Sicherheitsrisiko DSL

Die schnellen Internet-Verbindungen sind praktisch und preiswert. Kaum ein Unternehmer aber weiß, wie gefährlich sie für seine Firma sind.

Früher hatten es Hacker schwer: Nur wenige Unternehmen waren per kostspieliger Standleitung rund um die Uhr mit dem Internet verbunden. Die meisten Firmen wählten sie sich jeweils nur kurz ins Netz ein. Dann luden sie schnell Mails herunter. Oder die Angestellten riefen ein paar Web-Seiten auf. Dann wurde die Verbindung wieder gekappt. »Das war meist zu kurz, um Schwachstellen auszuloten und Firmenrechner zu knacken«, sagt Martin Junker, IT-Sicherheitsfachmann aus Wuppertal.

Diese Zeiten sind vorbei. Die meisten Firmen sind heute dauerhaft online. Seitdem schnelle DSL-Leitungen für jedes Unternehmen erschwinglich und Internet-Pausschaltarife, so genannte Flatrates, verfügbar sind, gibt es für die Firmen keinen Grund mehr, die Datenleitung zu unterbrechen. Eine Studie des Marktforschungsunternehmens TNS Emnid belegt, dass Besitzer eines DSL-Anschlusses rund 60 Prozent länger online sind als andere Websurfer. »Das gibt Hackern wesentlich mehr Zeit, Angriffe vorzubereiten und auszuführen«, bestätigt Security-Experte Junker.

Günstige Gegenmaßnahmen

Dieses Risiko unterschätzt mancher Firmenchef. Motto: Was gibt es bei uns schon zu holen. »Das ist irrelevant«, entgegnen IT-Sicherheitsexperten. Die Erfahrung zeigt vielmehr, dass Computerkriminelle versuchen, in jedes erreichbare Rechnernetz einzudringen. Die möglichen Schäden reichen vom Ausspionieren übers Verändern bis zum Löschen von Daten. »Besonders in kleinen Firmen klaffen große Sicherheitslücken«, warnt Jürgen Sponnagel, Vorstandschef der Mummert Unternehmensberatung in Hamburg. Das Problem aus seiner Sicht: »Häufig gibt es niemanden mit dem nötigen Know-how in der Firma.« Oder es hapert schlicht an der Organisation. »Kein Angestellter hat jemals die Verantwortung für diesen wichtigen Bereich übertragen bekommen«, sagt Sponnagel.

An einfachen und günstigen Gegenmaßnahmen mangelt es indes nicht. Die Palette reicht von kostenlosen Programmen, die den gesamten Datenstrom aus dem Internet checken bis zu spezieller Hardware, die keinen Hacker passieren lassen. Sie decken jeden Einbruchsversuch auf und schlagen sofort Alarm. Wichtig: Vor der Anschaffung der Sicherheitsausstattung empfehlen Experten, ein individuelles Security-Konzept fürs Unternehmen aufzustellen (siehe »Die wichtigsten Schutzmaßnahmen«).

Kostenlose Unterstützung bieten Institutionen wie das Bundesamt für Sicherheit in der Informationstechnik (BSI). Unter www.bsi.de finden Firmenchefs Leitfäden zur sicheren IT als Download. Ist die eigene EDV-Abteilung mit der Umsetzung derartiger Konzepte überfordert, helfen Dienstleister weiter. Doch Vorsicht: »Mittlerweile ist Sicherheit ein Werbeschlagwort geworden, das sich viele einfach auf die Fahnen schreiben«, warnt Jochen Bauer, Geschäftsführer der Inside Security IT Consulting GmbH. Er empfiehlt Chefs, den Dienstleister und seine Expertise beispielsweise über Referenzen zu überprüfen.

Dass ordentliche Sicherheitsmaßnahmen nicht überflüssig sind zeigt eine Studie der US-Sicherheitsfirma Symantec. Das Unternehmen aus dem kalifornischen Cupertino hat dafür die Alarmprotokolle von 400 ihrer Kunden auf Hackerangriffe ausgewertet. Mit beängstigendem Ergebnis: Jede Firma wurde im Durchschnitt 30-mal pro Woche von außen attackiert.

Wie die ungeheure Vielzahl der Angriffe zustande kommt, erläutert Patrick Heinen, Sicherheitstechniker bei Symantec: »Die meisten Angriffe gehen auf das Konto von automatisierten Computerprogrammen, die ein Hacker irgendwann gestartet hat und die dann im Internet kontinuierlich Rechner absuchen und direkt attackieren.« Der Hacker selbst wartet in aller Ruhe ab, bis ihm sein digitales Vorauskommando ein lohnendes Ziel für einen Computereinbruch auf dem Präsentierteller serviert.

Mit DSL kommen die Gauner

Gerade Deutschland ist auf dem besten Weg, sich in ein regelrechtes Hacker-Paradies zu verwandeln. Ende 2002 zählte das Marktforschungsunternehmen IDC rund 681000 DSL-Anschlüsse in deutschen Unternehmen. Das bedeutet, dass fast jedes fünfte Unternehmen so ans Internet angeschlossen ist. Mit stark steigender Tendenz: »Innerhalb der nächsten vier Jahre wird sich der Markt für DSL-Anschlüsse fast verfünffachen«, prognostiziert Jan Hein Bakkers, Senior Research Analyst bei IDC.

Wie sich ein solcher Boom auf die Aktivitäten der Datendiebe auswirkt, zeigt Südkorea. Dort sind jetzt rund 58 Prozent der Benutzer per DSL online. Und die Zahl der Hackerangriffe explodiert: Innerhalb weniger Monate registrierten Experten einen Anstieg um satte 62 Prozent. ●

Achim Wagenknecht *ressort.atprofit@impulse.de*

So helfen Dienstleister

Vom Konzept bis zur Umsetzung: Das Portfolio der IT-Security-Experten.

Beratung
IT-Sicherheit erfordert viel Know-how und kann schnell teuer werden. Berater helfen, Sicherheitsbedürfnis und Budget aufeinander abzustimmen. Sie erarbeiten ein zum Unternehmen passendes Konzept.

Managed Firewalls
Firewall-Systeme protokollieren jeden Einbruchsversuch. Per Fernwartungszugang werten IT-Dienstleister diese Aufzeichnungen aus, um die Sicherheit des Systems zu verbessern. Ebenso halten sie die Sicherheitssoftware stets auf dem neuesten Stand.

Sicherheitstest
Manche IT-Security-Experten bieten Einbruchsversuche an, um die Maßnahmen des Unternehmens zu prüfen. Gefundene Lücken helfen, das Sicherheitskonzept zu verfeinern.

Illustration: Xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Ihre wichtigsten Schutzmaßnahmen

Jedes Unternehmen, dass regelmäßig via DSL online ist, gerät ins Fadenkreuz der Computerkriminellen. Wie Sie am besten gegenhalten.

Firewall einrichten
Diese Maßnahme sperrt potenzielle Hacker aus: Ein spezieller Computer dient als Schutzzaun zwischen DSL-Zugang und Firmennetz. Günstiges Modell: Trendmicro Gatelock (www.gatelock.de). Die kostenlose Software IPCop (www.ipcop.org) verwandelt einen einfachen PC in eine Firewall. Dafür ist aber etwas Know-how nötig. Mehr unter: www.impulse.de/specials/cebit/sicherheit/184314.html.

Antiviren-Software installieren
Hacker nutzen Computerviren als Vehikel, um Daten zu sabotieren oder auszuspionieren. Davor schützt in kleinen Netzen G-Datas AntiVirenKit (www.gdata.de). Größere PC-Netze lassen sich mit E-Trust Antivirus absichern (www.ca.com/germany).

Updates durchführen
Für ihre Einbruchsversuche nutzen Hacker gern Software-Fehler aus. Daher sollten Chefs Programme immer auf dem neuesten Stand halten. Manchmal lässt sich eine automatische Update-Funktion einschalten, vor allem in Windows und im Antivirusprogramm.

Sicherheitsrichtlinie festlegen
Eine gründliche Analyse ist Pflicht: Wo liegen empfindliche Daten im Unternehmen, wer hat darauf Zugriff. Riskante Anwendungen wie beispielsweise Instant Messaging gehören verboten. Ebenso die private Nutzung des Internet, um die Virengefahr zu senken.