

Statement of the Month - Novell Consulting

Düsseldorf, im Oktober 2005

Gefahr erkannt - Gefahr gebannt?

Umfrage zu IT-Sicherheit unterstreicht Bedarf an zeitgemäßen Lösungen

Die Angriffe auf Unternehmensnetze werden immer zahlreicher und raffinierter. Nach internationalen Statistiken wurden in den letzten Jahren pro Woche im Durchschnitt 50 Sicherheitslücken in Betriebssystemen und grundlegenden Anwendungen gefunden (Quelle: www.silicon.de). Mit dem heutigen Stand der Technik können die meisten Sicherheitslücken rechtzeitig erkannt und geschlossen werden. Das Bewusstsein für die Gefahren ist vorhanden, so eine aktuelle Umfrage von Novell. Zwei Drittel aller Unternehmen schätzen das Schadenspotenzial von Angriffen auf ihr Netzwerk als hoch ein. Aber folgen Worten auch Taten? Stefan Schimansky, Director Novell Consulting, untersucht, wie intensiv sich deutsche Unternehmen mit Sicherheitsaspekten beschäftigen und welche Komponenten unentbehrlich sind:

Netzwerksicherheit beinhaltet die Planung, Umsetzung und Überwachung aller Maßnahmen und Aktionen zum Schutz der IT-Infrastruktur und der darauf laufenden Anwendungen. In der heutigen Zeit, in der unternehmensübergreifend eng zusammengearbeitet wird, müssen Unternehmensnetze durchlässig sein - aber nur für bestimmte Inhalte und Zugriffe. Vor schädlichen externen Einflüssen müssen sie ausnahmslos geschützt werden. Gleiches gilt aber auch für den Schutz nach innen - die Ursachen für Systemabstürze beispielsweise liegen nicht selten bei den eigenen Mitarbeitern. Zudem werden die Gefahren, die innerhalb der Unternehmen drohen, derzeit noch oft unterschätzt. Die Gefahren von außen werden erkannt, registriert, aber was folgt danach? Eine Umfrage von Novell unter 52 Unternehmen zeigt, wie die „Sicherheitsuhr“ bei den Anwendern tickt:

Gefahr erkannt

- ⌘ Mehr als zwei Drittel aller befragten Teilnehmer schätzen das Schadenspotenzial von Außenangriffen auf ihr Netzwerk als hoch bis sehr hoch ein.
- ⌘ 80 Prozent aller Unternehmen haben gleichzeitig verschiedene Lösungen für die Bereiche Firewall, VPN, Content Filtering und Spyware Protection im Einsatz. Mit dem Ergebnis, dass knapp 40 Prozent durch die eingesetzten Security Lösungen Leistungseinbußen bei ihren Webapplikationen oder dem Durchsatz der Internetverbindungen beobachten.
- ⌘ Nur knapp mehr als die Hälfte aller befragten Unternehmen verfügen über detaillierte Kostenübersichten für den Bereich Internet-Sicherheit.

Gefahr gebannt?

- ⌘ Für 79 Prozent der befragten Unternehmen ist die Flexibilität und Skalierbarkeit von Sicherheitslösungen sehr wichtig.
- ⌘ Nur 19 Prozent aller befragten Unternehmen mussten in den letzten drei Monaten Performanceverluste durch Spy- bzw. Adware hinnehmen. Experten gehen jedoch davon aus, dass knapp ein Viertel aller Spyware unentdeckt bleibt, weil die schädlichen Dateien sehr gut im System versteckt werden. Zudem gibt es Schadprogramme, die so programmiert sind, dass sie den Virensch scanner ausschalten. Entdeckt die Schutz-Software dann kritische Dateien und Registry-Einträge, installiert die Spyware die gelöschten Dateien einfach mit dem nächsten Rechnerstart

neu.

- ⌘ 42 Prozent der Unternehmen gaben an, über keinen Mechanismus zu verfügen, der Updates und Patches zentral verwaltet und taggleich einspielt.
- ⌘ Der Aufwand für Administration und Verwaltung der sicherheitsrelevanten Systeme wird von 57 Prozent aller Unternehmen als mittel bis hoch eingeschätzt.

Die Gefahren sind also bekannt, aber die Lösungen zur Gefahrenabwehr sind offenbar zu umständlich oder sie werden ignoriert. Wie muss ein zeitgemäßer Schutz für das Netzwerk aussehen, welche Komponenten sind nötig für umfassende Sicherheit?

1. Firewall Schutz:

Eine Firewall ist die Basis für Netzwerksicherheit, sie überwacht im Idealfall den gesamten Datenverkehr zwischen Internet und internem Netzwerk und blockiert unautorisierte Zugriffsversuche von außen wie auch unerlaubte Verbindungen nach außen.

2. VPN Gateway:

Ein Virtual Private Network (VPN) ermöglicht es Organisationen, das Internet als sichere und kostengünstige Kommunikationsplattform zu nutzen. Außenstellen, externe Mitarbeiter und Geschäftspartner lassen sich mit einer ebenso hohen Sicherheitsstufe anbinden, wie es sonst nur über teure Standleitungen möglich ist. Die Daten müssen mittels VPN Gateway über Verschlüsselungsmethoden geschützt werden. Nur so können unterschiedliche Benutzer komfortabel und sicher angebunden werden.

3. Surf Schutz:

Auch die unkontrollierte Internet-Nutzung am Arbeitsplatz verursacht hohe Schäden durch Produktivitätsausfälle und erhöht das Sicherheitsrisiko durch Viren- oder Spyware-Attacken. Administratoren müssen die Möglichkeit haben, den Web-Zugriff für unterschiedliche Gruppen im Unternehmen zu konfigurieren und so zum Beispiel den Zugriff auf indizierte Seiten zu unterbinden.

4. Viren Schutz:

Die Folgen von Angriffen durch Computerviren sind zahlreich: Datenverlust, Produktivitätsausfälle, Serverfehler, Bindung von Personal-Ressourcen sind nur einige davon. Ein umfassender Virenschutz erkennt und blockiert eMail- und Web-Viren zuverlässig, indem zum Beispiel eMail-Nachrichten und deren Anhänge untersucht werden.

5. Spam Schutz:

Spam eMails sind mit einem hohen Produktivitätsverlust verbunden, der Unternehmen mittlerweile Hunderttausende von Euro pro Jahr kostet. Zudem verstopft Spam die Netzwerke und sorgt für gefährliche Sicherheitslöcher. Die elektronische Massenwerbung muss daher durch den Einsatz verschiedener Erkennungsmechanismen aussortiert werden.

6. Schutz gegen unberechtigte Zugriffe:

Hacker werden immer einfallreicher, wenn es darum geht, Schwachstellen in modernen Computersystemen aufzuspüren, auszunutzen und neuartige Angriffe zu entwickeln, die die traditionellen Schutzmechanismen umgehen. Diese Ausspä- und Angriffsversuche müssen erkannt und blockiert werden.

Alle genannten Sicherheitssysteme sind im Markt erhältlich - die Herausforderung besteht darin, auf dem neuesten Stand zu bleiben, um stets gegen neue Angriffsarten gefeit zu sein.

Handeln ist dringend notwendig: Eine aktuelle Umfrage des IT-Beratungsunternehmens PricewaterhouseCoopers (www.pwc.com) unter mehr als 8.000 IT-Verantwortlichen aus 63 Ländern zum Thema Sicherheit zeigt, dass die Zahl der sicherheitsbezogenen Vorfälle im Jahr 2005 um 22,4 Prozent im Vergleich zum Vorjahr gestiegen ist - die Schutzmechanismen werden immer besser, doch gleichzeitig steigen die Gefahren.

Und noch bedenklicher: Marktforscher erwarten, dass in wenigen Jahren die existierenden

Sicherheitsmaßnahmen in Unternehmen obsolet sein werden - einfach weil die Gefahren sich zu stark verändert haben. Mittels Web Services zum Beispiel, einer zu Recht hochgelobten Technologie, umgehen Daten Firewalls und schaffen so neue Gefahren.

Was ist also zu tun: Die Anbieter müssen Technologien entwickeln, die denen der Angreifer immer einen Schritt voraus sind. Und in den Unternehmen müssen die Sicherheitsrisiken endlich realistisch eingeschätzt werden und ausreichend Gelder für IT-Sicherheit bereitgestellt werden.

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>