, die später das System administrieren, also beispielsweise IT-Abteilung, Sicherheitsbeauftragte, Facility Management oder Werkschutz.

Gleichzeitig bilden diese Beschreibungen die Grundlage für eine effiziente Teilautomatisierung der Administration, weil sich darüber Workflows elektronisch abbilden lassen und Rollenmodelle abgeleitet werden können, die den Großteil der Nutzerprofile reflektieren. Solche Rollenmodelle haben sich zum Beispiel in der elektronischen Vorgangsbearbeitung bewährt und finden auch im Objektschutz Einsatz, was die gemeinsamen Nutzenpotentiale nur unterstreicht. In einem voll ausgebauten IAM-System sind durch Rollenmodelle jeweils Standards für Personengruppen gesetzt – hinsichtlich der Zutrittsrechte für Gebäude, der Versorgung mit IT-Ressourcen und der Zugriffs- und Bearbeitungsrechte auf Daten. Wer jeweils für Anträge und Entscheidungen zuständig ist, kann genauso über Rollen definiert werden, wie Sicherheitsrichtlinien und wer berechtigt ist, diese durchzusetzen oder zu überprüfen. Der große Vorteil eines detaillierten Rollenmodells ist neben sinkendem Administrationsaufwand die deutlich höhere Flexibilität bei Rechteveränderungen – zum Beispiel beim Wechsel eines Mitarbeiters in eine andere Abteilung. Außerdem ist es möglich, den Umgang mit Besuchern, Lieferanten, Partnern oder Subunternehmern grundsätzlich und zuverlässig im Sinne der Compliance-Richtlinien zu regeln. Deutlich gestraffte Antragsprozesse und eine systematische und damit treffsichere Zuordnung von Rechten sind weitere IAM-Vorteile, die Mitarbeiter und Fachabteilungen schnell wahrnehmen und honorieren.

Diebstahlschutz für virtuelle Maschinen

Wissenschaftler der TU Darmstadt haben einen Weg gefunden, Hacker-Attacken auf virtuelle Maschinen frühzeitig zu erkennen. Unternehmen und Behörden, die virtuelle Maschinen einsetzen, können die dort gespeicherten Daten so vor Diebstahl schützen. Virtuelle Maschinen sind Computer, die keinerlei Hardware-Komponenten enthalten, sondern vollständig von einer Software simuliert werden. Im Vergleich zu herkömmlichen Computern sind virtuelle Maschinen deutlich flexibler und effizienter einsetzbar, weil sie sich – wie alle anderen Softwaredateien auch – schnell und ohne großen Aufwand von einem zum anderen Ort verschieben lassen. Das birgt allerdings auch ein Risiko: Der Nutzer merkt nämlich nicht, wenn eine virtuelle Maschine bei einem Hacker-Angriff illegal aus dem jeweiligen Firmen- oder Behörden-Netz heraus verschoben wird. In wenigen Sekunden kann so ein gesamter Rechner mit allen gespeicherten Daten in falsche Hände geraten. Der Diebstahl kann jedoch verhindert werden, wenn die Bewegung der Maschine rechtzeitig bemerkt wird. Ein solches Frühwarnsystem entwickelt ein Forscherteam um Dr. André König vom Fachgebiet Multimedia Kommunikation (KOM) der TU Darmstadt. Dabei machen sich die Wissenschaftler die Echoanfrage-Funktion zunutze, das so genannte „Anpingen". „Beim Umzug einer virtuellen Maschine sind einzelne Informationspakete länger im Netz unterwegs und gehen teilweise sogar verloren. Eine virtuelle Maschine in Bewegung sendet also ein spezifisches Echomuster aus", erklärt König. Er und sein Forscher-Team entwickeln nun eine Software, die dieses spezifische Echomuster erkennt und Schutzmaßnahmen gegen den Angriff auslöst. Wichtig sei dabei vor allem der Faktor Zeit, betont König: „Daten, die einmal entwendet sind, lassen sich nicht mehr zurückholen – der Angriff muss daher vor der vollständigen Migration der Maschine erkannt und gestoppt werden." ■

Troubleshooting aus der Ferne

Mit seinen Netzwerk- und Sicherheits-Produkten bietet Black Box maßgeschneiderte Lösungen zur Zweigstellenanbindung. Durch den Branch-Office-Ansatz lassen sich Ressourcen optimal nutzen und Abläufe verbessern. Gleichzeitig werden auf diese Weise die Wartungskosten reduziert und die Downtime minimiert. So ist es möglich, mit durchdachten KVM-over-IP-Konzepten Troubleshooting bis auf die BIOS-Ebene, Reboots oder Kaltstarts schnell und komfortabel aus der Ferne durchzuführen. Mit dem Servswitch CX Quad IP steht hierfür ein kompaktes Gerät zur Verfügung, mit dem bis zu vier User Remote-Server und serielle Geräte über das Internet kontrollieren und steuern können. Das jüngste Gerät der Servswitch CX-Familie verfügt über 16 Ports für den Anschluss unterschiedlicher Server oder von klassischen KVM-Switching-Systemen. www.black-box.de ■

Wer ist das?

Beim schrittweisen Aufbau einer IAM-Lösung spielt die Identifikation und Authentifizierung eines Mitarbeiters eine zentrale Rolle. Single-Sign-on, also die einmalige Authentifizierung für alle Berechtigungen, ist die benutzerfreundlichste Lösung. Sie hat den Vorteil, dass der Mitarbeiter nicht durch wiederholte Authentifizierungen in seiner Arbeit aufgehalten wird und er nicht versucht ist, Sicherheitsbestimmungen zu unterlaufen. Bei einem einzigen Passwort ist es eher unwahrscheinlich, dass es zu kurz gewählt oder aufgeschrieben wird. Single-Sign-on verlangt aber auch nach sicheren Identifikationsmethoden – schließlich könnte mit einer „gestohlenen Identität" besonders viel Schaden angerichtet werden.

Experten empfehlen daher, diese mittels einer 2-Faktor-Authentisierung zu schützen und bei Single-Sign-on-Lösungen auf hochwertige Standardprodukte zurückzugreifen. Deren Auswahl hängt zum einen von vorhandenen Lösungen ab, auf die man aufbaut, zum anderen von den Anwendungssituationen.

Basis der meisten „Starken-"Authentifizierungslösungen ist heute die Publik Key Infrastructure (PKI). In einer PKI wird jedem Benutzer ein kryptografisches Schlüsselpaar zugewiesen, das sich aus einem öffentlichen Schlüssel (public key) und einem privaten Schlüssel (private key) zusammensetzt. Die beiden stehen in einem mathematischen Verhältnis zueinander. Ein digitales Zertifikat verbindet den public key mit einer Person. Deren privater Schlüssel wird auf einem Token gespeichert, also zum Beispiel einem speziellen USB- oder Smartcard-Adapter.

Lösungen dieser Art lassen sich hervorragend erweitern, wenn mit einem „Ausweis" mehrere Funktionen innerhalb einer Identity- und Access-Management-Lösung erfüllt werden sollen. Wird ein Token zudem mit einem RFID-Tag ausgestattet, kann man ihn zum Beispiel dazu verwenden, den Mitarbeiter gegenüber Zutrittskontroll-, Zeiterfassungs- und Bezahlsystemen zu identifizieren.

Beispiele

Bei der VNG - Verbundnetz GAS AG nahm man beispielsweise die Einführung neuer Ausweise für rund 1.200 Mitarbeiter, am Standort Leipzig, zum Anlass, ein System verschiedener Ausweistypen mit entsprechenden Workflows für deren Ausstellung und Sperrung zu entwickeln. Zusätzlich zu den Transpondern für die Anwendungsbereiche Zutrittskontrolle, Zeiterfassung und Kantinenbezahlung wurden die Smartcards mit einem Java-Crypto-Chip ausgestattet, der die Basis für Funktionen wie digitale Signatur und Verschlüsselung von Dokumenten bildet. Bereits der Werkschutz kann anhand einer solchen Karte mit einem Blick sehen, welche Berechtigungen der Inhaber hat und diese, beispielsweise bei Kartenverlust, mit einem Klick komplett und zuverlässig sperren.

Bei einem anderen Projekt der Peak Solution war der Auslöser die Verwaltung und Bereitstellung von ca. 30.000 Benutzer- und Gruppeninformationen für eine Vielzahl von Systemen im IT-Servicezentrum der Universität Kassel. Hier lag der Effizienzhebel der Identity-Management-Lösung in der Einführung eines vereinheitlichten Antragsverfahrens und die Verlagerung von Entscheidungskompetenzen in die zuständigen Fachbereiche. Im Rahmen der Lösung wurden zuvor zeitaufwändige Administrationsprozesse weitgehend automatisiert, Zugriffe auf Systeme bedarfsgerecht bereitgestellt und die Einhaltung von Security Policies sichergestellt.

Compliance und vereinfachte Administration

Die Zusammenführung von Authentifizierungsszenarien ist ein zentraler Aspekt des IAM, doch bei Weitem nicht sein einziger Nutzen. Durch die rollenbasierte Verwaltung von Berechtigungen und klaren Regeln für Provisioning und Deprovisioning wird ein hohes Maß an nachvollziehbarer Durchführung von Sicherheitsstandards erreicht – Basis für die Erfüllung von immer strengeren Compliance-Bestimmungen. Ein hoher Grad an Automation reduziert die Notwendigkeit manueller Administration im Zusammenhang mit der Rechtevergabe. Bis zu 80 % der Routineaufgaben, zum Beispiel für die Einrichtung von Benutzerkonten für neue Mitarbeiter, können eingespart werden. Elektronische Antrags- und Genehmigungsverfahren beschleunigen zudem die Zuteilung von Zugriffsrechten, etwa bei der Zusammenstellung von Projektteams. Gerade mit Blick auf die enorme Arbeitsbelastung der IT-Abteilungen mit wenig wertschöpfenden Administrationsaufgaben muss man feststellen: Auch wenn nicht auf Anhieb eine All-in-one-Türöffner-Log-in-Zeiterfassungs-Kantinen-Smartcard ausgegeben werden kann, lohnt es sich, mit Hilfe erfahrender Berater und Systemintegratoren den Weg zu einem übergreifenden Identity- und Access-Management zu beschreiten.

Ga-Lam Chang
Leiter Identity and Security Management Solutions bei Peak Solution

KONTAKT

Peak Solution GmbH, Nürnberg
Tel.: 0911/800927-70, Fax: 0911/800927-99
g.chang@peak-solution.de, www.peak-solution.de