

## Statement of the Month – Novell Identity & Security

Düsseldorf im September 2007

### Veränderte Vorzeichen: Identität als Service

**wie jede andere Technologie auch, zum Beispiel das Auto, das Telefon oder das Internet, weckt Identitätsmanagement seit den Anfangstagen Bedürfnisse und Interessen, die vor dem Entstehen der Technologie in diesen Ausmaßen eigentlich unbekannt waren. Zunächst ging es um einfache Authentifizierung mittels Passwörtern und Zugriffskontrolle. Inzwischen gehören Multi-Faktor-Authentifizierung, Biometrie und Federated Identities zum Repertoire. Aber, wie bei allen anderen großen Technologien auch, ist das Ende der Fahnenstange noch lange nicht erreicht. Mit dem zunehmenden Einsatz und der Verbreitung von Identitätsmanagement wachsen die Anforderungen, denen sich die Technologie anpassen muss. Marina Walser, Director Identity & Security Management bei Novell Central Europe, erläutert, warum in Zukunft Service-orientierte Ansätze im Mittelpunkt stehen werden.**

In den mehr als zehn Jahren, seit das Thema Identitätsmanagement das erste Mal aufgetaucht ist - zu Beginn noch in Form von Meta-Directories - , hat sich die Technologie rasant weiterentwickelt. Inzwischen befinden wir uns in der dritten Generation und zwei weitere Generationen zeichnen sich schon am Horizont ab. Den Anfang machte die einfache Zugangskontrolle zu Systemen und Ressourcen. In einem zweiten Schritt wurden die Technologien zur Zugriffsüberwachung ausgefeilter, seitdem kommen Multifaktor-Authentifizierung, Biometrie und Meta-Verzeichnisdienste zum Einsatz. Statt lediglich Zugriff einzuräumen, beziehungsweise zu verweigern, ging es schnell um das Management von Verzeichnisdiensten und um Metaverzeichnisdienste, die eine Vielzahl an Systemen synchronisieren. In der aktuellen dritten Phase stehen Rollen und Rechte im Vordergrund sowie Genehmigungsprozesse und deren Dokumentation. Jeder kann so nur gemäß seiner Rolle auf Unterlagen und Systeme zugreifen. Die Sicherheitsrisiken, die Unternehmen aus eigenen Reihen drohen, werden dadurch minimiert. Seit dieser Generation verschiebt sich der ursprüngliche Fokus bereits auf die Anwendungen, aber es geht nach wie vor um Authentifizierung und Autorisierung. Im Kern wird das auch so bleiben. Nur die Herausforderungen, die damit gelöst werden, ändern sich in der nahen Zukunft.

Die vierte Generation wird zeigen, dass Identitätsmanagement-Systeme die besten Depots für Informationen über ihre Nutzer sind. Mit diesen Informationen lässt sich weitaus mehr machen, als lediglich Nutzer verwalten und in Gruppen einteilen. Compliance Systeme können zum Beispiel Identitäten nutzen, um Richtlinien einzuhalten und webbasierte Anwendungen können unter Verwendung der Identitäts-Informationen personalisierte Dienste anbieten. Dabei gilt: Je mehr Informationen die Anwendungen über ihre Nutzer haben, desto besser können sie personalisiert zur Verfügung stehen. Durch Identitätsmanagement als Service-basiertes Modell können Anwendungen leichter Informationen über Identitäten verwenden. Gleichzeitig werden die Administration und der Zusammenschluss von Identitäten (Federation) vereinfacht und so Identitätsmanagement schneller, besser und kostengünstiger.

### Paradigmenwechsel in der vierten und fünften Generation

In dieser Generation, die sich schon mehr und mehr durchsetzt, wird es also einen Paradigmenwechsel geben, weg vom Fokus auf Authentifizierung hin zu einem Fokus auf verschiedene Services, die Identitätsmanagement-Systeme den Anwendungen über eine konsistente Oberfläche zur Verfügung stellen. Das heißt, es wird weniger um die Technologie gehen, die Zugriffe, Zugänge und Zutritte regelt, sondern viel mehr darum, was mit den Identitäten gemacht werden kann. Dieser Paradigmenwechsel wird sich in der dann folgenden fünften Generation noch stärker herausbilden. Im Modell der Zukunft wird es verschiedenste Nutzer von Identitäten geben. Jeder dieser "Kunden" ist dabei beispielsweise eine andere Anwendung mit anderen Anforderungen an die Personalisierung. Identitäten müssen auf vielfache Arten definiert werden, je nach Datenbank und Quelle. Identitätsmanagement rückt damit technologisch sehr nah an das Konzept der Service-orientierten Architektur (SOA) und inhaltlich an die Ideen von Business Intelligence heran.

Einige der Daten-Quellen sind vielleicht vom Unternehmen selbst definiert, nach den Zugriffsregelungen im Unternehmen. Andere sind eigene Definitionen der Nutzer, zum Beispiel bei der Verwendung einer Internetbasierten Dienstleistung. Diese Veränderung hat es in sich: Es wird nicht mehr um Inselsysteme zur Aufbewahrung von Identitäten gehen, sondern darum, Quellen und Eigenschaften von Identitäten auf schlüssige Art und Weise zusammenzuführen und den verschiedenen Konsumenten zur Verfügung zu stellen.

## Praxisbeispiel

Herr Müller ist im Meta-Verzeichnisdienst seines Unternehmens als Abteilungsleiter gelistet, das heißt, er kann in allen angebundenen Systemen zum Beispiel auf die Personal-Daten seiner Mitarbeiter, nicht aber auf die seiner Vorgesetzten zugreifen. Er nutzt außerdem eine webbasierte Anwendung, um seine Geschäftsreisen zu buchen und das Intranet, um sein Passwort zu ändern, wenn er es nach dem Urlaub wieder einmal vergessen haben sollte. Identitätsmanagement der ersten, zweiten und dritten Generation verschafft ihm Zugriff zu all diesen Systeme oder blockiert neugierige Blicke in Systeme, die ihn nichts angehen. Die Reiseplanungs-Anwendung im Internet begrüßt ihn mit "Hallo Herr Müller" und zeigt ihm seine bisherigen Reisepläne auf. Mit der vierten und fünften Generation von Identitätsmanagement ist das alles natürlich nach wie vor möglich, aber zudem kennt die Anwendung die Reisekostenrichtlinien des Unternehmens und bietet Herrn Müller für seine anstehende Dienstreise nach Berlin die günstigsten Verbindungen per Bahn an, wenn auf dieser Strecke Flugreisen weder preiswerter noch schneller zu haben sind. Die Möglichkeiten sind quasi unbegrenzt.

## Feinschliff durch Open Source Projekte

Den letzten Schliff werden allerdings nicht einzelne Hersteller alleine anlegen können. Gute Ansätze für die Erweiterung der Modelle bilden Open Source Projekte wie das Bandit Projekt ([www.banditproject.org](http://www.banditproject.org)). Im Rahmen dieses Projekts wird ein freies Framework für Identitätsmanagement-Systeme geschaffen. Teil der Entwicklungsarbeit sind diverse Komponenten, auf deren Basis sich Anwendungen und Dienste entwickeln lassen, die auf eine Reihe von Identitätsquellen und Authentifizierungsmethoden zurückgreifen können.

Ein weiterer Baustein des Bandit-Projektes ist Common Identity, eine Implementierung des Higgins-Frameworks, das Anwendern und Unternehmen einen plattformübergreifenden Zugriff auf Anmeldungsdaten und Profile gestatten soll. Im Unterschied zu herkömmlichen Ansätzen, bei denen die Daten auf zentralen Servern von Unternehmen und Anbietern verwaltet werden, ist das Identitätsmanagement beim Higgins-Model anwenderzentriert. Nutzer sollen dabei selbst entscheiden, welchen Webseiten sie welche persönlichen Informationen zur Verfügung stellen.

Identitätsmanagement-Systeme müssen sich zu Dienstleistungen wandeln und so Daten aus ganz verschiedenen Quellen zusammenführen, harmonisieren und die richtigen Ableitungen vornehmen, so dass diese den Anwendungen zur Verfügung stehen. Die Anwender fordern es so und die Technologie ist ebenfalls fast reif dafür.

## Über Novell

Novell, Inc. (Nasdaq: NOVL) bietet Infrastruktur-Software für das Open Enterprise an. Novell ist eines der führenden Unternehmen bei unternehmensweiten Betriebssystemen für Unternehmen auf Basis von Linux und Open Source sowie bei Sicherheits- und System Management Services, die benötigt werden, um heterogene IT-Umgebungen zu betreiben. Novell unterstützt seine Kunden dabei, Kosten, Komplexität und Risiken zu reduzieren, damit sie sich auf Innovation und Wachstum konzentrieren können. Das Unternehmen mit Hauptsitz in Waltham, Massachusetts (USA), beschäftigt weltweit rund 4.700 Mitarbeiter. Seit 1986 ist Novell durch die Novell GmbH in Düsseldorf auch auf dem deutschen Markt vertreten. Von diesem Standort aus werden Vertrieb und Marketing für Deutschland, Österreich und die Schweiz koordiniert - Niederlassungen befinden sich in Berlin, Frankfurt, München, Nürnberg, Wien, Zürich und Genf. Weitere ausführliche Informationen über Novell Lösungen, Produkte und Services stehen im Internet zur Verfügung unter [www.novell.com](http://www.novell.com) oder [www.novell.de](http://www.novell.de).

## Pressekontakt:

Lars Basche  
Text 100 Public Relations  
Tel: +49 - (0)89 - 99 83 70-33  
E-Mail: [novell@text100.de](mailto:novell@text100.de)

Ihre Ansprechpartnerin bei Novell:  
Ulrike Beringer  
PR Manager Novell Central Europe  
Tel: +49 - (0)89 - 206002118  
E-Mail: [uberinger@novell.com](mailto:uberinger@novell.com)