Special Innovation

Der Sicherheit auf der Spur

Unternehmen bemerken Lücken in ihrer IT-Security erst dann, wenn etwas passiert ist. Um solche Worst-Case-Szenarien gar nicht erst aufkommen zu lassen, empfiehlt es sich, Experten zurate zu ziehen und unternehmenseigene IT-Systeme auf Sicherheitslücken überprüfen zu lassen.

Manfred Lechner

Das Sicherheitsthema wird von großen Firmen anders gehandhabt als von Klein- und mittleren Unternehmen. Wie aus einer Studie von Pricewaterhouse Coopers hervorgeht, stocken große Unternehmen ihre Sicherheitsbudgets auf, während der Mittelstand notwendige Investitionen derzeit eher nur im beschränkten Ausmaß tätigt.

Maßnahmen, die zu setzen sind, können nie endgültige Lösungen darstellen, da Sicherheitssysteme an die ständig wechselnden Bedrohungsszenarien angepasst werden müssen. „IT-Sicherheit wird immer noch oft als ausschließlich technische Disziplin verstanden und Fragen der Awareness zu wenig berücksichtigt“, erklärt Dalibor Galic, Consultant von Alcatel Enterprise Solutions.

Unternehmen haben in den vergangenen Jahren ein erhöhtes IT-Sicherheitsbewusstsein entwickelt, Defizite bestehen aber noch bei Maßnahmen, die die innere Sicherheit betreffen. Foto: Bilderbox.com

Innere Sicherheit

Festzustellen ist, dass das Sicherheitsbewusstsein in Unternehmen im Vergleich zu den vergangenen Jahren gewachsen ist. Zu den Vorreitern hoher und höchster Sicherheitsstandards zählen Banken und Versicherungen, die Telekombranche und Medienunternehmen, die einen 24-Stunden-Betrieb aufweisen. Optimierungsbedarf sieht Galic in Branchen der Old Economy, die ihre IT-Systeme hauptsächlich zur Abbildung der eigenen Geschäftsprozesse einsetzen. Firewall und Spam-Filter zählen mittlerweile bei allen Unternehmen, unabhängig von ihrer Größe, zur Standardausrüstung in Sachen Sicherheit. Galic: „Mitarbeiter von unerwünschten Spams zu entlasten, erhöht auf jeden Fall deren Produktivität.“ Hinzuweisen ist, dass unterschiedliche Institutionen wie das FBI oder die Gartner Group immer wieder darauf aufmerksam machen, dass die meisten Angriffe auf IT-Systeme intern, nämlich von Mitarbeitern verursacht werden. Dies muss nicht immer mutwillig sein, sondern kann auch aus Unachtsamkeit geschehen. Beispielsweise dann, wenn ein Außendienstmitarbeiter gefährliche Software aus dem Netz auf sein Notebook downgeloadet hat und sich später im Unternehmen in das Firmennetzwerk einklickt. „So verursachte Störungen beruhen in der Regel auf der nach wie vor weit verbreiteten Unwissenheit von Usern“, erklärt Galic.

IDS (Intrusion Detection System) und IPS (Intrusion Prevention System) sind in der Lage, diese Gefährdungspotenziale zu managen und Netzwerke frei von störenden Einflüssen zu halten. Vorteil einer solchen Lösung ist, dass mittels Rund-um-die-Uhr-Betrieb die Überwachung von Netzwerken gewährleistet ist, definierte Gegenmaßnahmen sofort ergriffen und Einbruchsversuche zur Beweiserbringung archiviert werden können. „Festzustellen ist, dass Unternehmen bisher nur in geringem Ausmaß bereit sind, Mittel für die Implementierung von IDS oder IPS bereitzustellen, nach wie vor werden als größte Gefahrenquellen Angriffe von außen betrachtet“, so Galic. Wobei es eine Anforderung der Zukunft sein wird, IDS und IPS nicht mehr im Netzwerk zu positionieren, sondern direkt am Endgerät. Aufgrund der zunehmend multimedialen Verwendung der IT-Infrastruktur wie Voice over IP oder Sticks wird umfassender Schutz in Zukunft noch wichtiger werden, ist Consultant Galic überzeugt.

Was den Einsatz von Wireless Lan betrifft, herrscht in Unternehmen nach wie vor große Skepsis. „Dies ist vorrangig auf die mittlerweile gelösten Sicherheitsprobleme zurückzuführen“, so Galic. Alcatel Enterprise Solutions zählt zu den Vorreitern im Bereich Wireless-Lan-Sicherheit, und mittlerweile sind Systeme verfügbar, die sicherer als verdrahtete Netzwerklösungen sind.

Rasch erweiterbar

„Weiterer Vorteil von Wireless Lan ist, dass Netzwerke bei Unternehmenswachstum ohne großen Aufwand erweiterbar ist.“ Was die Erhöhung der Mitarbeiter-Produktivität betrifft, erweisen sich drahtlose Netzwerke ebenfalls als überlegen. Mitarbeiter finden auch an unterschiedlichen Unternehmensstandorten auf ihrem Desktop die vertraute Umgebung vor. Zudem können Besucher mit einem zeitlich und auch, was die Zugriffsrechte betrifft, limitierten Account ausgestattet werden. Gerade in diesem Punkt sieht Golic Wireless Lan als vorteilhaft, denn limitierte Zugänge und Zugriffsrechte lassen sich bei Wireless Lan eindeutig zuordnen, während bei den meisten verdrahteten Netzwerken solche Sicherheitsvorkehrungen nicht implementiert, beziehungsweise aufwendiger durchzuführen sind. „Langsam scheinen die Vorteile mehr in das Bewusstsein zu treten“, so Galic, „da wir vermehrte Nachfrage nach diesen Lösungen feststellen können.“