

Statement of the Month – Novell Identity & Security Management

Düsseldorf im Juli 2008

Sicherheit als Teamaufgabe

In allen Unternehmen haben die Sicherheitsbeauftragten die gleiche Mission: die geschäftskritischen Posten wie Daten und Vermögen und anderes zu schützen. Ob es nun darum geht, dass nur autorisierte Mitarbeiter ein Gebäude betreten oder auf ein Netzwerk zugreifen, sowohl beim physischen als auch beim logischen (System-)Zugang dreht sich alles darum, die richtigen Personen reinzulassen. Und nur die Richtigen. Beide Bereiche verfolgen dasselbe Ziel, nähern sich diesem aber auf unterschiedlichem Weg und in den meisten Unternehmen auch von unterschiedlichen Stockwerken, sprich Abteilungen, aus an. Marina Walser, Director Identity & Security Management bei Novell Central Europe, untersucht, ob die strikte Trennung noch zeitgemäß ist.

Das externe Beraterteam, das drei Monate lang beim Kunden ein- und ausgegangen ist, hat das Projekt erfolgreich abgeschlossen. Der Projektleiter gibt dem IT-Verantwortlichen im Unternehmen Bescheid, dieser löscht umgehend die Zugriffe der Berater auf das firmeninterne Netzwerk und andere vertrauliche Daten. Eigentlich ist alles bestens und zu einem sauberen Abschluss gebracht. Aber was ist eigentlich mit den Keykarten? Sind die alle zurückgegeben bzw. gesperrt worden? Mitnichten. Die Abteilung, die für die Netzwerkzugänge, das heißt den logischen Zugriff, zuständig ist, hat nicht automatisch der Abteilung für physischen Zugriff Bescheid gegeben. Der Beraterfirma wird natürlich keinerlei böse Absicht unterstellt, wenn nicht alle Keykarten am letzten Projekttag auftauchen. Schließlich sind sie für ihre Arbeit gut bezahlt worden und werden die Kundenbeziehung auf keinen Fall gefährden. Eine mitgenommene Keykarte lässt ohnehin noch längst nicht auf Hintergedanken schließen - gerade Berater haben nicht selten eine wahre Sammlung an Hotelzimmer-Keykarten, die sie aus Versehen eingepackt haben. Kein Grund zur Besorgnis, die sind ohnehin wert- und nutzlos und werden dann einfach bei nächster Gelegenheit entsorgt. Beim Verlassen eines Hotels beziehungsweise der Begleichung der Rechnung wird die Keykarte sofort gelöscht. Das kann zwar unpraktisch sein, wenn der Gast etwas im Zimmer vergessen haben sollte und noch einmal dorthin zurück möchte, ist aber sicherheitstechnisch äußerst lobenswert. So einfach geht das in einem Unternehmen leider nicht. Eine Keykarte ist oftmals mit den Daten des Nutzers verknüpft, damit auch nachgewiesen werden kann, wann dieser sich wo aufgehalten hat und warum er zum Beispiel gerne mal nachts das Büro aufsucht.

Die aus Versehen eingesteckte Zutrittskarte für das Unternehmen ist beim seriösen Dienstleister natürlich eigentlich in guten Händen. Was aber, wenn einer der Berater auf einmal die Firma wechselt und noch eine Rechnung offen hat – ob nun mit dem Kunden oder dem eigenen Arbeitgeber. Auf jeden Fall ist eine Sicherheitslücke entstanden. Diese Art von Lecks entstehen nicht nur durch die Einbeziehung Externer. Mal angenommen, ein Mitarbeiter verlässt das Unternehmen, gibt seine physische Zutrittskarte ordnungsgemäß ab und probiert aus Spaß aus, ob er vom privaten Rechner von zuhause aus noch immer auf das Unternehmensnetzwerk zugreifen kann – in vielen Fällen kann er. Das sollte nicht mal im Spaß möglich sein.

In den meisten Unternehmen gibt es nach wie vor unterschiedliche Systeme, in denen der Status eines Mitarbeiters festgehalten ist und die darauf aufbauend Aktionen auslösen wie Karte sperren, Zugang löschen, Zahlungen einstellen etc. Diese Trennung der physischen und der IT-Sicherheitsabteilungen in Unternehmen ist traditionell gewachsen. Zunehmende Risiken und Gefahren sowie staatliche Vorschriften verlangen aber heute die enge Zusammenarbeit der beiden Abteilungen. Vorreiter bei der Zusammenführung sind Institutionen und Organisationen aus dem öffentlichen Bereich, die Industrie zieht langsam nach. Die Kombination der physischen und der digitalen Sicherheitswelt hat viele Vorteile: Der physische Zugang zu einem Gebäude kann eng mit dem logischen Zugriff auf Computer und Netzwerkressourcen gekoppelt werden. Unternehmen können so Sicherheitsrisiken minimieren und gleichzeitig Geld und Zeit sparen.

Grundlage dafür ist ein Identitätsmanagement-System, das mit einer Plattform für die Kontrolle von physischem Zugriff integriert ist. Damit können Rollen verwaltet werden und die richtigen Personen für die jeweiligen Zugriffe und Zugänge identifiziert werden. Auf diese Weise kann eine einheitliche Sicherheitsrichtlinie für das gesamte Unternehmen ausgerollt werden. Sicherheitssilos gehören damit der Vergangenheit an. Identitätsinformationen müssen zudem nicht mehr manuell in verschiedenen Systemen gepflegt werden. Nicht zuletzt bei Firmenzusammenschlüssen und -übernahmen, die meist mit schnellen Mitarbeiterveränderungen einhergehen, wird dadurch Zeit gewonnen. Für die manuelle Pflege in verschiedene Systeme bleibt da keine Zeit. Und zudem haben alle Sicherheitsmitarbeiter auf diese Weise eine zentrale Anlaufstelle für Nutzerinformationen aller Art und Abteilungen.

Es ist natürlich nicht damit getan, die beiden Abteilungen im Gebäude auf eine Etage ziehen zu lassen und darauf zu hoffen, dass so die Zusammenarbeit verbessert wird. Grundlage ist eine Kombination der Plattform für Zugriffskontrolle mit einer Identitätsmanagement-Lösung. So kann sichergestellt werden, dass der Zugriff sowohl auf physische als auch auf logische Ressourcen mit der Nutzeridentität verknüpft ist und nur autorisierte Personen tatsächlich Zugriff erhalten. Weit vorne auf der Agenda sollte die Automatisierung der Nutzer-Provisionierung stehen. Die Abteilungen werden dadurch von der manuellen Pflege entlastet, sparen Zeit und Geld ein. Dabei ist es nicht erforderlich, beide Abteilungen komplett ineinander zu integrieren. Jede Abteilung hat ihre Berechtigung im Unternehmen. Die Gebäudesicherheit ist schließlich nicht nur für die Zutrittssysteme verantwortlich und die IT-Security nicht nur für die Provisionierung der Mitarbeiter. Im Team kann aber mit weniger Aufwand gewährleistet werden, dass wirklich nur die richtigen Personen reinkommen - von der Eingangstür bis zur Computertastatur.

Über Novell

Novell, Inc. (Nasdaq: NOVL) bietet eine Linux-Plattform auf höchstem technischen Niveau, die vollständig kompatibel mit den Systemen zahlreicher anderer Anbieter ist. Ergänzt wird das Portfolio durch integrierte IT Management Software, mit der Unternehmen weltweit Kosten, Komplexität und Risiken reduzieren können. Mit dieser Infrastruktur-Software und einem umfassenden Partnernetzwerk integriert Novell heterogene IT-Umgebungen und ermöglicht so, dass Menschen und Technologie als eine Einheit zusammen arbeiten. Weitere Informationen unter www.novell.com.

Pressekontakt:

Ulrike Beringer
Novell GmbH
Tel.: +49 (0)89 20600 2118
E-Mail: uberinger@novell.com

Sabine Minar
Text 100 Public Relations
Tel.: +49 (0)89 99 83 70 20
E-Mail: novell@text100.de