

Die Verwaltung von Anwendern, deren Berechtigungen und zugeordneten Sicherheitskomponenten wie Zertifikate und Smartcards sind zentrale Aufgaben in einer IT-Organisation. Die Komplexität dieser Aufgaben hat in den letzten Jahren immer weiter zugenommen. Gleichzeitig sind die Anforderungen an die Sicherheit und die Einhaltung von Regularien gewachsen. Grund genug für Microsoft, sich um das Thema Identity and Access Management zu kümmern.

Identitäten effizient verwalten – Microsoft Identity Lifecycle Manager 2007

Am Anfang ist alles noch ganz leicht und übersichtlich: Sie stellen einen Mitarbeiter ein, legen ihn ordnungsgemäß als Anwender im Windows Active Directory-Verzeichnisdienst an, und schon macht sich der neue Kollege ans Werk. Doch bereits nach einigen Tagen oder Wochen muss er für seine Arbeit auf immer mehr Anwendungen zugreifen, und Sie legen ständig neue Konten und Berechtigungen für Ihren Mitarbeiter an. Und irgendwann entscheiden Sie sich auch noch dafür, mehr Gewicht auf Ihre Sicherheit zu legen – also führen Sie eine Public Key Infrastructure (PKI) ein und arbeiten fortan mit Zertifikaten und Smartcards. Spätestens jetzt wird die Arbeit des Administrators unübersichtlich.

Auch wenn das Eingangsbeispiel sicher nicht auf Ihren Betrieb zutrifft, so kämpfen viele Unternehmen mit der Verwaltung von Identitäten, Zugängen und Berechtigungen. Dabei

ser Umstand kostet Zeit, er verringert die Produktivität der Mitarbeiter und gefährdet oft die Sicherheit. Die zusätzlichen Verzeichnisdienste stammen entweder von anderen Netzwerkbetriebssystemen oder fremden Datenbanken. Aber auch andere Plattformen wie Großrechner besitzen, ebenso wie Telefonanlagen als isolierte Systeme, häufig eine eigene Benutzerverwaltung. Um die einzelnen Verzeichnisdienste zu synchronisieren, stand Ihnen bisher Microsoft Identity Integration Server (MIIS) 2003 zur Verfügung. MIIS hat als Metaverzeichnis den Abgleich zwischen den verschiedenen Verzeichnisdiensten übernommen.

Eine weitere Kernkomponente vieler Sicherheitslösungen sind Zertifikate. Von Smartcards bis SSL-Webseiten – Zertifikate sind das Schweizer Taschenmesser im Security-Umfeld.

Übernahme von Alacris – einem Spezialisten für Zertifikats- und Identitätsmanagement – weiterentwickelt hat.

Microsoft Identity Lifecycle Manager 2007

Die beiden Produkte CLM und MIIS 2003 führt Microsoft jetzt in Microsoft Identity Lifecycle Manager (ILM) 2007 zusammen. Für ILM 2007 sprechen vor allem drei starke Argumente: die Synchronisation von Identitätsinformationen, ein Bereitstellungssystem für Benutzerkonten und ein komfortables Management von Zertifikaten und Smartcards. ILM erfüllt dabei die Funktion eines administrativen Proxys, oder anders gesagt, er ist das Bindeglied zwischen den existierenden Technologien und dem ver-

liefert mit ILM 2007 eine ganze Reihe vorgefertigter Management-Agenten mit. Dazu gehören unter anderem Agenten für Novell, Sun, Lotus Notes oder SAP. Hinzu kommen noch Universal-Agenten, die Formate wie XML, CSV oder LDIF (LDAP Interchange Format) beherrschen. Auf diese Weise verbinden Sie sehr viele Systeme und Plattformen miteinander. Die Verbindungen zu ILM erfordern keine Veränderung an den Zielsystemen, was die Implementierung deutlich vereinfacht.

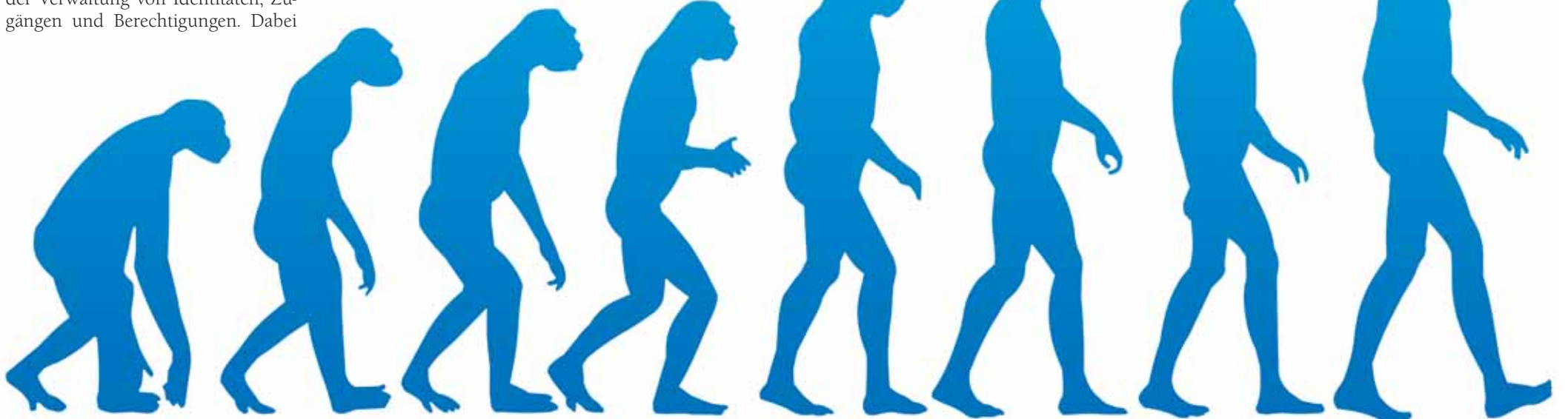
Von einem führenden System aus – etwa der Personaldatenbank – werden so alle wichtigen Verzeichnisse mit den Anwenderattributen versorgt. Auch wenn sich die Stammdaten än-

aufgaben ausführen darf. Sie können zum Beispiel bestimmte Arbeitsplätze einrichten, die sich für die Ausgabe von größeren Smartcard-Mengen, dem sogenannten Bulk-Roll-out, nutzen lassen. In gewissen Grenzen darf sich der Mitarbeiter auch selbst bedienen: Eine anpassbare Komponente erlaubt es bestimmten Anwendern, eine temporäre Smartcard auszustellen oder neue Zertifikate anzufordern.

Ein weiterer wichtiger Bestandteil des ILM 2007-Zertifikatsmanagements sind die anpassbaren Arbeitsabläufe. Damit definieren Sie typische Arbeits- und Genehmigungsprozesse rund um Zertifikate und Smartcards. Sie verändern die Abläufe in Abhängigkeit von der organisatorischen und regionalen Struktur eines Unternehmens oder nach Sicherheitsanforderungen.

Aufgaben delegieren, Abläufe definieren

Einzelne Aufgaben delegieren Sie entweder an den Anwender, an die Mitarbeiter des Helpdesks oder an den Empfang. Auch wenn dies nicht für alle Anwendungszwecke gedacht ist, kann sich ein Mitarbeiter so auch selbst ein Zertifikat für die Nutzung des Encrypting File Systems (EFS)



Mit Identity Lifecycle Manager 2007 folgt Microsoft dem Evolutionsprinzip: Das Produkt berücksichtigt die im Lauf der Jahre weiterentwickelten Sicherheitsstandards ebenso wie gestiegene Sicherheitsanforderungen.

geht es nicht nur um Sicherheitsfragen, sondern auch um die kostbare Zeit, die im alltäglichen Betrieb mit dem Identitätsmanagement verschwendet wird. Zahlreiche und voneinander isolierte Verzeichnisdienste und Berechtigungssysteme machen aus der Benutzerverwaltung ein undurchsichtiges Dickicht. Viele Unternehmen wissen aus diesem Dilemma keinen Ausweg. Jetzt kommen Sie ins Spiel. Microsoft bietet eine perfekte Lösung für Identity and Access Management an.

Identity and Access Management – die Komponenten

Microsoft hat schon seit vielen Jahren Produkte im Angebot, die Ihnen die Verwaltung von Netzwerkidentitäten erleichtern. Der zentrale Verzeichnisdienst Active Directory (AD) ist dabei das Kernstück. Es erleichtert den IT-Experten nicht nur die Benutzerverwaltung, auch die Arbeit der Anwender ist dank AD um vieles leichter. In vielen Fällen sind sogar Single-Sign-on (SSO-) Szenarien auf Basis von Active Directory möglich. Kurz gesagt: Je homogener das Netzwerk aufgebaut ist, desto besser lässt sich SSO nutzen.

In vielen Unternehmen müssen Sie neben Active Directory noch weitere Verzeichnisdienste pflegen. Doch die-

Während andere Firmen viel Geld für die dazu notwendige Public Key Infrastructure verlangen, ist sie bei Microsoft seit langer Zeit kostenfreier Bestandteil der Windows-Server-Betriebssystemfamilie. Technisch betrachtet haben Sie eine PKI mit wenigen Mausklicks eingerichtet.

Die Herausforderungen stecken jedoch im Detail. Bevor Sie eine PKI in Betrieb nehmen, müssen Sie alles sorgfältig planen und ein Design bestimmen. Später, im laufenden Betrieb, sind Sie dann tagtäglich mit vielen wichtigen Verwaltungsaufgaben konfrontiert: Zertifikate neu auszustellen, zu verlängern oder im schlimmsten Fall auch zurückzuziehen. Auch den Ablauf von Zertifikaten müssen Sie überwachen und ihn nicht erst nach den Anrufen verzweifelter Mitarbeiter melden. Als Einschränkung sei jedoch erwähnt, dass die in Windows Server enthaltenen Verwaltungswerkzeuge eher für einzelne Verwaltungsaufgaben gedacht und weniger für die alltägliche Arbeit in einem größeren Unternehmen geeignet sind.

Um die Nutzung von Zertifikaten besser in die Verwaltungsabläufe und den IT-Betrieb zu integrieren, hat Microsoft mit Certificate Lifecycle Manager (CLM) eine entsprechende Lösung entwickelt. CLM basiert auf Technologien, die Microsoft nach der

verantwortlichen IT-Personal. Eine positive Nachricht speziell für Unternehmen, da sie ihre bisherigen Investitionen, etwa eine Windows-PKI, weiter nutzen können. Diese Leistungsmerkmale stammen von den Vorgängern MIIS und CLM, die Microsoft jedoch überarbeitet hat.

Die Systemanforderungen für ILM 2007 sind moderat. Als Betriebssystem ist Windows Server 2003 die Voraussetzung. Die Ablage der zahlreichen Informationen und die Berichterstellung übernimmt Microsoft SQL Server. Detaillierte Informationen über die Anforderungen hat Microsoft auf einer FAQ-Seite zusammengestellt.

Synchronisation von Identitätsinformationen und User-Provisioning

Die Möglichkeit, verschiedene Verzeichnisdienste automatisiert abzugleichen, ist für Sie von dreifachem Wert. Der Verwaltungsaufwand sinkt, die Netzwerksicherheit und die Produktivität der Mitarbeiter steigen. Die Informationen über die Netzwerkidentitäten liegen in einem zentralen Repository, dem sogenannten Metaverse.

Management-Agenten stellen als Connectoren die Verbindung zu den einzelnen Verzeichnisdiensten und Benutzerdatenbanken her. Microsoft

dern oder ein Mitarbeiter die Firma verlässt, der Synchronisationsprozess sorgt für einen sofortigen Abgleich mit allen integrierten Systemen. Ehemalige Angestellte, die noch Monate nach ihrem Ausscheiden aus dem Unternehmen Zugriff auf sensible Anwendungen haben, gehören dank ILM 2007 der Vergangenheit an.

Zertifikats- und Smartcard-Management

Identity Lifecycle Manager 2007 stellt selbst keine Zertifikate aus. Dazu bedarf es weiterhin der Windows Server Certificate Authority (CA). Nach deren Implementierung im Netzwerk werden alle Zertifikats- und Smartcard-Funktionen durch ILM 2007 geleitet. ILM stellt Ihnen dafür eine Reihe von Verwaltungswerkzeugen als Webanwendungen zur Verfügung.

Neben einer Serverkomponente profitieren Sie zusätzlich von verschiedenen Clientanwendungen. Als Verwalter von Zertifikaten und Smartcards genießen Sie eine komfortable Verwaltungsoberfläche und eine Fülle von Berichten. Wichtige administrative Aufgaben wie das Entsperren einer Smartcard gehen Ihnen so leicht von der Hand.

Über hinterlegte Profile definieren Sie exakt, wer welche Verwaltungs-

beschaffen. Bei höheren Sicherheitsanforderungen steht es Ihnen frei, einen Ablauf zu definieren, der vorsieht, dass Zertifikatsmanager und Zertifikatsnutzer gemeinsam agieren müssen. Alle notwendigen Technologien wie Einmalpasswörter sind in ILM 2007 integriert.

Fazit

Microsoft Identity Lifecycle Manager 2007 bietet Ihnen bisher ungeahnte Möglichkeiten. Vor allem Unternehmen, die ihre Sicherheit und eine funktionierende Organisationsstruktur im Auge haben, werden Sie von den Vorteilen der Lösung überzeugen. Wenn Ihnen bereits eine Windows-Server-PKI implementiert haben oder eine Einführung in nächster Zeit planen, ist ILM 2007 die erste Wahl. Dank seines problemlosen Umgangs mit verschiedenen Verzeichnisdiensten sorgt ILM 2007 zudem für eine Senkung der IT-Betriebskosten.

Identity Lifecycle Manager 2007 (englisch)

www.microsoft.com/windowsserver/ilm2007/default.mspx

Identity Lifecycle Management (englisch)

www.microsoft.com/windowsserver2003/technologies/idm/ilm.mspx