Special Innovation

Keine Chance den Viren

Egal ob Kleinunternehmer oder Global Player: Wer von unliebsamen, zumeist kostspieligen Überraschungen verschont werden will, muss sein Computernetz vor externen und internen Bedrohungen schützen.

Sonja Gerstl

Unternehmensnetzwerke sind sensible Gebilde. Böswillige Attacken, Hacker-Aktivitäten oder auch fahrlässiges Handeln können Betriebssysteme empfindlich beeinträchtigen und immense Folgekosten verursachen. Geeignete Software kann alle Aktivitäten eines Netzwerkes überwachen sowie Auskunft über eventuell vorhandene Sicherheitslücken erteilen und entsprechende Gegenmaßnahmen setzen.

Die Basics hierfür sind jedem PC-User bekannt. Punkt 1: die Firewall. Jeder, der Zugriff auf das Internet hat oder mittels E-Mail mit anderen kommuniziert, braucht eine intelligente Firewall-Lösung. Das gilt selbstredend auch für die Absicherung von Netzwerken. Ein Firewall-System soll effektiv und leicht administrierbar sein. Punkt 2: Antivirus-Lösungen. Der lokale Virenschutz am Arbeitsplatz hat ausgedient, seitdem Mail Server und Server die bevorzugten Betätigungsfelder von Viren, Würmern und sogenannten Trojanischen Pferden sind. Die Software-Industrie offeriert jährlich neue Produkte, die einen umfassenden Schutz versprechen. Mitunter ist ein enormer infrastruktureller Aufwand notwendig, um in vernetzten Unternehmen Daten vor unerlaubten Zugriffen zu schützen. Viele IT-Security-Anbieter sind deshalb dazu übergegangen, Packages anzubieten, die neben konventionellen Sicherheitsfunktionen auch noch zahlreiche Goodies wie zum Beispiel Net Flow Analyzer, die eine permanente Kontrolle von Netzwerken garantieren, offerieren.

High-End-Lösungen

Die Angebotspalette reicht hierbei von Einsteigerapplikationen bis hin zu High-End-Lösungen mit Monitoring und automatischer Alarmierung. Darüber hinaus bietet der Markt auch All-in-one-Security-Lösungen, die effizienten Schutz vor externen und internen Bedrohungen gewährleisten. Vor allem interne Bedrohungen machen Betriebssystemen diversen Statistiken zufolge schwer zu schaffen. Demnach ereignen sich rund 80 Prozent der Vergehen gegen die IT-Security innerhalb des eigenen Datennetzwerkes. Nicht immer steckt Absicht dahinter. Oftmals ist es Unwissenheit oder Neugier, die Mitarbeiter die Grenzen des Systems austesten lassen. Damit derlei Experimentierfreudigkeit nicht massive Schäden anrichten kann, verfügen viele Firmen mittlerweile über ein Intrusion-Detection-System. Vergleichbar mit einer Alarmanlage, reagiert dieses unverzüglich bei Auffälligkeiten – also wenn etwa ein Mitarbeiter versucht, an Unternehmensdaten zu gelangen, für die er keine Zugriffsberechtigung hat. Automatisierte Reaktionen, die bis zur Blockierung der Anbindung des betreffenden Users an das Netzwerk reichen, sind die Folge.

Zugriffsberechtigungen für sensible Unternehmensdaten sollten sorgsam ausgestellt werden. Foto: Bilderbox.com

Viren & Würmer

Gezielt, effizient und zerstörerisch.

Viren, Würmer und Trojanische Pferde gehören zu den Schattenseiten des Computerzeitalters. Sie beschädigen Hardware, Software und Daten, belegen Arbeitsspeicher und deaktivieren Firewalls und Antivirenprogramme. Auch wenn Bedrohungen à la Sasser-Wurm vorerst gebannt sind – Entwarnung ist nicht angesagt. Um sich vor katastrophalen Folgen zu schützen, empfehlen Experten einen sorgsamen Umgang mit E-Mails unbekannter Absender. Darüber hinaus wird zu einem permanenten Update der Antivirus-Software geraten. Finger weg auch von Software-Programmen, die kostenlos zum Download angeboten werden – diese gelten als anfällig für Trojanische Pferde, also Computerprogramme, die wie nützliche Software aussehen, in Wahrheit aber Viren ins Netzwerk schleppen. Virenkarten (wie auf *www.de.trendmicro-europa.com*) informieren laufend über weltweit akute Bedrohungen. *sog*

Erhöhte Wachsamkeit ist angezeigt. Foto: Kapsch BusinessCom

Interne Verlustträger

Mitarbeiter stellen höchstes Sicherheitsrisiko für Firmen dar.

Als hätten sie nicht schon alle Hände voll damit zu tun, potenzielle externe Gefahren wie Hacker-Attacken abzuwehren, droht Unternehmen nun auch eine sukzessive Zersetzung von innen. Schuld daran haben der durchschnittliche europäische Mitarbeiter und sein allzu leichtfertiger Umgang mit vertraulichen Geschäftsdaten. Zu dem Ergebnis kam jedenfalls eine im Auftrag des IT-Sicherheitsunternehmens McAfee erstellte Umfrage. Demnach verlassen pro Woche und Mitarbeiter neun Dokumente gemeinsam mit ihren jeweiligen Sachbearbeitern das Büro. Meistens handelt es sich um Unterlagen zum laufenden Geschäftsverkehr, die auf elektronischem Wege oder auf Speichermedien wie USB-Sticks aus Unternehmen gelangen. Aber auch Kundendaten und Kundenakte werden gerne nach Hause mitgenommen. Dalibor Galic, Sales-Spezialist der Alcatel-Lucent AG: „Das höchste Sicherheitsrisiko ist der Mitarbeiter – ob absichtlich oder unabsichtlich sei dahingestellt." Vor allem die zunehmende und häufig unternehmensintern forcierte Mobilität ihrer Belegschaft mache Firmen immer mehr zu schaffen. „Oftmals werden Laptops, Handys und andere Datenträger gar nicht als Unternehmens-, sondern vielmehr als Privateigentum betrachtet", erläutert Thomas Blaschka, Head of Product Management bei Kapsch Business Com, die Problematik. Künftig, so ist man sich einig, müsse das Sicherheitsmanagement von Unternehmen verstärkt nach innen gerichtet sein. *sog*

Ein sorgloser Umgang mit Unternehmensdaten kann fatale Folgen haben. Foto: Kapsch BusinessCom

Beruf: Hacker

Experten decken Sicherheitslücken auf.

Aktive Datensicherheit ist allen Unternehmen wichtig. Nicht immer ist allerdings auf den ersten Blick ersichtlich, wie die bestehende Infrastruktur abgesichert werden kann, welche Daten und Applikationen geschützt werden müssen und wie das firmeninterne Netzwerk vor Missbrauch bewahrt werden kann. Abhilfe versprechen Security-Spezialisten, die Unternehmen bei der Erstellung, Umsetzung und dem Betrieb eines maßgeschneiderten Konzeptes unter die Arme greifen.

Risikoanalyse

Kapsch Business Com bietet als spezielles Security Service einen sogenannten Hack Check, der Sicherheitslücken in Netzwerken sichtbar machen soll. Dabei werden Komponenten wie Firewall, Mail Server oder Web Server überprüft. Kapsch dringt dabei von außen in das Netz des Kunden ein – agiert also wie ein „normaler" Hacker. Selbstverständlich erfolgt dieser „Angriff" in Abstimmung mit dem zu „hackenden" Unternehmen. Neben der technischen Überprüfung wird noch eine andere Form der Risikoanalyse angeboten. Hierbei wird zwecks Mängelaufdeckung physisch in das Unternehmen des Auftraggebers eingedrungen. Thomas Blaschka, Head of Product Management bei Kapsch Business Com: „Wir versuchen Dokumente, die eigentlich geshreddert werden müssten, aus Papierkübeln rauszufischen. Oder wir stehlen uns in Besprechungsräume, benutzen die Telefonanlage, aktivieren Computer und testen, wie weit wir an unternehmensinterne Daten herankommen können." Nur: So genau wollen es Österreichs Unternehmen anscheinend nicht wissen – die Nachfrage nach diesem Full-Service ist derzeit noch enden wollend. *sog*