Statement of the Month – Novell Identity & Security Management

Düsseldorf im September 2008

Endgeräte und Datensicherheit: Achilles lässt grüßen

Der moderne Wissensarbeiter steht im ständigen Spannungsfeld zwischen Büro, Mobilität und Meetings, immer mit dem Laptop oder anderen mobilen Geräten unter dem Arm, immer einsatzbereit. Das muss man mögen und es ist nicht selten anstrengend – nicht nur für den Anwender, sondern auch für den, der ihm diese Mobilität ermöglicht und dabei gleichzeitig die Sicherheit wahren muss. Die IT-Abteilungen werden immer stärker gefordert. Carsten Grashorn, Director Systems and Resource Management bei Novell, untersucht, welche Wechselbeziehungen im modernen Datenverarbeitungsumfeld bestehen und wie sichere Mobilität gewährleistet werden kann:

Die Ursachen von Datenmissbrauch sind vielfältig, in den meisten Fällen handelt es sich um verlorene Endgeräte wie Laptops oder Handhelds. Auch wenn kritische Daten an Externe oder Outsourcer übergeben werden, entsteht eine nicht unbedenkliche Sicherheitslücke. Und nicht zuletzt spielen Papieraufzeichnungen sowie Angriffe von intern oder extern eine wichtige Rolle dabei, dass Daten zunehmend unsicherer und deren Schutz zunehmend aufwändiger wird.
Interessanterweise reagieren Unternehmen nach einem Datenmissbrauch jeglicher Art oft sehr schnell. Verschlüsselung von Daten, Datenverlustvorbeugung, Identitäts- und Zugriffsmanagement, Endpoint-Security-Kontrollen und Sicherheits-Ereignismanagement: Die Liste der Maßnahmen, die im Schadensfall ergriffen werden, ist lang. Die Industrie hat sich hier einiges einfallen lassen. Aber warum wird damit eigentlich immer erst gewartet, bis etwas passiert ist? Ein wesentlicher Grund liegt in der Schwierigkeit, Schadensfälle wirklich zu beziffern, also die tatsächlichen Kosten und Folgen zu benennen, die ein Vorfall mit sich bringt. Was würde es bedeuten, wenn Daten in falsche Hände geraten? Welche finanziellen und für das Image relevanten Auswirkungen würde das haben? Bestürzt werden Vorfälle bei anderen Unternehmen zur Kenntnis genommen, in dem vermeintlich sicheren Wissen, dass das im eigenen Unternehmen aber nie passieren könnte. Bis es dann passiert. Erst dann laufen die Mühlen und auf einmal ist keine IT-Lösung zu teuer.

Zu diesen Adhoc-Lösungen müssen Unternehmen heute immer öfter greifen, nicht zuletzt weil die Anzahl der mobilen Geräte rasant zunimmt. Von einer verstärkten Mobilität erwarten sich viele Firmen eine erhöhte Produktivität und größere Flexibilität. Voraussetzung dafür ist, dass der Nutzer auf alle Daten, die er für die Verrichtung seines Jobs benötigt, dezentral zugreifen oder sich diese Daten sogar auf sein jeweiliges Endgerät verschieben kann. Das geht allerdings mit erhöhten Risiken und entsprechenden Kosten einher. Aber echte Mobilität lässt sich nur realisieren, wenn auf Daten von außen zugegriffen werden kann, die entweder lokal gespeichert sind oder über das Internet genutzt werden. Und dabei entstehen gefährliche Lücken.

Eine umfassende Sicherheitslösung für Endgeräte, neudeutsch auch Endpoint Security genannt, muss sowohl Datenschutz, als auch Zugriffssteuerung und den Gerätezustand, das heißt die Einstellungen und Zustände des Endgeräts, einbeziehen. Endgeräte sind natürlich nicht immer nur Laptops, mit denen Anwender sich in ein Netzwerk einwählen und auf Daten zugreifen, sondern auch kleinere Datenträger wie USB-Sticks, deren Speicherkapazität inzwischen beeindruckende Ausmaße annimmt. Die große Mehrzahl der Anwender nutzt die USB-Sticks mit bestem Wissen und Gewissen: einfach um Daten auszutauschen. Aber auf der neuen Generation dieser handlichen Helfer hat nicht selten eine ganze Festplatte Platz. Ausgeklügelte Scripts erlauben es, dass USB-Speichergeräte für illegale Downloads vertraulicher Daten verwendet werden, ohne dass der Endnutzer etwas davon merkt. Der USB-Stick wird einfach angeschlossen und lädt automatisch Daten herunter.

Moderne Endpoint-Security-Lösungen können derartige Vorgänge unterbinden oder den Zugriff eines USB-Sticks auf ein Endgerät komplett blockieren. Aber wie komme ich dann an Daten auf einem USB-Stick, um die es in ursprünglich harmloser Absicht eigentlich ging?

Es geht also um die Gratwanderung zwischen der Gewährleistung von Mobilität und Produktivität und der Wahrung größtmöglicher Sicherheit. Kein leichtes Unterfangen für die IT-Abteilungen. Basis ist zunächst die Erkenntnis beim Anwender, dass überhaupt Gefahren bestehen und diese minimiert werden müssen. Diese Einsicht fehlt noch in den meisten Unternehmen. Die gewonnene Freiheit des mobilen Arbeitens möchte sich niemand so einfach nehmen lassen. Ein kombinierter Ansatz, mit dem nicht nur die Endgeräte der Mitarbeiter sondern gleichzeitig auch die Geräte von externen Beratern und Gastnutzern verwaltet und gesichert werden können, führt am ehesten zum Ziel, ohne die „Freiheiten“ zu stark einzuschränken.

Ähnlich wie in der griechischen Mythologie, in der Achilles am ganzen Körper unverwundbar gemacht werden sollte, die Ferse aber verhängnisvollerweise frei blieb, geht es heute vielen Unternehmen. Firewalls, Zugriffsbeschränkungen, Verschlüsselungen und viele andere IT-Lösungen schützen die meisten Zu- und Ausgänge zu Unternehmensnetzwerken, aber mit der zunehmenden Mobilität steigt auch die Komplexität deutlich an. Endgeräte, die heute mit allen PCs kommunizieren können – meist ohne Transparenz und Kontrolle – sind die Schwachstellen der Unternehmenssicherheit. Achilles wurde diese Schwäche zum Verhängnis. Moderne IT-Lösungen für Endpoint Security können dagegen sicher stellen, dass ein Unternehmen nicht in die Fußstapfen des Halbgottes treten muss, sondern seine „Fersen“, das heißt die internen und externen Endgeräte, optimal absichert.

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