Sichere Zugriffe durch „Single-sign-on" ermöglichen

Identitäten im Griff

von Matthias Kirchhoff

Steigende Nutzerzahlen, expandierende IT-Infrastrukturen und komplexer werdende Applikationsportfolios sind nicht die einzigen Probleme – viele IT-Verantwortliche sehen sich zudem mit der Frage konfrontiert: Wer verbirgt sich hinter einer Benutzerkennung? In solchen Fällen kann ein ausgefeiltes Identitätsmanagement durchaus hilfreich sein.

IT-Verantwortliche, die sich die Verwaltung und Überwachung der Zugriffsberechtigungen im Unternehmen auf die Fahne geschrieben haben, werden um den Einsatz eines durchdachten Identitätsmanagement nicht herumkommen. Zu einem solchen System gehört neben der effizienten und zentralen Benutzerverwaltung auch die sichere Authentifizierung der einzelnen Benutzer. Weiterhin muss ein solches Konzept auch die konsistente Administration der Zugriffsmöglichkeiten auf Daten und Clients in einem dynamischen Umfeld beinhalten.

Single-sign-on: Pionier für den Einstieg ins Identitätsmanagement. Moderne Netzwerkinfrastrukturen, die mit Hilfe von Kerberos oder durch den Einsatz von Smartcards gesichert werden, stellen auch heute schon Techniken zur Verfügung, mit deren Hilfe ein Administrator die sichere, einmalige Authentifizierung zur Nutzung beliebig vieler Anwendungen regeln kann. Damit ist bereits die Basis für ein „Single-sign-on" (SSO) im Anwendungsnetzwerk vorhanden. Wenn es dann allerdings um die eigentliche Anmeldung bei den jeweiligen Anwendungen geht, so findet der Anwender ganz unterschiedliche Ansätze. So werden viele Anwendungen nach wie vor über Host-Terminal-Zugriffe erreicht, während andere Applikation extern gespeichert werden und sich damit der Netzwerkadministration entziehen. Schließlich wird man in vielen Netzwerkumgebungen dann auch Programme und Anwendungen finden, die nur über das Internet erreichbar sind. Gegenwärtig benötigt ein Benutzer für jede Anwendung die entsprechenden Zugangsdaten in Form von Benutzername und Passwort. Denn trotz der Gefahr, dass Passwörter vergessen werden können, gilt dieses Prinzip weiterhin als eine effektive Möglichkeit, um Benutzer für den Zugriff auf Anwendungen zu authentifizieren. Diese derholten Eingeben von Benutzername und Passwort. Traditionelle SSO-Lösungen setzen genau an dieser Stelle an: Ihr Ziel ist es , diese Anmeldeprozesse zu automatisieren. Dabei müssen die Anmeldeinformationen für die verschiedenen Anwendungen natürlich sicher gespeichert und bei Bedarf abgerufen werden können, nachdem ein Nutzer sich einmalig authentifiziert hat.

Einfaches Prinzip: Angriffsmöglichkeiten werden verringert. Dieses Prinzip verringert Angriffsmöglichkeiten, die durch zu simple oder mehrfach verwendete Passwörter entstehen, erhöht den Komfort für den Anwender, der sich keine Passwörter mehr merken muss, und reduziert spürbar die Kosten im Helpdesk-Bereich. Wer die Anmeldung für seine Anwendungen auf diese Art und Weise automatisiert, sollte jedoch größten Wert auf die sichere Erst-authentifizierung legen. Eine Möglichkeit dazu bietet der Einsatz personalisierter Hardware-Komponenten wie beispielsweise Smartcards. Auf ihnen können neben Private Keys und Zertifikaten meist auch Datenobjekte PIN-geschützt und damit sicher gespeichert werden. In solchen Datenobjekten lassen sich die für eine Anmeldung notwendigen Informationen problemlos unterbringen.

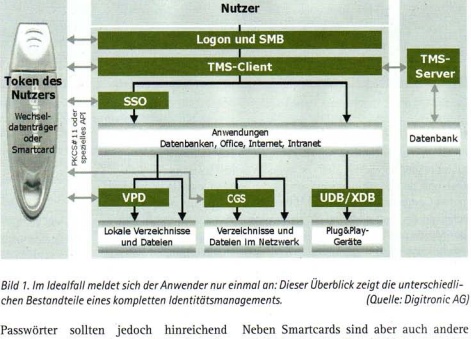

Bild 1. Im Idealfall meldet sich der Anwender nur einmal an: Dieser Überblick zeigt die unterschiedlichen Bestandteile eines kompletten Identitätsmanagements. (Quelle: Digitronic AG)

Passwörter sollten jedoch hinreichend komplex und lang sein, damit sie nicht einfach per Zufallstreffer umgangen werden können. Im täglichen Umgang bedeutet dies aber auch, dass sich der Anwender zahlreiche Passwörter merken muss, um auf seine Daten zugreifen zu können. Über das Jahr gerechnet verbringt der Benutzer so schnell mehrere Arbeitstage mit dem wie-

Neben Smartcards sind aber auch andere mobile Speichermedien denkbar, wenn eine zusätzliche Schutzfunktion (analog zur PIN) den unberechtigten Zugriff verhindert und eine sichere Ablage der Informationen gewährleistet wird. Allgemein bedeutet dies: Ein Nutzer besitzt einen Token (Smartcard, herkömmlicher USB-Memory-Stick oder biometrisch abgesicherter USB-Me-

mory-Stick) und das Wissen um die zugehörige PIN beziehungsweise den passenden Finger. Beides zusammen öffnet ihm den Zugang zu seinen Anwendungen und den entsprechenden Daten.

Durch eine nahtlose Einbindung von SSO-Lösungen in die bestehende Infrastruktur lassen sich so die meisten Benutzerkennungen, Anwendungsdialoge, Zugangsmöglichkeiten und personalisierte Daten zusammenfassen und können zentral durch die Administratoren verwaltet werden. Durch den Einsatz einer SSO-Lösung löst sich eine der wichtigen Fragen im Bereich Zugriffsschutz. Wollen die IT-Verantwortlichen jedoch ein umfassendes Identitätsmanagement zur Einhaltung sicherer Prozesse umsetzen, so müssen mehrere Maßnahmen Hand in Hand arbeiten. Zudem ist es wichtig, dass sich alle Maßnahmen ohne Schwierigkeiten in die bestehende Infrastruktur und Anwendungen integrieren lassen.

Ohne Vorsicht geht es nicht: Sicherheitsaspekte des Identitätsmanagements.

Sensible Daten und Informationen gehören zum Vermögenswert eines jeden Unternehmens. Deshalb muss auch genau geregelt sein, wer Zugriff auf diese Daten hat und wie sie sich sinnvoll gegen Missbrauch oder Manipulation schützen lassen. Vieles lässt sich mit einer sicheren Authentifizierung, einem gut geplanten Rollenkonzept und sorgfältig vergebenen Berechtigungen klären. Durch den Einsatz von Verschlüsselung können die IT-Verantwortlichen zusätzliche Sicherheit bei besonders sensiblen oder personenbezogenen Daten erreichen. Dem unberechtigten Einblick eines Administrators in vertrauliche Informationen der Geschäftsführung wird damit ebenso ein wirkungsvoller Riegel vorgeschoben wie dem Missbrauch von Daten auf gestohlenen Datenträgern.

Gängige Verschlüsselungswerkzeuge wie die Software „Authention" der Firma Digitronic bieten die Möglichkeit, eine Verschlüsselung sowohl lokal als auch auf einer Netzwerkfreigabe durchzuführen. Bei der lokalen Variante hat der Benutzer die Möglichkeit, über einen wählbaren Laufwerksbuchstaben auf eine Containerdatei zuzugreifen und dort weitere Dateien und Verzeichnisse anzulegen. Die Containerdatei wird hier als virtueller Datenträger ins System eingeblendet. Der Nutzer muss dieses Laufwerk analog zu einem Netzlaufwerk nach der Anmeldung verbinden und das zugehörige Passwort kennen. Wird ein Token eingesetzt, kann dieser Vorgang automatisiert werden, da die Zugangsdaten zum Container, analog zu den Informationen zur Anmeldung an einer Anwendung, ebenfalls in Datenobjekten gespeichert werden können.

Die Verschlüsselung auf einer Netzwerkfreigabe erlaubt dagegen die verschlüsselte Speicherung von Daten im Netzwerk, auf die mehrere autorisierte Personen gleichzeitig zugreifen können. Dabei ist in diesem Fall keine Serverkomponente nötig. Nutzer können durch die Eingabe eines Passwortes auf ein speziell initialisiertes Share zugreifen und in diesem Dateien und Verzeichnisse anlegen. Das Management der Passwörter für die zugriffsberechtigten Nutzer wird von einem „Master-Nutzer" geregelt und die Aktivierung eines solchen Shares kann wieder manuell oder bei Einsatz eines Tokens automatisiert erfolgen.

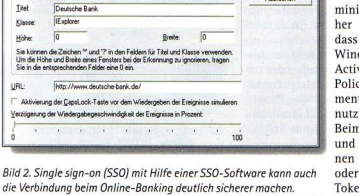

Bild 2. Single sign-on (SSO) mit Hilfe einer SSO-Software kann auch die Verbindung beim Online-Banking deutlich sicherer machen. (Quelle: Digitronic AG)

Eine ebenfalls nicht zu unterschätzende Gefahr stellen die verschiedenen Geräteschnittstellen dar: Über Massenspeicher oder sonstige Peripheriegeräte wie externe Festplatten oder Digitalkameras können schnell Daten ohne Berechtigung abgezogen oder Viren eingeschleust werden. Daher sollte jedes Unternehmen bei der Umsetzung eines Konzepts für das Identitätsmanagement berücksichtigen, welcher Nutzer welche Peripheriegeräte verwenden darf. Auf Grund des hohen Verbreitungsgrades von USB-Geräten sollte die Aufmerksamkeit der Administratoren dabei ganz besonders den USB-Ports gelten. Viele Lösungen bieten zu diesem Zweck die zentrale Verwaltung der Peripherie der Clients beispielsweise mit Hilfe von Gruppenrichtlinien an. Dabei sollten die Verantwortlichen einen wichtigen Aspekt beachten: Solche Geräteberechtigungen können personenbezogen, also zum Beispiel anhand der Mitgliedschaft in bestimmten Gruppen vergeben werden. Bei der Spezifikation von zugelassenen Geräten sollte deshalb sowohl eine detaillierte Spezialisierung, im Idealfall bis hin zur produktspezifischen Seriennummer des Gerätes, als auch die Definition von ganzen Gerätegruppen wie Druckern oder CD-ROM-Laufwerken möglich sein.

Nicht jede Lösung für alle Gelegenheiten: Mittelstandsgerechte Gesamtlösungen.

Das Ziel des Einsatzes einer sicherheitsorientierten Identitätsmanagement-Lösung ist die kosteneffiziente Verwaltung von Identitäten in einem Unternehmen bei gleichzeitig geschützten Geschäftsprozessen. Im Grunde genommen handelt es sich dabei zumeist um eine Erweiterung der Funktionen der Windows-Betriebssysteme. Eine Vielzahl an Optionen ermöglicht die zentrale Verwaltung von Identitäten und die Einhaltung von Sicherheitsstandards. Die Installation und die Administration sollten daher so aufgebaut sein, dass die Funktionen der Windows-Systeme wie Active Directory, Group Policies und Management-Konsole voll genutzt werden können.

Beim Einsatz von Token und der damit verbundenen Gefahr des Verlustes oder der Zerstörung des Tokens sollten die auf dem Token gespeicherten Informationen zentral verwaltet und gesichert werden. Dadurch wird gewährleistet, dass im Ernstfall schnell ein Ersatz-Token mit allen notwendigen Anmeldeinformationen des Nutzers wieder herstellbar ist. Bei Lösungen wie dem bereits erwähnten „Authention" wurde deshalb die Möglichkeit eines zentralen Token-Managements integriert, mit dessen Unterstützung regelmäßig und automatisch Sicherungen von Tokens erstellt und zentral gespeichert werden können. Da die meisten Unternehmen bereits eine „wild gewachsene" Landschaft verschiedenster Authentifizierungsmethoden und unterschiedlichster Token aufweisen, empfiehlt es sich, eine Lösung zu finden, die verschiedene Token integrieren kann. *(fms)*

Der Autor:

Matthias Kirchhoff ist Geschäftsführer der Firma digitronic mit Sitz in Chemnitz.