

Statement of the Month – Novell Identity & Security

Düsseldorf im November 2007

IT-Sicherheit auf dem Desktop – der menschliche Faktor

Für die Sicherheit der IT-Systeme hat sich der Mensch als Unsicherheitsfaktor Nummer 1 herausgestellt; schließlich ist es immer ein Mitarbeiter, der verseuchte E-Mails öffnet oder dem USB-Sticks mit wertvollen Unternehmensdaten gestohlen werden. Demnach wäre die IT nur hundertprozentig sicher, wenn der Mensch gar nicht mehr mit ihr in Berührung kommt. Zu dumm nur, dass er die IT, zuallererst in Form eines Desktops, zum produktiven Arbeiten benötigt. Marina Walsler, Director Identity & Security Management, Novell Central Europe, rückt das Verhältnis zwischen Mensch und IT zurecht und zeigt einen gangbaren Weg für mehr Sicherheit auf dem Desktop und um ihn herum auf.

Das Thema Sicherheit ist schon allein deshalb menschlich, weil es ebenso widersprüchlich ist wie der Mensch: Einerseits ist Sicherheit eines der Grundbedürfnisse des Menschen, andererseits ist der Mensch selbst der größte Unsicherheitsfaktor, vor allem wenn es um die IT geht: Schließlich ist es menschlich, sich von Social Engineering-Tricks aufs Kreuz legen zu lassen, die um Liebe werbende E-Mail zu öffnen oder sich den mit sensiblen Daten bestückten USB-Stick aus der Jackentasche klauen zu lassen.

Was also tun gegen den Unsicherheitsfaktor Mensch in der IT? Die einfachste Lösung wäre sicher, ihm die Ressource IT generell zu sperren. So abwegig scheint das in gewissem Maße für einige Unternehmen gar nicht zu sein. Nicht wenige nehmen nämlich tatsächlich den Aufwand auf sich, USB-Ports an PCs und Notebooks zu verblenden, damit die Mitarbeiter über diese Schnittstelle nichts ein- oder ausschleusen können. Aber ist das eine Lösung? Bestimmt nicht, schließlich kann der USB-Port durchaus die Produktivität eines Mitarbeiters erhöhen. Die Logik einer solchen Maßnahme: Wenn du es nicht benutzt, kannst du es nicht kaputt machen. Das ist bestechend einfach, aber auch töricht. Und alles andere als menschlich.

Auch ein gegenteiliges Vorgehen hat seine Tücken: Denn wo käme ein Unternehmen wohl hin, wenn es sich gerade in punkto Sicherheit voll auf die Eigenverantwortlichkeit der Mitarbeiter verlässt und keine Kontrollen einbaut? Würde jeder Mitarbeiter eigenständig Patches vornehmen oder Antivirendateien aktualisieren, würden sensible Unternehmensdaten bei unkontrolliertem Zugriff nicht nach außen dringen? Es steht zu befürchten, dass ein solch naiver Appell an das Verantwortungsbewusstsein auch nicht weit führen würde – allenfalls in ein höchst menschliches Chaos, siehe etwa die aktuelle Misere um die beiden verschwundenen CDs mit Bürgerdaten aus dem britischen Finanzministerium.

Was also tun? Vielleicht ist es an dieser Stelle angebracht, einen alten Grundgedanken vom Staub zu befreien, nämlich: Technik ist für den Menschen da, nicht umgekehrt. Der Mensch steht im Mittelpunkt, der Rest ist zuallererst ein Arbeitswerkzeug. Von hier aus kann man weiter gehen und kommt dann vielleicht zu einem weiteren Grundgedanken: Nicht jeder Mensch ist gleich, nicht jeder hat die gleichen Aufgaben, nicht jeder braucht die gleichen Arbeitswerkzeuge.

Wäre es nicht sowohl aus wirtschaftlicher wie auch aus sicherheitstechnischer Sicht äußerst wünschenswert, wenn jeder Mitarbeiter genau das Set an Werkzeugen, sprich: genau die IT-Ressourcen, Daten-Pools, Speichermenge, Applikationen, USB-Ports zur Hand hat, die er benötigt, um seine Arbeit mit maximaler Effizienz erledigen zu können? Allerdings – diese individuelle IT-Einrichtung des Arbeitsplatzes beansprucht nicht geringen Aufwand. Angesichts von Personalknappheit und der zunehmenden Komplexität der IT-Verhältnisse in Unternehmen ist die Bereitschaft für ein solches Unterfangen gering. Automatisierte IT-Lösungen helfen hier aus.

Ein Patch-Management sorgt dafür, dass alle Programme und Anwendungen, die Mitarbeiter auf ihrem Desktop nutzen, immer auf dem neuesten und damit sichersten Stand sind. Ein automatisiertes Zugangs- sowie Endpoint Security Management hilft dabei, die Sicherheit der Unternehmens-Netzwerke immer zu gewährleisten – egal, wer wann von wo auf welche Ressourcen zugreift. Schließlich ermöglichen Asset Management-Lösungen der IT-Abteilung – ohne langes Zusammensuchen und Erfragen – einen schnellen Überblick über alle IT Ressourcen und deren Nutzung, über Lizenz-Laufzeiten sowie über alle IT-Verträge und Budgets. Dies spart Zeit, Geld und Nerven der ITler und der Unternehmensleitung. Und es kommt noch besser: In diesem Fall gilt nämlich der schöne Spruch, was gut für das Unternehmen ist, ist auch gut für den Mitarbeiter. Dieser muss sich keinen unnötigen Kopf um Sicherheits- und Administrationsfragen machen und kann seine Arbeit so erledigen, wie es für ihn am besten ist. Die IT ist also für den Menschen da – ganz so, wie es sein soll.

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