Gefahren aus dem Netz

Grundschutz in der Praxis

Ein Ausfall der IT oder ein Befall mit Viren und Würmern verursacht in Unternehmen enorme wirtschaftliche Schäden. Die Sicherheit wird leider oft vernachlässigt, auch wenn es einfachen und wirkungsvollen Schutz gibt. VON INGO STEINHAUS

Im Frühjahr befiel ein weltweit grassierender Computerwurm Millionen Rechner von Unternehmen und Behörden. Das als „Conficker" bezeichnete Schadprogramm springt in einem ungeschützten Netzwerk relativ ungehindert von einem System zum anderen und verbreitet sich rasch weiter. Die befallenen Computer lassen sich dann via Internet für illegale Aktionen wie den Versand von unerwünschter Werbung („Spam") missbrauchen – für das betroffene Unternehmen ein riesiger Imageschaden und eine teure Angelegenheit. Das russische Sicherheitsunternehmen Kaspersky hat die weltweiten Verluste durch Internet-Kriminalität vor einiger Zeit auf 100 Milliarden Dollar pro Jahr beziffert.

Die Lösung zur Vermeidung solcher Schäden lautet ganz schlicht: Nutzen Sie die aktuellen Standards zur IT-Sicherheit. Doch leider ist die Einarbeitung in das Thema schwer. Ein Beispiel: Der „Kompass der IT-Sicherheitsstandards" soll Unternehmern mehr Übersicht geben. Auf gut 50 Seiten beschreiben darin der IT-Branchenverband Bitkom und das Deutsche Institut für Normung (DIN) die annähernd 50 technischen Standards zur IT-Sicherheit. Was dort in Stichworten zusammengefasst wird, schreckt durch stark technische Formulierungen eher ab, als dass es zur Sicherheit ermuntert. „Brauchen wir das eigentlich alles?", fragt sich jeder, der in dieser Broschüre blättert. Leider ja, lautet die Antwort, denn nach einer Studie des Bundeswirtschaftsministeriums haben 80 Prozent aller Unternehmen wenigstens einmal pro Jahr schwere IT-Probleme.

Oft sind Fahrlässigkeit oder Unwissen der Mitarbeiter der Grund: „Wenn es keine technischen oder organisatorischen Beschränkungen gibt, passiert auch etwas. Zum Beispiel öffnen Mitarbeiter irgendwelche Dokumente in E-Mails, ohne sich über Gefährdungen im Klaren zu sein", sagt IT-Sicherheitsexperte Reiner Kraft vom Fraunhofer Institut für Sichere Informationstechnologie in Darmstadt. Er empfiehlt trotz der anfänglichen Lernhürde die Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI). Sie bieten eine umfassende Beispielkonzeption für IT-Sicherheit, die eigentlich nur noch angewendet werden muss. Mit deutscher Gründlichkeit geht es dem BSI dabei um „die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen", so die Autoren in der Einleitung zu dem mehr als 4.000 Seiten umfassenden Werk.

Grundlegender Schutz ist einfach

„Die Unternehmer starren erschreckt auf diesen Wust an Informationen", meint Reiner Kraft. Auf Maßnahmen zur IT-Sicherheit solle aber kein Unternehmen verzichten, betont der Informatiker. „Oft bewirken bereits sehr einfache Maßnahmen eine höhere Sicherheit." (Siehe Kasten „Basisschutz mit Firewall und Virenscanner", Seite 62.) Doch in vielen Fällen bieten Virenscanner und Firewall nicht genug Sicherheit. Dies gilt zum Beispiel bei der Nutzung eines komfortablen WLAN-Funknetzes oder beim Aufbau eines Fernzugriffs, mit dem der Geschäftsführer von seinem Heim aus Firmendaten nutzen kann.

Auch wer weitergehenden Rat für solche Anwendungsbereiche sucht, wird beim BSI kostenlos fündig. Unter anderem bietet die Behörde den „Leitfaden für IT-Sicherheit" an, der einen fundierten Überblick über die Knackpunkte bei der Abschirmung von Computern enthält. Weitere praktische Ratschläge für kleinere Unternehmen, wie zum Beispiel Arztpraxen, Rechtsanwaltskanz-

INTERNET-LINKS

www.bitkom.org
Kompass der IT-Sicherheitsstandards

www.bsi.de
Leitfaden IT-Sicherheit, Grundschutzprofil für eine kleine Institution und BSI-Standard zum Notfallmanagement

Foto: Manuel Lesch/pantheremedia.net

leien, Steuerberaterbüros, Handwerksbetriebe, Reisebüros oder Hotels, gibt das „Grundschutzprofil für eine kleine Institution". Es vermeidet die Umständlichkeiten der Grundschutzkataloge und liefert stattdessen Anleitungen für Sofortmaßnahmen.

Kostengünstige Angebote für KMU

Trotzdem bleibt immer noch ein Problem übrig, das wirkungsvolle IT-Sicherheit verhindert: die Kosten für die notwendige Software und Hardware, die vor allem Selbstständige und kleinere Unternehmen zu schlechten Kompromissen verführen. Eine recht günstige und unkomplizierte Lösung sind spezielle Software-Pakete für Unternehmen. Sie werden von verschiedenen Herstellern wie McAfee, Symantec oder Trendmicro vermarktet und kosten für fünf Arbeitsplätze ab etwa 300 Euro pro Jahr. Solche Pakete sind ideal für kleine Unternehmen ab fünf Nutzern, die sich umfassend schützen und gleichzeitig den Aufwand für die Verwaltung ➤

WIRKSAMER SCHUTZ

Die Top 10 der Sicherheitsregeln

1. Schützen Sie Rechner und Anwendungen mit Kennwörtern. Ein sicheres Kennwort ist eine zufällige Abfolge von mindestens acht Ziffern und Buchstaben. Es kann über eine Eselsbrücke ermittelt werden. Zum Beispiel ergeben die ersten Buchstaben aus „Nützliche Kennwörter sind 15 Zeichen & Ziffern lang" das ziemlich sichere Kennwort „NKs15Z&Zl".

2. Beschränken Sie Datenzugriffe auf ein Mindestmaß. Jeder Benutzer (und auch jeder Administrator) sollte nur auf die Daten und Programme zugreifen dürfen, die er für seine tägliche Arbeit wirklich benötigt.

3. Beschränken Sie auch die Administratorrechte – Admins sollten nur Zugriff auf Ressourcen haben, für die sie zuständig sind.

4. Verbergen Sie jeden PC mit Internet-Zugriff hinter einer Firewall – entweder eine Personal Firewall am Arbeitsplatz oder eine zentrale Firewall in einem Netzwerk-/DSL-Router.

5. Schirmen Sie alle Rechner mit Antivirenprogrammen ab. Internet-Daten (Web, Mail) sollten zentral über einen Server geleitet und dort geprüft werden. Aktualisieren Sie die Virendatenbanken täglich, am besten häufiger!

6. Installieren Sie Sicherheitsaktualisierungen sofort, vor allem für Betriebssysteme, Browser, E-Mail-Programme und Office-Anwendungen.

7. Sichern Sie alle wichtigen Daten regelmäßig. Prüfen Sie außerdem, ob die Sicherungskopien funktionsfähig sind.

8. Schützen Sie alle IT-Systeme gegen Überhitzung, Feuer, Wasserschäden, Stromausfall und Diebstahl.

9. Schulen Sie Ihre Mitarbeiter regelmäßig. Viele Sicherheitsprobleme entstehen aus Unkenntnis oder mangelndem Problembewusstsein.

10. Prüfen Sie die IT-Sicherheit: Werden Kennwörter gewechselt? Werden die Sicherheitseinstellungen nicht geändert? Sind nur zulässige Anwendungen installiert?

Leider noch keine Wirklichkeit: Der Schutzknopf gegen Trojanerbefall auf der Tastatur.

der Software gering halten wollen. Integrierte Hilfsfunktionen und vereinfachte Bedienoberfläche sollen den Betrieb der Sicherheitspakete ohne umfangreiches Fachwissen ermöglichen.
Trotzdem wird der Einsatz solcher Paketlösungen für viele Anwender noch zu umständlich sein. Selbst die einfachste Software-Lösung muss korrekt installiert und betrieben werden, damit echte Sicherheit die Folge ist. Eine sinnvolle und erschwingliche Komplettlösung ist „Sicherheit zum Mieten", wie sie zum Beispiel die Kölner Druckerei Moeker Merkur nutzt. Eine kleine Box am zentralen Telefonanschluss ist die Schnittstelle zum Internet. Sie reicht automatisch sämtliche Internet-Verbindungen in beiden Richtungen an einen Dienstleister für Internet-Sicherheit weiter. Dort werden die Daten nach höchsten Standards geprüft und dann erst an die Druckerei und – bei ausgehender E-Mail – an ihre Kunden geschickt.

Sicherheit gibt es auch zur Miete

Im IT-Jargon heißt so etwas „Managed Security Services". Über mehrstufige Firewalls blockiert der Dienstleister Angriffe auf die Rechner seiner Kunden, aktualisiert die Virenscanner im halbstündlichen Rhythmus und sichert die Dokumente. Dabei wird eine abgesicherte und verschlüsselte Internet-Verbindung eingesetzt. „Die Übertragungsgeschwindigkeit leidet dabei nicht unter dem Umweg über den IT-Dienstleister", berichtet Friedhelm Spohr, einer der Geschäftsführer der Druckerei. Diese externe Sicherheitsleistung kostet eine monatliche Mietgebühr, die je nach Art der eingesetzten Sicherheitsbausteine und der Anzahl der Arbeitsplätze berechnet wird. Für die Druckerei fallen Kosten von etwa 1.000 Euro im Jahr an. Im Gegenzug muss sich kein Mitarbeiter um Aktualisierungen und neue Sicherheitstechniken kümmern, der Dienstleister liefert immer „State of the Art". Für Friedhelm Spohr ist das die perfekte Lösung: „Umfassende IT-Sicherheit ohne große Investition."

Für Notfälle vorsorgen

Doch ein wirkungsvoller Schutz der Firmendaten ist mehr als nur Schutz der IT, denn was ist, wenn die Computer wegen eines Notfalls nicht mehr arbeiten? „Dabei muss ein Notfall nicht einmal durch eine Naturkatastrophe ausgelöst werden, der Fund einer alten Fliegerbombe oder die plötzliche Pleite eines Lieferanten reicht aus", sagt Matthias Hämmerle, IT-Manager beim Beratungsunternehmen KPMG in Frankfurt. Er betreibt unter www.bcm-news.de einen Blog zu „Business-Continuity-Management". Unter diesem Stichwort, das oft auch unter der Abkürzung BCM erscheint, werden Strategien zur Erhaltung des Geschäftsbetriebs in Katastrophenfällen zusammengefasst.

Matthias Hämmerle, IT-Manager bei KPMG, beobachtet bei Unternehmenskunden eine starke Nachfrage nach IT-Risikoschutz.

Foto: privat

Darunter fallen Vorkehrungen wie ein Dieselaggregat als unterbrechungsfreie Stromversorgung, aber auch brandgeschützte Schränke für Computer mit wichtigen Firmendaten. Ebenso wichtig ist ein Plan, wo und von welchem Geld in einem extremen Notfall neue Computer besorgt werden. „Viele Unternehmen verlangen inzwischen von ihren Kunden den Nachweis dieser Notfallvorsorge, um fatale Verluste auszuschließen", sagt Matthias Hämmerle. „Auch Banken achten mittlerweile bei der Bonitätsprüfung im Kreditgeschäft verstärkt auf die Risikovorsorge." Eine gute Notfallplanung schlägt sich dann schnell in günstigeren Kreditbedingungen nieder.
Es gibt inzwischen sogar eine Art Standard dafür: Im Februar 2009 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Norm „BSI 100-4 Notfallmanagement" veröffentlicht. Sie ist in Buchform im Handel und als E-Book auf der Webseite des BSI (www.bsi.de) erhältlich. Die Publikation bietet praxisnahe und wie in einem Baukastensystem umsetzbare Maßnahmen für kleine und mittelgroße Unternehmen. Matthias Hämmerle: „Damit können Mittelständler sehr leicht eine Vorsorge treffen, und zwar für die geschäftskritischen Aktivitäten und Ressourcen (zum Beispiel Mitarbeiter, Gebäude, Dokumente) wie auch für die wichtigen Dienstleister und Lieferanten."

BASISSCHUTZ MIT FIREWALL UND VIRENSCANNER

Firewall heißt „Brandschutzmauer" und bezeichnet eine Software, mit der ein LAN vor unerlaubten Zugriffen aus dem Internet geschützt wird. Normalerweise ist sie auf einem Netzwerkgerät direkt am Internet-Anschluss (etwa ein DSL-Router) installiert. Zusätzlichen Schutz bringt eine **Personal Firewall** auf jedem PC. Sie überwacht alle ein- und ausgehenden Datenpakete auf diesem Rechner und erlaubt nur bestimmten Anwendungen den Zugriff auf das Internet.

Ein **Virenscanner** ist ein Programm, das die Daten des Rechners anhand einer Datenbank mit sogenannten „Virussignaturen" überprüft und Schadprogramme unschädlich macht. Doch ein Virenscanner funktioniert nur so gut, wie seine Virendatenbank aktuell ist. Diese Datenbank enthält die sogenannten Virussignaturen, anhand derer der Virenscanner die Schadprogramme identifizieren kann. Virenscanner nutzen meist eine automatische Aktualisierung, die unter keinen Umständen ausgeschaltet werden sollte.