Alles sicher?

Neue Attacken, bessere Abwehr: Wie Unternehmer Hard- und Software jetzt vor Hackern und Viren schützen.

Niemand bei der Essener Thiesbürger GmbH bemerkte den Einbruch. Und auch die Mitarbeiter des Lübecker Leitern- und Gerüsthändlers Rieckermann & Sohn, der Cooper European Aircraft Parts GmbH in Kassel oder der Kieler Firma BWB entdeckten den ungebetenen Besuch auf ihren Webservern nur zufällig. Ein Hacker hatte die Maschinen gekapert – und sein Markenzeichen auf den Festplatten hinterlassen: »Status-x was here«.

Problemlos hätte der Computerkriminelle auch Preislisten und Produktinformationen fälschen können. Oder den Webserver als Speicher für Pornobilder, Videos oder Musikstücke missbrauchen. Durch immer raffiniertere Methoden, unerkannte Sicherheitslücken oder fehlende Schutzmechanismen haben Computerschädlinge und Datendiebe besonders bei kleinen und mittleren Firmen leichtes Spiel. Daher bildet die IT-Sicherheit einen wichtigen Schwerpunkt der Computermesse Cebit. Vornehmlich in Halle 7 finden Firmenchefs Produkte und Anregungen, um ihre Rechner optimal zu schützen. Denn: »Bedrohungspotenzial und Anzahl der Attacken werden 2005 noch stärker als bisher ansteigen«, prognostiziert Udo Helmbrecht, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Damit Firmen leichter und schneller gegenhalten können, haben Anbieter von Sicherheitstechnik neue Hard- und Software entwickelt, die einfacher zu bedienen ist. Besonderes Augenmerk liegt auf dem Security-Management innerhalb des Netzwerks. »Ein wichtiges Thema werden Lösungen sein, die ein Netzwerk automatisch auf Sicherheitslücken, fehlende Updates und weitere sicherheitsrelevante Merkmale hin untersuchen können«, verspricht Toralv Dirro, Sicherheitsexperte beim Antiviren-Hersteller McAfee. Derartige Technologien erkennen Attacken, falls sich ein Hacker an der Firewall vorbeigemogelt hat und sich nun im Computernetz der Firma umsieht.

Denn Angreifer begnügen sich unter Umständen nicht damit, den Webserver zu missbrauchen. Größere Gefahr droht, wenn Shopsysteme oder interaktive Datenbanken mit Kundeninformationen auf der Firmenhomepage eingebunden sind. Denn von dort bestehen häufig direkte Verbindungen zur Warenwirtschaft oder Lohnbuchhaltung im Unternehmen – ein gefundenes Fressen für Computerganoven. »Simple Programmierfehler machen solche Webanwendungen zum beliebten Ziel für Hacker«, sagt Olaf Lindner, Director Security Services bei Symantec, dem Marktführer für IT-Sicherheit. Selbst Standardprogramme von renommierten Herstellern wie SAP oder Sage sind davor nicht gefeit.

Computer gekapert

Wer seinen Mitarbeitern dennoch den Zugriff von außen via Internet auf Rechner und Programme in der Firma gestatten muss, sollte die Kommunikation besonders schützen. Hersteller wie etwa Nortel (siehe »Weitere Infos«) vertreiben solche Geräte: Mit Hilfe einer Verschlüsselungstechnik, die bislang kein Hacker knacken konnte, verhindern sie den externen Zugriff durch Datenlauscher.

Indes glauben immer noch zu viele Firmenchefs: »Bei uns gibt es nichts zu holen.« Doch sie irren gewaltig. Denn heute hacken Computerganoven sich meist nicht mehr mit viel Geduld in ein einzelnes fremdes Rechnersystem. Sie schreiben Programme,

die das Internet automatisch und wahllos nach Sicherheitslücken durchforsten. Werden diese fündig, nisten sie sich im PC ein. Dagegen helfen Firewall und Antiviren-Software.

Weitere Gründe, warum Chefs besser auf ihre IT aufpassen müssen: Maßnahmen zur IT-Sicherheit fließen jetzt auch in Kredit-Ratings (Basel II) ein. Und wer allzu sorglos ist, kann sogar mit dem Gesetz in Konflikt geraten – etwa dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG): »Führen Nachlässigkeiten im Umgang mit der IT-Sicherheit zu einer Unternehmenskrise, haftet der Chef«, sagt Andreas Mertz, Geschäftsführer des Münchner Systemhauses IT-Cube. Nur wer Maßnahmen zur Risikofrüherkennung und Gefahrenabwehr vorweisen kann, entgeht dieser juristischen Falle (siehe »Ihre Grundausstattung«).

Neuester Clou der Computerkriminellen sind »Bot-Netze« (von englisch »robot«): ein Geflecht aus tausenden geknackter PCs, die von einem Hacker ferngesteuert werden können. Die Besitzer dieser Rechner merken gar nicht, dass ihre Computer für kriminelle Zwecke missbraucht werden. Beispielsweise für den Versand unerwünschter Werbe-Mails (»Spam«). Wer seine Rechner mit einer aktuellen Firewall sowie Antiviren-Software schützt, ist eigentlich gegen derartige Entführungsversuche gefeit. Dennoch erwarten Experten, dass die Zahl der gekaperten PCs weiter steigen wird. Problem: »Geeignete Gegenmittel sind allesamt verfügbar, werden aber noch nicht immer konsequent genug eingesetzt«, beobachtet BSI-Chef Helmbrecht.

Achim Wagenknecht
ressort.computer@impulse.de

[x] WEITERE INFOS

Ratgeber zur PC-Sicherheit finden Sie unter www.impulse.de/it-security.
Wo entsprechende Anbieter ausstellen, steht unter www.impulse.de/cebit.

Ihre Grundausstattung gegen Hacker, Viren, Würmer und Trojaner

Viele Sicherheitslücken lassen sich schnell und einfach schließen. Andreas Mertz, Geschäftsführer des Münchner Systemhauses IT-Cube, erläutert die wichtigsten Standardmaßnahmen in den Bereichen Technik und Management.

TECHNIK

Back-ups
Alle wichtigen Daten sollten zentral auf dem Server gespeichert und täglich gesichert werden, am besten vollautomatisch. Wichtig: Regelmäßig prüfen, ob die Daten im Ernstfall reproduzierbar sind.

Antiviren-Software
Virenschutz gehört auf jeden Arbeitsplatzrechner und auf jeden Server. Die automatische Aktualisierungsfunktion muss eingeschaltet sein. E-Mail-Anhänge sollten zentral auf Viren gescannt werden.

Firewall
Jede Internetverbindung ist angreifbar. Wirksamen Schutz bieten Firewall-Rechner. Allerdings müssen die Geräte oder Programme regelmäßig aktualisiert werden. Komfortabler sind so genannte Managed Firewall Services, die komplett von einem Dienstleister betreut werden.

Updates
Um neu entdeckte Sicherheitslücken schnell zu schließen, sollten Chefs die automatische Update-Funktion von Windows aktivieren. Noch besser: Spezialsoftware von Foundstone, Qualys oder eEye.

MANAGEMENT

Strategie
IT-Sicherheit ist keine Frage des IT-Budgets. Bei knappen Ressourcen ist es besser, wenige einfache Maßnahmen konsequent umzusetzen, als aufwendige Security-Richtlinien zu entwickeln, die dann nicht realisiert werden können.

Dokumentation
Nur schriftlich fixierte Sicherheitsregeln können verbindlich von den Mitarbeitern eingefordert werden.