

Statement of the Month – Novell Identity & Security

Düsseldorf im Juli 2007

Von Kaffeepausen und Wettbewerbsvorteilen

Die Herausforderungen, denen sich die IT-Verantwortlichen heute gegenübergestellt sehen, ähneln sich – egal in welcher Branche oder Unternehmensgröße: Es geht darum, Kosten zu reduzieren oder zumindest konstant zu halten, den Betrieb aufrecht zu erhalten und gleichzeitig neue oder veränderte Geschäftsprozesse optimal zu unterstützen. Dabei ist natürlich die Sicherheit der Informationen zu gewährleisten und dies auch im Sinne der Compliance zu dokumentieren. Das ist nichts Neues und nicht erst seit gestern so. Marina Walser, Director Business Development Identity & Security bei Novell, erläutert, wieso neue Ansätze dennoch dringlicher denn je gebraucht werden.

Meist spielen mehrere Aspekte ineinander, wenn es darum geht, Lösungen für die zunehmend komplexer werdenden IT-Herausforderungen zu finden. Die IT wird im Unternehmen längst nicht mehr separat betrachtet, sondern ist immer mehr gefordert, aktiv die Geschäftsprozesse zu unterstützen.

1. Zugriff auf Web- und Unternehmensanwendungen

Die Anzahl der Anwendungen im Unternehmen hat sich drastisch erhöht und verändert: Neben den klassischen Host-Anwendungen sind eine Vielzahl von Web-Anwendungen dazugekommen. Jedoch bringt jede Anwendung ihre eigene Benutzerverwaltung mit sich, mit eigenen Formaten und Schnittstellen. Einzelne Abteilungen wollen zudem die Hoheit über Ihre Anwendungen häufig nicht abgeben und deshalb auch weiterhin ihre Datenspeicher selbst verwalten. Benutzer benötigen daher verschiedene Log-ins, um auf ihre jeweiligen Anwendungen zuzugreifen. Die Folgen sind bekannt: Vergessene Passwörter schrauben die Kosten für den Helpdesk in die Höhe und verringern die Produktivität, während notierte Passwörter auf gelben Zettelchen der Sicherheit wenig zuträglich sind. Eine Lösung, die den Abteilungen die Kontrolle über die Applikationen überlässt, ohne dass hierfür Agenten installiert oder andere Anpassungen an den Anwendungen vorgenommen werden müssen, kann diese Herausforderung lösen.

2. Mobile Nutzer

Die Mitarbeiter im Unternehmen werden immer mobiler. Die manuelle Verwaltung der mobilen Endgeräte ist nicht mehr zeitgemäß und effizient. Eine klassische Herausforderung ist der Zugriff auf Unternehmensanwendungen von außen und zwar auf alle Anwendungen, nicht nur die Web-basierten. Der Zugriff soll schnell, mit hoher Performanz und einfach funktionieren. Gleichzeitig muß die Sicherheit der Daten gerade beim Zugriff von außen gewährleistet bleiben, so dass keine unberechtigten Benutzer die Systeme ausspionieren können. Hier bieten sich eine VPN-Lösung und reverse Proxy an, die deutlich flexibler und einfacher einzurichten sind als klassische IP-Sicherheits-VPN-Lösungen.

3. Temporäre, externe Mitarbeiter

Im Zuge der Flexibilisierung der Geschäftsabläufe sind nicht mehr nur fest angestellte Mitarbeiter im Unternehmen tätig, sondern immer mehr temporäre Mitarbeiter, die projekt-bezogen eingesetzt werden. Für diese Personengruppe dürfen natürlich vom ersten Tag an nur die Systeme freigeschaltet werden, die sie tatsächlich benutzen dürfen, um keine unnötigen Kosten zu verursachen. Mittels Selbst-Registrierung und Rollen-basierten Genehmigungs-Prozessen für die Freischaltung von Systemen können diese Vorgänge vereinfacht und beschleunigt werden. Systemgestützt kann dann der Zugriff auch wieder entzogen und vor allem dokumentiert werden. Dies gibt einem Unternehmen die Möglichkeit, vor dem Wirtschaftsprüfer jederzeit Rechenschaft über Zugriffe auf die einzelnen Systeme abzulegen. Gleichzeitig lassen sich so die Lizenzkosten optimieren, da einsehbar ist, wer auf welche Systeme zugegriffen hat und welche Benutzerkonten gelöscht werden können. Ein angenehmer Nebeneffekt ist, dass auch sichtbar wird, welche Systeme überhaupt genutzt werden und welche nur Kosten verursachen, ohne Nutzen zu bringen. Schon alleine dadurch kann sich eine Investition in Identitätsmanagement rechnen.

4. Prozess-Integration mit Kunden und Lieferanten

Lieferanten und Kunden werden immer enger mit einem Unternehmen verzahnt und greifen auf interne Systeme zu – ohne dass das Unternehmen diese Zugriffe wirklich zu kontrollieren, geschweige denn zu dokumentieren vermag. Die Mobilfunk-Branche arbeitet zum Beispiel stark über indirekte Vertriebskanäle. Diese müssen schon allein aus Wettbewerbsgründen schnell und problemlos auf die Systeme des Anbieters zugreifen können. Die vorhandenen IT-Systeme (CRM / ERP) sind allerdings meist auf die Unterstützung von internem Vertrieb ausgerichtet und nur kostspielig umzurüsten. Lösungen Marke Eigenbau mit Sammel-Accounts für Vertriebspartner bergen hohe Risiken und Probleme beim Nachweis von Compliance. Abhilfe für eine flexible und gleichzeitig sichere Anbindung bietet Identity Federation. Dabei wird eine Gruppe von

Partnern gebildet, die auf Basis von geschäftlichen- und technologischen Vereinbarungen den Nutzern oder Mitgliedern eines Partners den Zugriff auf Ressourcen ermöglicht, ohne dass dieser sich noch einmal registrieren muss. Die Kernelemente sind Single Sign-On, Zugriffskontrolle, der sichere Austausch der Identitäten und Identitäts-Mapping oder die Verlinkung von Nutzerkonten. Damit können die vielen festen und wechselnden Mitarbeiter eines Vertriebspartners etwa einer Handelskette angebunden werden und es wird lückenlos dokumentiert, welcher Mitarbeiter eine Bestellung ausgelöst hat. Wann immer die Identität von Kunden oder privaten Konsumenten verbunden werden soll, sollten sie die Hoheit über die eigenen Identitätsdaten behalten, das heißt, sie entscheiden selbst, ob und zu welchem Anbieter ihre Identitäten übertragen werden.

5. Merger & Acquisitions umsetzen

Unternehmenszusammenschlüsse sind heute eher die Regel als die Ausnahme. Damit sich die vielbeschworenen Synergien auch tatsächlich realisieren lassen, muss die IT-Abteilung die Systeme so schnell wie möglich integrieren und optimieren. Hier kommen alle oben genannten Aspekte in Kombination zum Tragen. Unterschiedliche Abteilungen mit unterschiedlichen Standards und Sicherheitskonzepten müssen einheitlich und am besten identitätsbasiert auf Anwendungen und Informationen zugreifen können. Die Bedeutung von Datensicherheit steigt, da weitere Standorte und zusätzliche mobile Mitarbeiter angebunden werden. Personalveränderungen im Zuge von Akquisitionen müssen sich möglichst umgehend auch in den Systemen widerspiegeln. Zudem werden die Beziehungen zu Kunden, Lieferanten und Absatzkanälen konsolidiert. Die IT-Verantwortlichen sind gefordert, den Kunden möglichst schnell den einheitlichen Zugriff auf ihre Informationen und, sobald die Strategen ihre Arbeit beendet haben, auch auf neue Anwendungen zu verschaffen. Und auch die Lieferanten werden nur für begrenzte Zeit ihre Bestellungen über zwei unterschiedliche Systeme verwalten wollen.

Es geht also in allen Facetten darum, Zugriffe auf Anwendungen und Informationen effizient, sicher und für alle Seiten zufriedenstellend zu gestalten. Unterstützung bieten Access Management Lösungen, die die Identität des Benutzers durch Authentifizierung validieren, den Zugriff auf Systeme basierend auf der validierten Identität des Benutzers gewähren, eine konsistente "User Experience" durch Web Single Sign-On ermöglichen, für eine sichere Übertragung der Informationen und Daten sorgen und die Informationen über eine Identität einer Anwendung so zur Verfügung stellen, dass personalisierte Services möglich sind. Eine möglichst einfache Handhabung einer solchen Lösung setzt dem Ganzen dann noch die Krone auf. Eine technische Lösung, die alle diese Herausforderungen auf einen Streich löst, gibt es leider nicht und wird es wohl auch nie geben. Organisation, Prozesse und nicht zuletzt die Kommunikation spielen eine wesentliche Rolle beim Gelingen. Solche Veränderungen sind natürlich nicht umsonst und fordern finanzielle sowie personelle Mittel. Da Sicherheit schwer messbar ist - zumindest so lange noch nichts passiert ist - fällt die Zuweisung von Budgets nicht immer leicht. Aber gerade beim Thema Access Management geht es nicht nur um drei Minuten Zeitersparnis beim Einloggen in die Systeme, die dann für eine zusätzliche Tasse Kaffee wieder drauf gehen. Es geht um Wettbewerbsfähigkeit, neue Geschäftspotenziale und einen schnelleren Marktzugang. Wenn der CIO diese Themen adressiert und die Vorteile für die Geschäftsprozesse klar formuliert, kann er bei seinen Kollegen von der Fachseite punkten und die IT als Nutzenbringer für das Unternehmen positionieren.

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 oder www.novell.de.

Pressekontakt:

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

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