

Eigene Mitarbeiter sind das IT-Sicherheitsrisiko Nummer eins

Risikofaktor Mensch

Zum Thema IT-Sicherheit findet man nur selten Beiträge, die ohne die schon sehr strapazierten Schlagworte Hacker, Viren und Trojaner auskommen. Der daraus resultierende Gewöhnungseffekt ist enorm: Das Bewusstsein für die Gefahren von Außen ist vorhanden, weswegen Unternehmen auf Netzwerke mehr oder weniger umfangreiche Schutzvorkehrungen treffen. Dabei übersehen sie eine wichtige Tatsache: mehr als die Hälfte aller Sicherheitsvorfälle ist auf menschliches Fehlverhalten zurückzuführen. Zu diesem Ergebnis kommen mehrere Untersuchungen. Vor allem kleine und mittelständische Unternehmen schenken dem Thema zu wenig Beachtung, einerseits aus Unterschätzung des Themas, andererseits aus der Unsicherheit heraus: Welche Vorsorgemaßnahmen sind die Richtigen? Wie hoch ist der Aufwand, der sich daraus ergibt?

Ohne Frage sind Schadprogramme, allen voran jene die an Spam-Mails gekoppelt sind, ein lästiges und nicht zu unterschätzendes Risiko für jedes Unternehmen. Noch im Frühjahr 2004 prophezeite Bill Gates ein Ende der Spam-Plage bis 2006. Ein schöner Gedanke! Doch ein kurzer Blick in den E-Mail-Eingangsortner und wir sind ernüchert. 300 neue Schadprogramme jeden Tag, Tendenz steigend, so die aktuellen Schätzungen. Dabei werden Malware-Schreiber immer raffinierter: Allein der Besuch einer manipulierten, vermeintlich sicheren Webseite reicht aus, um den Rechner zu infizieren. Ein entsprechendes Drag & Drop-Javascript-Exploit nutzt dabei die Sicherheitslücken im Internet Explorer, so dass allein durch das bloße Scrollen mit der Maus über

die mit manipulierte Seite eine .exe-Datei herunter geladen wird. Der Computer verwandelt sich unmerklich zu einem offenen Proxy und verschickt selbständig weiteren Spam oder fungiert im Botnetz als Zwischenlager für illegale Inhalte - ein sich selbst aufrechterhaltendes System.

Unternehmen steht eine große Zahl hocheffektiver Security-Tools zur Verfügung, mit denen sie ihr Netzwerk effektiv schützen können. Das Angebot ist vielfältig, aber auch verwirrend.

Unified Threat Management (UTM)-Appliances sind die Königslösung, denn sie vereinen alle wichtigen Funktionen wie Firewall, VPN-Gateway, Intrusion Prevention, E-Mail-Security etc. und ermöglichen eine bequeme Verwaltung der Komponenten über eine zentrale Bedienoberfläche. Anbieter wie gateProtect haben dabei an den Anwender gedacht und eine übersichtliche und grafisch gestaltete Bedienoberfläche geschaffen. Die Ähnlichkeit zum Windows-Desktop - sowohl funktionell als auch grafisch - ist gewollt und garantiert dadurch auch IT-Laien höchste Sicherheit bei einfachster Bedienung.

Jedoch muss generell gesagt werden, dass jede noch so hocheffiziente UTM-Firewall machtlos ist, wenn Mitarbeiter ein Unternehmen von innen heraus gefährden. Es ist daher Aufgabe des Managements, eine klare Informationspolitik zu betreiben, Mitarbeiter für die Gefahren zu sensibilisieren und den

Stellenwert von IT-Sicherheit insgesamt zu erhöhen. Klare Verhaltensregeln gegenüber Personen und Geräten bilden eine Basis, auf der weiteres Wissen über die Funktionsweise von Firewall, Spamfilter & Co. aufgebaut werden kann. Empfehlenswert ist eine kontinuierliche Weiterbildung durch Fachliteratur und Schulungen. Denn wie einst in einem Forum für IT-Administratoren zu lesen war: „Es gibt keinen Patch für die menschliche Dummheit.“

Eine umfassende Vorsorgestrategie kann hier aber zumindest das Risiko auf ein Minimum reduzieren. ↓

Dennis Monner
www.gateprotect.de



Der Autor dieses Beitrags, Dennis Monner, ist CEO bei der gateProtect AG, Hamburg.

IT-Sicherheit / Teil II

In der nächsten Ausgabe von CHEFBÜRO, die Ende Januar 2008 erscheint, finden Sie weitere Berichte zum Thema IT-Sicherheit. Hier präsentiert Robert Rothe, Geschäftsführer der eleven GmbH, acht Punkte zur Auswahl einer geeigneten Antispam-Lösung und Peter Lorant, Senior Director of Marketing & Channel Enablement bei Postini begibt sich auf die Spur der „Blended Threats“. Lesen Sie zudem, warum Pankl Racing Systems auf Aladdin eSafe Gateway vertraut und wie Blue Coat WebFilter Unternehmen in Echtzeit vor Phishing-Websites schützt.