



NETFOX

IT-Sicherheit

Viren, Hacker und der Faktor Zufall

IT-Sicherheit – damit Ihr Unternehmen arbeitsfähig bleibt

Mehr als die Hälfte der Unternehmen in Deutschland sind bereits Opfer von Virenangriffen geworden. Nach einer Statistik der Koordinationszentrale der amerikanischen Computer Emergency Report Teams (CERT) hat sich die Zahl der erfassten Attacken im Internet seit 1998 jährlich verdoppelt. IT-Sicherheit ist daher ein vielzitiertes Thema – es steckt jedoch im Detail mehr dahinter, als vielen Unternehmen bewusst ist.

Die Gefahr lauert im Innern

Was viele Unternehmer nicht wissen: Die Mehrzahl der Störfälle wird durch die eigenen Mitarbeiter oft unbewusst und z.T. auch bewusst verursacht. Der Ursprung liegt in der Regel in der geringen Sensibilisierung der Mitarbeiter gegenüber der hausinternen IT-Sicherheit. Untersuchungen bei deutschen Unternehmen belegen, dass 80 % aller Angriffe auf die IT-Sicherheit von innen kommen. Eine Schulung des Personals zum verantwortungsvollen Umgang kann hier bereits Abhilfe schaffen.

System- und Netzausfälle oder unumkehrbare Datenverluste können zu existenziellen Schäden führen. Umso beunruhigender ist es, dass die Verletzlichkeit digitaler Informationen immer häufiger an die Oberfläche tritt. Ist die eine Sicherheitslücke geschlossen, tauchen an anderer Stelle zwei neue Probleme auf. Hinzu kommt, dass jede Saison ihre eigene digitale Plage mit sich bringt, die sich in Form von neuen Viren und Würmern über das Internet verbreitet.

Der Zufallsfaktor entscheidet

Viele Angriffe von außen sind nicht einmal zielgerichtet. Eine bestimmte Art von Hackern (Script Kiddies) ist einzig darauf aus, Systemschwächen auszumachen, um sie dann destruktiv auszunutzen. Unternehmen täuschen sich, wenn Sie glauben, von Hackerangriffen verschont zu bleiben, weil diese sich nicht für ihre Daten interessieren. Hacker suchen vielmehr nach Sicherheitslücken und gehen dabei meist nach dem Zufallsprinzip vor.

Je weiter das Feld der potenziellen Gefährdungen für Netze und Systeme ist, desto dringlicher ist die Aufgabe des modernen Managements, flexibel auf die Herausforderungen zur Verwirklichung von IT-Sicherheit zu reagieren. Dabei sind auch rechtliche Aspekte zu berücksichtigen. So existiert bereits seit 1998 ein Gesetz (KonTraG), in dem der Gesetzgeber die Etablierung eines Risiko-Management-Systems vorschreibt.

Schneller als jedes Risiko

Kundenorientierte Lösungen für wirksame Sicherheit

Jedes Unternehmen hat individuelle Bedürfnisse. Das gilt auch in Bezug auf wirksame Sicherheitskonzepte. Um hinreichende Sicherheit zu gewährleisten, muss das Gefährdungspotenzial zuerst individuell abgeschätzt werden. Erst dann ist es möglich, geeignete Maßnahmen einzuleiten.

So unentbehrlich IT-Sicherheit auch geworden ist, der Arbeitsablauf innerhalb eines Unternehmens sollte dadurch nicht beeinträchtigt werden. Schutzmaßnahmen dürfen für den Arbeitsalltag nicht so angelegt sein, dass sie die Effektivität hemmen. Sicherheitskonzepte als „Out of the box“-Lösungen sind daher weniger effektiv.

Weniger ist mehr

Weitaus sinnvoller ist es, wenn die Konzepte exakt auf das Sicherheitsbedürfnis zugeschnitten sind, d.h. wenige Schritte konsequent durchzuführen und dafür einige Lücken bewusst in Kauf zu nehmen. Und komplexe Lösungen, die eine ohnehin nicht erreichbare absolute Sicherheit anstreben, werden auch oftmals nur halbherzig genutzt.

Potenzielle Gefahren für die IT-Sicherheit sind nicht statisch. Lösungen sollten es ebensowenig sein. Dann ist es möglich, eine Sicherheitspolitik zu gestalten, die dem Unternehmen Schritt für Schritt und mit wirtschaftlich vertretbarem Aufwand zu mehr Sicherheit verhilft.

Gefahren sind nicht
statisch. Unsere
Lösungen können gut
damit leben –
und Sie mit unseren
Lösungen.

Damit Persönliches sicher bleibt

IT-Sicherheit bedeutet auch den Schutz sensibler Daten. Aus diesem Grund sind Unternehmen, die mit vertraulichen Kundendaten arbeiten, besonders daran interessiert, ihre Daten gegen Angriffe und Spionage zu schützen.

Das IT-Grundschutzhandbuch, dem vor allem Behörden verpflichtet sind, liefert hier wichtige Hinweise zur Gewährleistung des Datenschutzes.

Erkennen Sie Ihre Feinde



Jeden Tag werden
Millionen Computer
von sogenannten
„Sniffer“ Programmen
unbemerkt gescannt.

Mit NETFOX zu mehr Sicherheit

Entscheidend sind Lösungen, die individuell auf die Bedürfnisse des Unternehmens zugeschnitten sind. NETFOX hat das Problem schon länger erkannt und setzt darauf, kundenorientierte Konzepte in enger Zusammenarbeit mit dem Unternehmen zu entwickeln. Die Fachleute von NETFOX stehen Ihnen in folgenden Bereichen zur Verfügung:

- ▶ Sicherheitsanalysen
- ▶ Beratung bei der Auswahl geeigneter Maßnahmen
- ▶ Realisierung geeigneter technischer Maßnahmen
- ▶ Firewall-Systeme
- ▶ Auditing
- ▶ Schulungen
- ▶ Virenschutz
- ▶ Intrusion-Detection-Systeme
- ▶ Datensicherung
- ▶ Zugriffsschutz
- ▶ Kontinuierliche Überwachung der Systeme mittels Remote Management und Logfile-Auswertung
- ▶ Service durch umfassende Betreuungs- und Wartungsleistungen

NETFOX Aktiengesellschaft

Europarc Dreilinden
Heinrich-Hertz-Straße 1b
14532 Kleinmachnow / Berlin
Tel.: 03 32 03 / 290-600
Fax: 03 32 03 / 290-999
e-Mail: netfox@netfox.de
<http://www.netfox.de>