

Statement of the Month

Novell Consulting, im Mai/Juni 2006

Kabellos surfen - mit Sicherheit?

Der Trend zum drahtlosen Netz im Unternehmen (WLAN) ist nicht aufzuhalten. Eine drahtlose Datenübertragung ist jedoch immer auch eine Einladung für Hacker oder Chalker, wie die ungebetenen Lauscher genannt werden, die sich von außerhalb eines Gebäudes in ein WLAN einklinken können. Chalker sind findige Freaks, die eine Zeichensprache aus dem Mittelalter in das Web-Zeitalter übertragen haben. Im Mittelalter hinterließen Reisende häufig Kreidemarkierungen, um Empfehlungen oder Warnungen, beispielsweise zur Qualität von Unterkünften, an nachfolgende Reisende zu übermitteln. Heutige Chalker (engl. Chalk = Kreide) zeichnen mit Kreide auf, an welchen Standorten sich frei zugängliche drahtlose Netzwerke befinden. Drahtlose Datenübertragung oder auch generell Computernetze stellen eine Einladung für Hacker dar, egal ob von außen oder innerhalb des Unternehmens. Zum Glück gibt es Gegenmaßnahmen, beispielsweise in Form moderner Verschlüsselungstechniken. Marina Walser, Director Business Development Identity Management bei Novell, untersucht gemeinsam mit Klaus Schmech vom Novell Partner Cryptovision, wie sich im Netz mit Sicherheit arbeiten lässt:

WLAN ist praktisch, ob für Unternehmen oder für private Zwecke. Einfach Laptop anschalten und ins Netz einloggen, egal wo, ohne lästige Einschränkungen durch fehlende oder zu kurze Netzkabel. Einzige Voraussetzung: Innerhalb der Reichweite des kabellosen Netzwerkes muss es schon sein. Aber die ist inzwischen dehnbar und relativ flexibel. Selbst in Biergärten kann der Unersättliche kabellos surfen und auf Messen lässt sich damit fast so reibungslos arbeiten wie in den eigenen vier Bürowänden. Wenn da nicht nur wieder das leidige Thema Sicherheit wäre. Ein WLAN stellt mindestens so hohe Sicherheitsansprüche wie ein LAN. Es geht schließlich um wesentlich mehr als um die Mitbenutzung der Bandbreite durch Schnorrer, sondern um den Schutz vertraulicher und sensibler Unternehmensdaten, die nicht in fremde Hände geraten sollten.

Datennetze stellen heute in den meisten Unternehmen lebenswichtige Kommunikationsadern dar. Informationen müssen fließen, damit Unternehmen ihre Kunden besser bedienen, ihren Umsatz erhöhen und ihre Effizienz steigern können. Der Netzwerkzugang wird daher zwangsläufig für Telearbeiter und Geschäftspartner freigeschaltet. Außerdem sollen die eigenen Mitarbeiter natürlich von unterwegs zugreifen können und per VPN ins Extranet kommen. Ein weltoffenes Unternehmen lässt es sich zudem nicht nehmen, Beratern und anderen Auftragnehmern Zugriff einzuräumen. Das Ergebnis ist eine äußerst heterogene Netzwerk- und Anwenderstruktur - mit unzähligen potenziellen Sicherheitslücken.

Der erste Schritt zur Behebung dieser möglichen Schwachstellen besteht aus einer richtigen Nutzung der LAN-Bordmittel. Mit den relevanten Standards können Netzwerknamen verborgen (SSID-Hidding), Zugriffsadressen gefiltert und Nutzer mit zuvor festgelegten Schlüsseln authentifiziert werden. Für eine noch weiter gehende Absicherung bieten sich portbasierende Zugangskontrollen an, die Sicherheitsabfragen schon am Netzzugangspot durchführen - eine sinnvolle Maßnahme sowohl für WLAN als auch für LAN. Darüber lassen sich Zugangskontrollen (benutzerorientiertes Regel-/Rollensystem),

Abrechnung (Billing, Accounting) und Bandbreitenzuweisung (Quality of Service pro User) umsetzen sowie Benutzerprofile anlegen.

Mit diesen Hilfsmitteln kann gesteuert werden, welche Endgeräte und Clients Zugriff auf bestimmte Netzwerk-Ressourcen haben. Natürlich muss dahinter ein durchdachtes Rollen-Management stehen, das heißt es muss genau geklärt sein, wer was darf und wer nicht, sonst nützen die besten Zugangskontrollen nichts.

Die Anmeldung am Netz kann über ein Passwort erfolgen. Sicherer als ein Passwort ist jedoch die Nutzung einer Public-Key-Infrastruktur (PKI), wie sie Security-Spezialisten anbieten, beispielsweise Cryptovision. Als PKI bezeichnet man die Gesamtheit von Hardware und Software, die zum sicheren Einsatz von Verschlüsselung und digitaler Signatur in einer größeren Organisation benötigt wird. Digitale Zertifikate bescheinigen dem Anwender, dass der verwendete Schlüssel korrekt ist. LAN und WLAN werden damit umfassend abgesichert und vor allem beim Einsatz von Smartcards ist eine PKI deutlich sicherer als Passwortabfragen. Ihr gesamtes Potenzial entfaltet eine PKI jedoch erst, wenn sie für weitere Zwecke eingesetzt wird. Hierbei bieten sich vor allem Datei-Verschlüsselung, die Absicherung von Web-Portalen und E-Mail-Verschlüsselung an. Gerade Unternehmen, bei denen Berater ein und ausgehen, die eine hohe Mitarbeiterfluktuation haben oder generell zahlreichen Personen Zugriff auf ihr Netzwerk gewähren (müssen).

Die Lösungen sind also vorhanden. Eine Untersuchung des Marktforschungsunternehmens Experton Group bei ausgewählten Anwenderunternehmen in Deutschland hat allerdings kürzlich ergeben, dass die zur Verfügung stehenden technologischen Möglichkeiten noch nicht ausgeschöpft werden. "Die Lage wird besser" so Andreas Burau, Vorstand der Experton Group. "Kein Unternehmen lässt sein WLAN vollkommen schutzlos". Aber wie lange dauert es noch, bis Chalker keine Verwendung mehr für ihre Kreide haben?

Über Novell

Novell, Inc. (Nasdaq: NOVL) ist seit mehr als 20 Jahren im Markt und entwickelt und vertreibt „Software for the Open Enterprise“. Mit offener, Standard-basierter Software unterstützt Novell mehr als 50.000 Unternehmen und Institutionen in 43 Ländern dabei, ihre IT-Umgebungen einfacher und sicherer zu gestalten und zu verwalten sowie besser zu integrieren. Novell Kunden erhalten die Kontrolle über ihre IT-Infrastruktur zurück und senken die Kosten. Dabei werden sie weltweit von 5.200 Novell Mitarbeitern, 5.000 Partnern und technischen Support Centers unterstützt. 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.

Weitere Informationen:

Ulrike Beringer
Manager Public Relations
Novell GmbH
Phone +49 (0) 89 206 002 118
eMail: <mailto:uberinger@novell.com>
Internet: <http://www.novell.com>

Novell Presseservice
vibrio Kommunikationsmanagement Dr. Kausch GmbH
Markus Pflugbeil
Senior PR Consultant
Phone +49 (0) 89 32 15 18 62
Fax +49 (0) 89 3 21 51 77
eMail: <mailto:markus.pflugbeil@vibrio.de>
Internet <http://www.vibrio.de>