Wie sicher ist die Wissensgesellschaft?

Christoph Riedner

Business Development Manager
Novell Central Europe
criedner@novell.com

Sicherheit auf dem Betriebsgelände gehört in den meisten Unternehmen bereits zum Alltag: Pförtner überprüfen an zentralen Zugangsstellen die Identität von Besuchern und melden diese im Haus an, Mitarbeiter oder Besucher mit Sonderberechtigungen erhalten über elektronische Ausweise Zugang zu den relevanten Bereichen und Sicherheitsdienste überwachen das Gelände. Auch der Mitarbeiter an sich ist Bestandteil des Sicherheitssystems, kann er doch gerade in kleineren Betrieben unbekannte Besucher von Mitarbeitern unterscheiden und durch sein Einschreiten eventuellen Sicherheitsvorfällen vorbeugen.

Im Zeitalter der Wissensgesellschaft ist das wertvollste Gut eines Unternehmens jedoch nicht zwingend ein materielles Gut, sondern oftmals sind es die elektronischen Geschäftsdaten, die es vor unbefugtem Zugriff zu schützen gilt. Eine Sicherung des Betriebsgeländes vor unbefugtem Betreten reicht hierfür nicht mehr aus; längst erfordert der Zugang zu Unternehmensdaten nicht mehr die persönliche Anwesenheit auf dem Betriebsgelände. Unternehmensnetzwerke erstrecken sich über die Unternehmensgrenzen hinweg in das Internet und ermöglichen Mitarbeitern, Partnern und teilweise auch Kunden den direkten Zugriff auf Unternehmensdaten. Das Sicherheitsrisiko ist durch die Anonymität und geographische Unabhängigkeit des digitalen Zugangs gerade hier signifikant.

Die Hersteller von Standardsoftware haben auf die stetig steigende Sensibilität der mittels ihrer Produkte verwalteten Daten reagiert und integrieren umfangreiche Berechtigungskonzepte, die eine granulare Steuerung der Zugriffsberechtigungen ermöglichen. Mit der zunehmenden Umstellung von Geschäftsprozessen auf elektronische Datenverarbeitung ist jedoch auch die Vielfalt der in einem Unternehmen eingesetzten Software und damit die Anzahl der zu verwaltenden Berechtigungssysteme gestiegen.

Gerade diese entstandene Komplexität stellt die Unternehmen vor eine erneute Herausforderung, deren Bewältigung der Gegenstand dieses Artikels ist: wie stellt ein Unternehmen mit wirtschaftlich sinnvollem Einsatz von Resourcen die Aktualität der vielfältigen Berechtigungssysteme sicher? Eine Herausforderung die nur wenige Unternehmen für sich gelöst haben, deren Bewältigung für die Sicherheit des Unternehmens jedoch von kritischer Bedeutung ist.

Wie sicher ist ein Berechtigungssystem...

- *das nicht aktuell ist*
- *in dem Veränderungen in der Zuständigkeit nicht nachvollzogen werden*
- *in dem bereits ausgeschiedene Mitarbeiter oder ehemalige Lieferanten nach wie vor über Berechtigungen verfügen?*

1 Berechtigungssysteme – eine zentrale Herausforderung?

Die Herausforderung der Verwaltung von Berechtigungssystemen stellt sich für jede im Einsatz befindliche Software gleich, so dass sich eine einheitliche, zentrale Lösung anbietet. Die Entscheidung für eine zentrale Lösung bietet – wie auch bei der Gebäudesicherheit – entscheidende Vorteile:

Effizienz – Eine zentrale Lösung – im Fall der Gebäudesicherheit der Pförtner – ist mit erheblich weniger Aufwand im täglichen Betrieb verbunden, als eine dezentrale Lösung.
Flexibilität – Zentrale Lösungen geben Unternehmen die Fähigkeit, schnell auf veränderte Anforderungen zu reagieren. So können veränderte Sicherheitsanforderungen zeitnah und effizient an zentraler Stelle implementiert werden.
Skalierbarkeit – Braucht ein Unternehmen eine zweite Pforte, nur weil ein neues Gebäude auf dem Gelände errichtet wurde? Nicht zwingend. Zentrale Lösungen skalieren hinsichtlich der dadurch kontrollierten dezentralen Einheiten – entsprechende Standardisierung der Prozesse und Schnittstellen vorausgesetzt.

2 Secure Identity Management – eine zentrale Lösung

Secure Identity Management bietet die zentrale Lösung für eine zeitnahe, effiziente und sichere Verwaltung von Berechtigungssystem. Dabei handelt es sich weniger um eine technologische Revolution als eine konzeptionelle Evolution, vereint Secure Identity Management doch eine Vielzahl bereits bekannter Funktionalitäten:

- Meta Directory
- (e)Provisioning
- De-Provisioning
- Single Sign On
- Zero Day Start
- Zero Day Change
- Last Day Stopp

Mittels Secure Identity Management wird ein Unternehmen in die Lage versetzt, die Konsistenz von Benutzerbezogenen Daten inklusive der erforderlichen Berechtigungen über Anwendungsgrenzen hinweg sicherzustellen. Secure Identity Management integriert dabei nicht nur die im Einsatz befindlichen Software-Anwendungen, sondern auch die Gebäudeinfrastruktur, wie zum Beispiel Telefonanlagen, Zeiterfassungs- und Gebäudezugangssysteme.

Die durch den Einsatz von Secure Identity Management erzielten Vorteile fallen je nach Unternehmen und Anwendungsgebiet unterschiedlich aus, lassen sich jedoch grundsätzlich in folgende Bereiche unterteilen:

- Sicherheit
- Effizienz
- Flexibilität

Sicherheit – Secure Identity Management reduziert durch die weitreichend automatisierte Verwaltung von Berechtigungen die Anzahl der unzutreffenden Berechtigungen. Diese entstehen insbesondere bei Wechsel der Zuständigkeit eines Mitarbeiters und damit Wechsel der erforderlichen Berechtigungen, aber auch beim Ausscheiden eines Mitarbeiters aus dem Unternehmen. Von diesen Vorgängen sind nicht ausschließlich fest angestellte Mitarbeiter eines Unternehmens betroffen, sondern insbesondere externe Mitarbeiter die nur befristete Zeiträume in bestimmten Unternehmensbereichen verbringen und anschließend entweder für einen anderen Unternehmensbereich tätig werden oder aber die Tätigkeit einstellen.

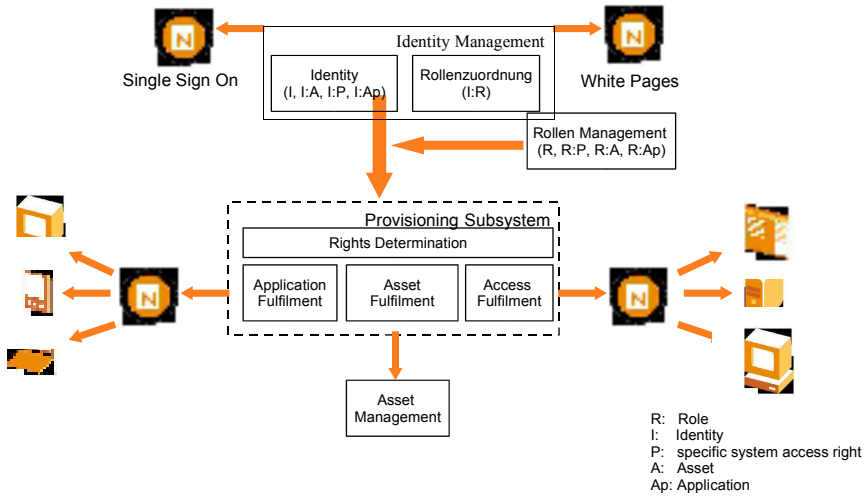
Effizienz – die Automation von Prozessen impliziert den Wegfall von manuellen Prozesschritten. Secure Identity Management erhöht somit die Effizienz der Verwaltung von Berechtigungssystemen. Über die rein administrativen Bereiche hinaus – die in der Regel lediglich einen geringen Teil der Personalkosten darstellen – lassen sich durch Secure Identity Management jedoch auch Effizienzsteigerungen im Bereich der Endanwender realisieren: So reduziert zum Beispiel Single Sign-On die täglichen Aufwände für den Endanwender, während eProvisioning den Produktivitätsausfall bei Neueinstellungen oder internen Versetzungen minimiert.

Flexibilität – Flexibilität wird als die Fähigkeit von Unternehmen und Privatpersonen definiert, sich veränderten Bedingungen anzupassen. Secure Identity Management bietet Unternehmen die Flexibilität organisatorische Veränderungen zeitnah in den Berechtigungssystemen abzubilden. Hierbei kann es sich sowohl um interne Umstrukturierungsmaßnahmen handeln, als auch um Zukäufe oder Ausgliederungen von Unternehmensbereichen. Diese Flexibilität lässt sich als „horizontale Flexibilität“ bezeichnen. Als „vertikale Flexibilität“ hingegen kann die Fähigkeit bezeichnet werden, die Berechtigungssysteme jederzeit veränderten Sicherheitsbedürfnissen anzupassen, zum Beispiel durch starke Authentisierungsmechanismen.

3 Architektur einer Secure Identity Management Lösung

Secure Identity Management wurde bereits Eingangs als eine konzeptionelle Evolution bezeichnet. Insofern besteht eine Secure Identity Management Lösung aus verschiedenen Komponenten, die – je nach Unternehmen und Anwendungsgebiet – in unterschiedlichen Ausprägungen ein Bestandteil der Gesamtlösung werden.

Die folgende Abbildung zeigt die generische Architektur einer Secure Identity Management Lösung. Die einzelnen Komponenten und ihre Bedeutung werden im nachfolgenden Text erläutert.



3.1 Identity Management

Der zentrale Bestandteil einer jeden Secure Identity Management Lösung ist das Identity Management. Bei dieser Komponente handelt es sich um einen zentralen Datenspeicher zur Ablage der aus den angeschlossenen Anwendungen konsolidierten Benutzerinformationen. Vielfach wird mit dieser Komponenten auch der Begriff des „Meta Directory“ verbunden, also ein übergeordnetes Verzeichnis. Neben der ausschließlich passiven Konsolidierung von Benutzerinformationen kann das Identity Management aber auch zur zentralen Steuerung von dezentralen Benutzerinformationen und -berechtigungen dienen. Hierzu können den im Identity Management hinterlegten Benutzern Berechtigungen direkt oder über Rollen zugewiesen werden.

3.2 Provisioning Subsystem

Das Provisioning Subsystem verbindet das Identity Management mit den Anwendungen zum Abgleich der relevanten Daten. Der Abgleich kann dabei bi-direktional erfolgen, also sowohl Datentransfer aus den dezentralen Anwendungen in das zentrale Identity Management, als auch Datentransfer aus dem zentralen Identity Management in die dezentralen Anwendungen. Durch diese Komponente erreicht Secure Identity Management eine hochgradige Flexibilität und die Möglichkeit zur Abbildung komplexer Geschäftsprozesse: Unternehmen können für jedes einzelne Datenfeld eines Benutzers entscheiden, ob dieses durch das zentrale Identity Management zur Verfügung gestellt oder aus einer dezentralen Anwendung bereitgestellt wird und das zentrale Identity Management lediglich die Verteilung an die darüberhinaus angeschlossenen System übernimmt.

Mit dem Begriff „Provisioning“ (Engl. to provision = einrichten) verbinden sich eine Vielzahl weiterer Begriffe:

- eProvisioning
- De-Provisioning

- Zero Day Start
- Last Day Stopp

Das Provisioning Subsystem vollzieht das Einrichten von neuen Benutzern bzw. die Aktualisierung von Benutzern in angeschlossen System automatisiert (= eProvisioning). Die Automation dieses Prozesses ermöglicht zum Beispiel bei neu eingestellten Mitarbeitern die Bereitstellung sämtlicher erforderlicher Berechtigungen binnen weniger Stunden (=„Zero Day Start“). Als sicherheitsrelevanter wird das zeitnahe Entfernen von Berechtigungen bewertet („De-Provisioning“ oder „Last Day Stopp“), das ebenfalls durch das Provisioning Subsystem für alle angeschlossenen Systeme automatisiert erfolgen kann.

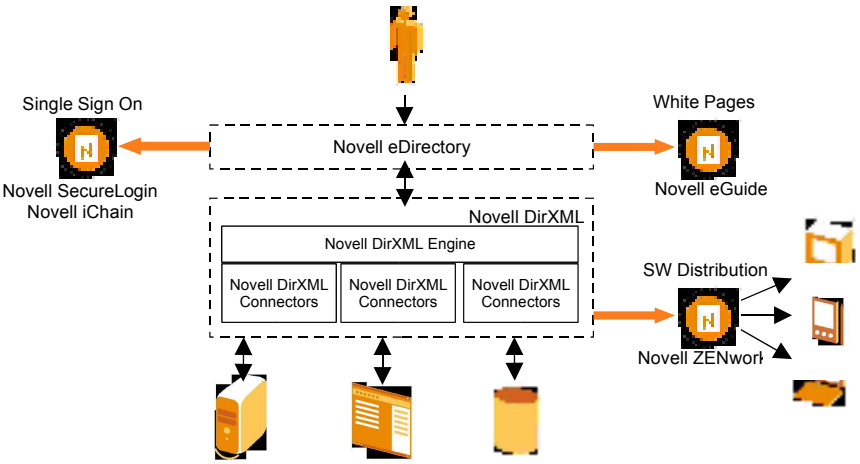
Über die **Fulfilment Agents** ist das Provisioning Subsystem zusätzlich zur Vergabe von Berechtigungen in dezentralen Anwendungen in der Lage, beliebige Prozesse anzustossen. Die Abbildung zeigt beispielhaft die Anbindung an eine Softwareverteilung, so dass einem Anwender auch benötigte Anwendungen automatisiert installiert und de-installiert werden können. Ein vergleichbares Szenario ist durch die Anbindung eines Asset Managements für Arbeitsgeräte wie Laptops oder Mobiltelefone denkbar. Die Informationen über die zur Verfügung gestellten Berechtigungen, die installierten Anwendungen und die ausgehändigten Arbeitsgeräte werden hierbei stets auch zentral im Identity Management dokumentiert.

3.3 Rollen Management

Eine zentrale Bedeutung für die weitestgehende Automation der Verwaltung von Berechtigungssystemen spielen Rollenkonzepte und das Management von Rollen. Unter Rollen versteht man hierbei eine Gruppierung von unterschiedlichen Berechtigungen für Anwendungen, Gebäude oder sonstige Arbeitsmittel. Durch eine sinnvolle Gruppierung dieser Berechtigungen nach Aufgabengebieten können die Berechtigungen standardisiert und die Aufwände reduziert werden. Bei Einsatz eines Rollenkonzeptes wird in der Komponente Identity Management lediglich die Rolle zugeordnet. Das auftrennen der zugeordneten Rolle in die dahinter gruppierten Berechtigungen übernimmt das Provisioning Subsystem auf Basis der vom Rollenmanagement zur Verfügung gestellten Rollenbeschreibungen.

4 Novell Nsure – Novell’s Secure Identity Management

Novell ist als führender Anbieter von Informationslösungen bekannt geworden durch das Betriebssystem Novell NetWare. Mit den Novell Directory Services verfügte Novell NetWare bereits frühzeitig über ein leistungsfähiges Berechtigungssystem. Novell Nsure stellt die konsequente Weiterentwicklung dieses Berechtigungssystems zu einer plattformunabhängigen, systemübergreifenden Secure Identity Management Lösung dar. Dabei basiert auch diese Lösung auf einem modularen Konzept, welches durch Hinzunahme verschiedener Komponenten an die individuellen Anforderungen eines Unternehmens angepasst werden kann.



4.1 Novell eDirectory

Novell eDirectory ist die Weiterentwicklung der Novell Directory Services und stellt als LDAP-basierender Verzeichnisdienst das zentrale Identity Management dar. Als fester Bestandteil enthält Novell eDirectory das Produkt Novell eGuide, eine Web-basierende Applikation zur Abfrage von LDAP-Verzeichnissen über die bei entsprechender Authentisierung auch im Identity Management hinterlegte Daten modifiziert werden können.

4.2 Novell DirXML

Novell DirXML ist ein auf XML basierendes Provisioning Subsystem. Fulfilment Agents – die sogenannten „Konnektoren“ – stehen u.a. für die Standardschnittstellen JDBC und LDAP, sowie für eine Vielzahl weiterer Applikationen in den Bereichen Mail, Netzwerkbetriebssysteme und ERP zur Verfügung. Über eine Entwicklungsumgebung können jederzeit individuelle Anbindungen realisiert werden.

4.3 Novell SecureLogin / Novell iChain

Single Sign-On – die Anmeldung eines Benutzers an sämtlichen für ihn freigeschalteten Systemen mit lediglich einem Anmeldevorgang – verspricht erhebliche Verbesserungspotentiale bei Sicherheit und Effizienz. Identity Management – ein zentrales Verzeichnis sämtlicher Benutzer – ist eine grundlegende Voraussetzung hierfür. Novell bietet mit Novell SecureLogin Single Sign-On für den Desktop, sowie mit Novell iChain Single Sign-On für Web-basierende Umgebungen.

4.4 Novell ZENworks

Die automatisierte Bereitstellung von Anwendungen basierend auf individuellen Benutzerprofilen wurde bereits als Anwendungsbeispiel für Secure Identity Management genannt.

Novell ZENworks ermöglicht die Verteilung von Anwendungen auf verschiedene Endgeräte. Durch die Integration von Novell ZENworks in das Identity Management kann dies als automatisierter Prozess basierend auf den hinterlegten Regeln und Rollen erfolgen. Darüberhinaus bietet Novell ZENworks umfangreiche Management-Funktionalitäten, wie z.B. Remote Control und Inventarisierung.

5 Zusammenfassung

Secure Identity Management adressiert das Bedürfnis von Unternehmen nach effektivem Schutz ihrer Daten, die im Zeitalter der Wissensgesellschaft ein wertvolles Gut darstellen. Der zentrale Lösungsansatz verspricht Flexibilität und Effizienz, der integrative Lösungscharakter macht Secure Identity Management zu einer wirtschaftlich sinnvollen Investition. Novell bietet als führender Anbieter von Informationstechnologie mit Novell Nsure markterprobte Secure Identity Management Lösungen, die durch ein modulares Konzept auf die individuellen Unternehmensanforderungen zugeschnitten werden können.