Special Innovation

Besserer Schutz für Computer

Neue Bedrohungen aus dem Internet erfordern neue Sicherheitsmaßnahmen für die Informationstechnologie.

Ernst Brandstetter

90 Prozent aller ankommenden Mails sind bereits Spam. Mailboxen ohne entsprechenden Spam-Schutz sind unbrauchbar und wertlos. Firmen gehen verstärkt in Richtung Managed Services. Foto: Brandstetter

Die Sicherheit der Informationstechnologie (IT) in Unternehmen gewinnt vor dem Hintergrund zunehmender externer Bedrohungen sowie im Hinblick auf den Datenschutz im Inneren der Unternehmen immer mehr an Bedeutung. Die Fachwelt spricht in diesem Zusammenhang von „Blended Threats“, erklärt Wolfgang Schwarz, der bei Telekom Austria im Marketing Retail die Produktgruppe Business Internet & Services betreut.

Der neue Name der Gefahr wurde laut Schwarz deshalb üblich, weil sich Angriffe auf die Funktionalität und Integrität von IT-Anwendungen längst nicht mehr bloß auf virusinfizierte E-Mail-Dateianhänge konzentrieren. Heute würde sich quasi jeder einzelne IT-Nutzer allein durch die normale Inernet-Nutzung einem riesigen und perfiden Gefahrenpotenzial bestehend aus Spyware, Trojanern, Würmern oder neuen und unbekannten Viren aussetzen. „Durch die rasche und unentwegte Mutation dieser Arsenale wird das Risiko, Opfer einer Attacke aus dem Netz zu werden, zusätzlich potenziert“, konstatiert Schwarz. Gleichzeitig bieten häufig genutzte Applikationen wie P2P Filesharing, Instant Messenger und Remote Access in Firmennetzwerke weiträumige Angriffsflächen für Cyber-Kriminelle.

Mit Hinweis auf dieses Szenario geht die Gartner Group davon aus, dass Mail- und Web-Security bis 2010 zu einer konvergenten Dienstleistung verschmelzen werden. Das ist auch durchaus sinnvoll, meint Schwarz: „Bei Privatkunden werden E-Mail-Dienste von den Providern mehrheitlich im Internet-Paket inkludiert angeboten. Hier bietet sich die Verschränkung von Viren- und Spam-Schutz einerseits und einer Filterung des kompletten Internet-Datenflusses nach schädlichen und produktivitätshemmenden Inhalten in Echtzeit ganz besonders an.“ Die Schlagworte hinter einem künftigen umfassenden Web-Schutz lauten daher eingängig „saubere Leitung“ oder „Secure Access“.

IT-Sicherheit aus Unternehmenssicht

Telekom Austria hat gemeinsam mit neun weiteren IT-Anbietern bei Tech Consult eine entsprechende Studie in Auftrag gegeben, in deren Zuge IT-Entscheidungsträger von insgesamt 150 österreichischen Unternehmen mit mehr als 50 Mitarbeitern befragt worden sind. Die wichtigsten Resultate der Studie sind: verbessertes Bewusstsein für IT-Schutz, Vorbildrolle Österreichs beim Thema „Mobile Security“, Schutz vor Datenverlusten auf mobilen Geräten und Daten-Recovery (Datenschutz) sowie Identity Management (zielgerichteter Umgang mit Identitäten und Gestaltung von Zugriffsrechten über Authentifizierungstechnologien, proaktive Sicherheitstests über Security Audit, Ethical Hacking und Penetration Testing).

Ferner hat die Studie erhoben, dass sich IT-Security im Rahmen der Gesamt-IT-Investments mit einem Mittelwert von rund zwölf Prozent zu Buche schlägt. Zwei Drittel der befragten Unternehmen geben im Jahr mehr als 10.000 Euro für IT-Security-aus. Auf Basis dieser Daten und vorhandener Daten des Marktmodells E-Analyzer hat Tech Consult den Markt für IT-Schutz in Österreich hochgerechnet und kommt für die untersuchte Zielgruppe (Unternehmen mit mehr als 50 Mitarbeitern) für 2008 auf ein Gesamt-Investment für IT-Security von rund 800 Mio. Euro. Für 2009 wird bei einem Wachstum von 14 Prozent ein Marktvolumen von 913 Mio. Euro erwartet.

www.telekom.at

Managed Services

Bei Business-Kunden, wo an die Stelle einzelner Mailboxen Mailserver mit mehreren elektronischen Postfächern treten, wird E-Mail-Schutz heute zu einem marktrelevanten Teil über gemanagte Services abgewickelt. Ein Upgrade hin zu konvergentem Kombischutz von Mail und Web kann im Outsourcing-Modell von hochprofessionellen ASP-Partnern anforderungsgenau auf die Bedürfnisse des Kunden hin durchgeführt werden. Schwarz erklärt: „Die Möglichkeiten für Web-Security umfassen zum Beispiel Schutz vor Malicious Codes *(Schad-Software, Anm. d. Red.)*, vor Exploits *(Ausnutzen von Sicherheitslücken in der Nutzsoftware)*, vor Trojanern *(gezielt eingeschleuste „ferngesteuerte“ Schad-Software)* und Würmern *(in großer Menge und Kopien auftretende Schad-Software)*, eine mehrstufige Spyware-Abwehr *(anhand von Signaturen Vermeidung unbewusster Installation, Blockierung von Downloads und Unterbindung der Spyware-Kommunikation zwischen bereits infizierten PC mit dem Spyware-Server im Internet)* und zu guter Letzt Application Filtering nicht autorisierter Anwendungen *(etwa P2P Clients)*.“

Ungeschützt unbrauchbar

Experten gehen davon aus, dass bereits 90 Prozent aller ankommenden Mails Spam und Mailboxen ohne entsprechenden Spam-Schutz unbrauchbar und wertlos sind. Mailbox-Schutz und umfassende Sicherheit für die Nutzung von Web-Applikationen sind im Arbeitsalltag und auch zu Hause unverzichtbar geworden. Die existierenden Maßnahmen reichen jedoch noch immer nicht aus, weil mit der hohen Marktdurchdringung bei externen Medien und mobilen Endgeräten und ihrer stark verbreiteten Nutzung neue Angriffslinien für Hacker, Phisher und andere kriminelle Netzaktivisten eröffnet worden sind.

Beim Einsatz von CDs, DVDs, externen Festplatten, USB-Sticks und den mobilen Endgeräten Laptop, Personal Digital Assistant (PDA) oder Smartphone kommt dem Arbeitsplatzrechner in den Security Policies als „letzte Risikoinstanz“ besondere Beachtung zu. Die Antwort auf diese Form der Bedrohungen ist Desktop-Security, erklärt Schwarz. Hier werden dann alle Kunden-Clients proaktiv vor Sicherheitsrisiken und Netzwerkzugriffe geschützt. Der Leistungsumfang umfasst dabei klassischen Virenschutz, Personal Firewall und Intrusion Prevention, Spyware-Schutz-Funktionalitäten, Viren- und Spamschutz für E-Mail Accounts, Kindersicherung, Antiphishing, Schütz vor Online-Identitätsdiebstahl und Website-Prüfung in Echtzeit.

Sicherheitstrends

Wichtigster Trend im Sicherheitsdenken ist Security-Konvergenz, also die Zusammenfassung ausgewählter Sicherheitslösungen und -komponenten zu einem Security-Paket auf Basis einer integrierten Hardware-Box. Im Fachjargon wird diese Entwicklung auch Security Appliance genannt. Großen Handlungsbedarf orten Experten und immer mehr IT-Verantwortliche in Unternehmen zudem beim Schutz mobiler Endgeräte: einerseits unmittelbar, durch Installation entsprechender Software, die gegen Datenverluste, die immer häufiger Folge einer mobilen Web-Anwendung sind; andererseits durch umfangreichen Schutz bei mobiler Client-Server-Einwahl über Firewalls, Verschlüsselung der Übertragungswege über VPN oder Extranet-Zugänge und andere Varianten.

Der dritte große Trend sind „Managed Security Services“, also die Auslagerung von IT-Schutz-Dienstleistungen an professionelle Anbieter.