

Statement of the Month

Frankfurt / München / Düsseldorf, im Mai 2005

Die Identität im Mittelpunkt

Identity Driven Computing umfasst mehr als Personen und Passwörter

Das Thema Identitätsmanagement ist inzwischen in den Chefetagen angekommen. Die Marktforscher der International Data Corporation (www.idc.com) erwarten eine jährliche Wachstumsrate von 9,7 Prozent zwischen 2003 und 2008. Als Gründe dafür nennt IDC die Prozessoptimierung im B-to-B-Geschäft sowie die Revisionsrichtlinien der Politik. Aber was genau versteckt sich hinter dem Begriff Identitätsmanagement? Und geht es nicht sogar um viel mehr als die Verwaltung von Identitäten der Mitarbeiter, Lieferanten und Kunden? Muss der Begriff Identität daher nicht ausgeweitet werden? Marina Walser, Marketingleiterin bei Novell und Cambridge Technology Partners, untersucht die Bedeutung der Verwaltung von Identitäten.

In den Neunziger Jahren karikierte ein Cartoon das neu aufkommende Medium Internet. Zwei Hunde saßen vor einem Computer und der eine sagte zum anderen: "On the Internet, nobody knows that you are a dog." Diese Anonymität war der Schlüssel zur rasanten Verbreitung des World Wide Web. Die Freiheit, Informationen und Services ohne die „Blicke Dritter“ zu konsumieren, ist heute immer noch einer der Hauptgründe das Internet zu nutzen. Seriöse Kommunikation, egal ob im privaten oder im geschäftlichen Umfeld und egal über welchen Kanal, setzt allerdings voraus, dass keine Partei mit verdeckten Karten spielt. Denn natürlich muss jede Information überall und jederzeit verfügbar sein - aber nur für die richtigen Augen und Ohren, kurz: für autorisierte Identitäten. Um die Verwaltung der unzähligen Identitäten von Mitarbeitern, Partnern und Kunden ist in den letzten Jahren ein wichtiger Markt entstanden. Identitätsmanagement beschäftigt sich mit den so genannten 3As, das heißt Access (Zugangs)-Management, Authentication und Authorization sowie Provisioning.

In Unternehmen arbeiten zahlreiche Mitarbeiter, jeder mit einer anderen Identität. Jede dieser Identitäten benötigt andere Informationen für die tägliche Arbeit. Und geheime Informationen sind nur für einen Bruchteil dieser Identitäten freigegeben. Daher sollten Identitäten immer genau die Rechte zugestanden werden, die ihre Rolle im Unternehmen impliziert. Derzeit ist es in vielen Unternehmen aber noch eine große Herausforderung, zu verwalten, wer wie wann auf was zugreift. Jede Datenbank, jede Applikation, jedes Betriebssystem hat andere Sicherheits- und Zugriffskontrollen. Und jedes Unternehmen hat unterschiedliche Regeln, wer auf was zu welchem Zeitpunkt zugreifen kann und wie dieser Zugriff gewährleistet wird. Das Management von Identitäten und Zugriff muss daher grundlegende Infrastrukturkomponente sein.

Mit der Zuordnung von Identitäten zu Personen sind die Möglichkeiten aber längst noch nicht ausgeschöpft. Es reicht schließlich nicht aus, einer Person Zugriff zu gewähren, egal von wo aus. Oftmals sind die Endgeräte nicht geeignet, bestimmte Informationen zu erhalten und deren Sicherheit zu wahren. Identifiziert das IT-System also einen autorisierten Zugriff, aber über ein weniger geschütztes Endgerät oder das Internet, werden die Zugriffsrechte umgehend eingeschränkt - sofern die Technologie mitspielt. Ein Finanzchef will zum Beispiel am Flughafen in Los Angeles über seinen PDA auf interne Unterlagen zugreifen. Dafür müssen

Formate und Sicherheitsstandards angepasst werden. Oder ein Mitarbeiter aus der Personalabteilung druckt die Gehaltsliste aus - allerdings ist das nur auf dem Drucker am Schreibtisch möglich, nicht auf dem Abteilungsdrucker. Es gibt unzählige alltägliche Situationen in denen eine „menschliche“ Identität auf die Identität eines Systems trifft. Das heißt, die Sicherheit wird erhöht, weil zusätzlich zum Mitarbeiter auch noch sein Endgerät bekannt ist, also eine eigene Identität hat. Eine Identität ist demzufolge ein Identifizierungsmerkmal, das in einem IT-System vorgehalten oder einem solchen System präsentiert wird, um eine Person oder im erweiterten Sinne ein Gerät/eine Software zu identifizieren. Demzufolge kann jede Person/Hardware/Software über verschiedene Identitäten verfügen - je nach Anzahl der genutzten Systeme und abhängig von den verschiedenen Rollen, die zum Beispiel dem Angestellten einer Firma zugewiesen sind. Zudem können auch Daten oder Prozesse über eine Identität verfügen.

Künftig werden daher auch Hardware und IT-Systeme als Identitäten in der Infrastruktur geführt werden. Denn nur so ist es möglich, die Anforderungen nach Flexibilität und Sicherheit zu erfüllen. Zum Beispiel mit Web Services, die in Abhängigkeit von der Identität, die sie angefordert hat, Aktionen ausführen oder nur beschränkt umsetzen. Die IT wird also intelligent, von der Identität getrieben und um die Identität herum aufgesetzt - neudeutsch: Identity Driven Computing.

Ein Beispiel verdeutlicht diesen Ansatz: Ein Unternehmen stellt einen neuen Manager ein. Wie jeder andere neue Mitarbeiter benötigt er eine Identität: einen Zugangsnamen, ein Passwort, eine eMail Adresse, Datei- und Druckdienste sowie Zugang zum ERP-System des Unternehmens. Die IT-Abteilung muss einen Usernamen für den Manager kreieren, einen Server Account einrichten und mit dem Laptop des Managers abgleichen, einen Account innerhalb des ERP-Systems einrichten, breite Nutzungsrechte einräumen, die Passwörter einstellen. Das Netzwerk muss über den neuen Manager und den neuen Rechner informiert werden, damit er seine Informationen vom Büro oder von unterwegs abrufen kann. Ähnliche Vorgänge müssen gestartet werden, wenn ein Mitarbeiter in ein anderes Büro oder auf ein neues Projekt wechselt oder durch einen Nachfolger ersetzt wird. Wenn vorab Regeln für den neuen Job definiert worden wären und die Identität im Zentrum des Unternehmens stehen würde, ließen sich die zahlreichen, dahinter liegenden IT-Prozesse auf wenige Mausklicks reduzieren.

Die Identität sollte daher in den Mittelpunkt eines Unternehmens gestellt werden. Nur so lassen sich erhebliche Kosteneinsparungen, eine Vereinfachung der IT-Prozesse, eine deutliche Erhöhung der Produktivität und Effektivität sowie der Sicherheit im Unternehmen erreichen. Identitätsmanagement beschleunigt sicheren und regulierten Zugriff auf Informationen und Systeme und steigert so zudem die Agilität, das heißt die Fähigkeit, sich schnell zu wandeln und neuen Anforderungen anzupassen - und verschafft den Unternehmen damit einen entscheidenden Wettbewerbsvorteil.

Über Novell

Novell, Inc. (Nasdaq: NOVL) ist seit mehr als 20 Jahren im Markt und entwickelt und vertreibt „Software for the Open Enterprise“. Mit offener, Standard-basierter Software unterstützt Novell mehr als 50.000 Unternehmen und Institutionen in 43 Ländern dabei, ihre IT-Umgebungen einfacher und sicherer zu gestalten und zu verwalten sowie besser zu integrieren. Novell Kunden erhalten die Kontrolle über ihre IT-Infrastruktur zurück und senken die Kosten. Dabei werden sie weltweit von 5.200 Novell Mitarbeitern, 5.000 Partnern und technischen Support Centers unterstützt. 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 oder www.novell.de.

Weitere Informationen:

Ulrike Beringer
Manager Public Relations
Novell GmbH
Phone +49 (0) 89 206 002 118
eMail: <mailto:uberinger@novell.com>
Internet: <http://www.novell.com>

Novell Presseservice
vibrio Kommunikationsmanagement Dr. Kausch GmbH
Markus Pflugbeil
Senior PR Consultant
Phone +49 (0) 89 32 15 18 62
Fax +49 (0) 89 3 21 51 77
eMail: <mailto:markus.pflugbeil@vibrio.de>
Internet <http://www.vibrio.de>