

Statement of the Month - Oktober 2008

Novell Identity & Security Management

Gut integriert ist halb gewonnen

Knappe Budgets hin oder her, die aktuelle Situation an den Finanz- und sonstigen Märkten rückt das Thema Risk Management plötzlich wieder stärker in den Vordergrund und zeigt, dass es in diesem Bereich nach wie vor mehr als genug zu tun gibt. Die Verantwortlichen müssen zahlreiche gesetzliche Anforderungen erfüllen, Compliance-Prüfungen bestehen und ihre Unternehmen und Kunden vor internen und externen Angriffen und Gefahren schützen. Die Technologien und Lösungen, die sich für diese Herausforderungen auf dem Markt derzeit finden, sind dabei nur die halbe Miete. Die Unternehmen brauchen Wege, um die hohen Ausgaben in IT-Sicherheit zu rechtfertigen und gleichzeitig zu belegen, dass sie die Compliance-Vorgaben erfüllen und die sensiblen Daten ihrer Kunden schützen. Marina Walser, Director Identity & Security Management bei Novell Central Europe, untersucht, wie sich dieser Spagat ohne Verrenkungen bewerkstelligen lässt:

Das Management von IT-Sicherheit hat inzwischen – endlich muss man fast sagen - einen festen Platz auf den Agenden der CIOs ergattert. Grund sind die wachsenden Anforderungen von Seiten der Politik, der Unternehmen und der Kunden, aber nicht zuletzt auch die jüngsten Ereignisse, die jedem vor Augen führen, auf welch wackligen Beinen die Sicherheit von sensiblen Daten manchmal steht. Unternehmen achten immer stärker darauf, wer auf was zugreifen kann und ob das alles seine Richtigkeit hat. Das sind sie ihren Kunden schließlich auch schuldig.

Ineffiziente Überwachungsprozesse stehen dem guten Willen allerdings oftmals noch im Weg. Nutzer warten manchmal Wochen auf einen voll aktivierten Account. Andererseits existieren viele Benutzerkonten noch lange über ihr Verfallsdatum hinaus, das heißt nicht selten Wochen nachdem der Nutzer das Unternehmen verlassen hat. Zudem werden Provisionierungsmechanismen, Regeln für Zugriffskontrollen und Security Information Management-Lösungen in den meisten Fällen in Silos vorgehalten. Von einem holistischen Blick in Echtzeit auf die unternehmensweiten IT-sicherheitsrelevanten Aktivitäten sind die meisten weit entfernt.

Es ist also eines, automatisierte Lösungen zur Gewährleistung von IT-Sicherheit und zur Überwachung von Ereignissen im Einsatz zu haben, ein anderes ist es aber, diese Lösungen auch miteinander zu verknüpfen. Unternehmen müssen in der Lage sein, Sicherheitsdaten mit Identitäts-Informationen anzureichern und automatisiert unangebrachte und verdächtige Aktivitäten im Unternehmensnetzwerk festzustellen, zu berichten und zu beseitigen. Nur so erhalten sie ein komplettes Bild der Sicherheitsvorkommnisse im Unternehmen und können entsprechend reagieren – im Idealfall sogar automatisiert. Wenn diese Verknüpfung fehlt, wie das heute in den meisten Unternehmen der Fall ist, so werden zwar einerseits der Zugriff geregelt und Rollen- und Rechte verteilt, andererseits wird aber nicht überprüft, ob diese eingehalten werden. Lösungen für Identitätsmanagement und Ereignis-Überwachung sind jeweils die halbe Miete. Eine Integration dieser ist hilfreich. Die ganze Miete und ein komplettes Bild ermöglichen aber erst „integrierende“ Lösungen.

Über Novell

Novell, Inc. (Nasdaq: NOVL) bietet eine Linux-Plattform, die für die nahtlose Integration in verschiedenste Plattform- und Anwendungsumgebungen konzipiert ist, sowie ein Portfolio an integrierter IT-Management-Software, mit der Unternehmen weltweit Kosten, Komplexität und Risiken reduzieren können. Mit dieser Infrastruktur-Software und einem umfassenden Partnernetzwerk verbindet 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
Email: uberlinger@novell.com

Sabine Minar / Julia Zeisberger
Text 100 Public Relations
Tel: +49 (0)89 - 99 83 70-20/-19
Email: novell@text100.de