

Nirgends haben Sicherheitslücken so dramatische Folgen wie im IT-Bereich. Aber das Risiko lässt sich durch geeignete Schutzmaßnahmen verringern – und diese betreffen nicht nur technische Bereiche.



Viren, Trojanische Pferde und andere unerwünschte Besucher

Im Herbst 2008 wurde bekannt, dass im Jahr 2006 T-Mobile Datensätze von rund 17 Millionen Mobilfunkkunden entwendet worden waren. Die gestohlenen Daten umfassten Namen, Anschrift und Mobilnummer der betroffenen Kunden, zum Teil auch Geburtsdaten und E-Mail-Adresse. Telekom-Chef René Obermann sprach von einem „sehr ärgerlichen Vorfall“, Datenschützer von einem „Super-Gau“.

Wielandt Mundt kennt sich aus in Sachen Sicherheit. Er ist Geschäftsführer des Verbandes für Sicherheit in der Wirtschaft Niedersachsen mit Sitz in Hannover. „Nirgends kann ein Unternehmen so schnell komplett

Nirgends kann ein Unternehmen so schnell komplett lahm gelegt werden wie durch einen Angriff auf das IT-System.

Wielandt Mundt

Geschäftsführer des Verbandes für Sicherheit in der Wirtschaft Niedersachsen

lahm gelegt werden wie durch einen Angriff auf das IT-System. Lücken in diesem Bereich können für Betriebe zu einem existenziellen Problem werden“, warnt er. Wenn der Server ausfällt, die Kundendaten verschwunden sind oder Programme abstürzen, stehen alle Räder still – egal ob in einer Bank oder in einem Handwerksbetrieb. Dagegen wirkt sich unbemerkte Werksspionage über ein IT-Netzwerk erst mit Verzögerung aus – ist aber nicht minder bedrohlich.

Nach Angaben des Bundeskriminalamtes sind in Deutschland mehr als 750.000 Rechner mit so genannten Trojanern infiziert. Diese können vertrauliche Daten unbemerkt wei-



Oft wird bei falschem Risikomanagement Geld an den falschen Stellen ausgegeben.

Gernot Beu

Consultant im Bereich IT-Sicherheit
Hönigsberg & Düvel Datentechnik, Wolfsburg

terleiten – oft auf direktem Wege zur Konkurrenz. Auf diesem Wege passiert Ideenklau aus dem Bereich Forschung und Entwicklung genauso schnell und elegant wie das Überspielen kompletter Kundendateien.

IT-Sicherheit ist ein viel diskutiertes Thema. Neue Programme, neue Anwendungen und die zunehmende Nutzung des Internets bringen neue Chancen, aber auch immer neue Risiken in unser tägliches Leben. IT-Sicherheit (IT-Security) bezeichnet eine Vielzahl von Mechanismen. Sensible Daten und Geschäftsvorgänge müssen geschützt werden, eine Beeinträchtigung der Geschäftsprozesse durch Ausfall oder Störung der IT-Systeme nach Möglichkeit ausgeschlossen werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet so genannte IT-Grundschutz-Kataloge an. Das BSI macht es dabei den IT-Entscheidern in Unternehmen mit mehr als 3.000 Seiten Katalog-Umfang allerdings nicht gerade einfach, eine durchgängige Sicherheitsstrategie zu entwickeln. Deshalb empfehlen Experten zur Umsetzung von Sicherheitsmaßnahmen die Inanspruchnahme externer Beratungskompetenz. Gernot Beu, Consultant im Bereich IT-Sicherheit bei der Hönigsberg & Düvel Datentechnik in Wolfsburg, spricht aus Erfahrung: „Oft wird bei falschem Risikomanagement Geld an den falschen Stellen ausgegeben.“ IT-Sicherheitsmaßnahmen müssten aber im direkten Zusammenhang mit einer kompetenten Risikoanalyse umgesetzt werden. „Ein Großbetrieb mit wenig Datenverarbeitung, wie vielleicht eine Großschlachtereier, benötigt ein völlig an-

deres Sicherheitspaket als ein kleines medizinisches Labor mit vergleichsweise erheblichem EDV-Aufwand“, so Beu weiter.

Dabei ist IT-Sicherheit mehr als nur ein technisches Problem, denn gerne wird übersehen: Ein Großteil aller Sicherheitsprobleme ist hausgemacht! Jeder Angestellte kann durch unerlaubten Zugriff auf geschützte Daten, Einschleusen von Schadprogrammen und fahrlässige Bedienfehler zum entscheidenden Sicherheitsrisiko werden – Zyniker sprechen in diesem Zusammenhang vom Mitarbeiter als ‚Datenschleuder‘. Da werden zur Autorisierung für den Zugriff auf Programme oder Datenbanken unsichere Passwörter gewählt, unbekannte E-Mail-Anhänge geöffnet oder bedenkenlos Datenträger an den Büro-PC gestöpselt, die keiner Sicherheitsprüfung standhalten. In einer Befragung des britischen Beratungsunternehmens Deloitte aus dem Jahr 2007 („Global Financial Services Survey 2007“) sahen etwa vier Fünftel aller befragten Unternehmen ihre eigenen Mitarbeiter als Urheber für die Preisgabe sicherheitsrelevanter Daten – sei es durch Irrtümer, Fahrlässigkeit, Fehler oder Vorsatz. ▶

Bereiche der IT-Sicherheit

- Antiviren-Lösungen
- Netzwerke (Firewalls, Notstromversorgung)
- Passwörter für Zugang zu Datenbanken
- Richtlinien zur E-Mail- und Internetnutzung
- Server-Sicherheit (Feuer, Wasser, Spannungsschwankungen usw.)
- Sicherheitskopien
- Sicherung von Kundensowie Forschungs- und Entwicklungs-Daten
- Telekommunikations-Anlagen
- Verschlüsselungs-Software

Anzeige

ENDLICH
kann ich, so oft ich will!

Deutschlands erste Kino-Flatrate ist da!
1-mal zahlen, X-mal ins Kino: ein Jahr lang mit der CinemaxX GoldCard, ein halbes Jahr mit der SilverCard.

Das perfekte Geschenk für Ihre Mitarbeiter!
Weitere Infos und Bestellung: CinemaxX Wolfsburg, Tel.: 0 53 61 / 4 64 97 10 oder Mail: wolfsburg@cinemaxx.de

CINEMAXX
Mehr als Kino

Glossar

Backdoor Schadfunktion, die üblicherweise durch Viren, Würmer oder Trojanische Pferde eingeschleust und installiert wird. Sie ermöglicht Dritten unter Umgehung der Sicherheitseinrichtungen einen unbefugten Zugang (= Hintertür) zum Computer.

Computer-Virus (oft nur Virus) Älteste Art der Schadfunktionen. Nichtselbstständige Programmroutine, mit der Fähigkeit sich selbst in Programme, Dokumente oder Datenträger zu kopieren und andere IT-Systeme oder Netzwerke zu infizieren. In der Regel, um den Betriebsablauf eines IT-Systems zu beeinträchtigen.

Dialer Im Hintergrund und vom Nutzer unbemerkt ablaufendes Einwahlprogramm über Telefonmehrwertdienste ins Internet als Zugang zu besonderen Inhalten, deren Nutzung meist mit hohen Gebühren verbunden ist.

Firewall Die Firewall (Brandmauer) überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht. Auf diese Weise versucht die Firewall, das entsprechende Netzsegment vor unerlaubten Zugriffen zu schützen.

IT (Informationstechnik) Gesamtheit der technischen Mittel zur Erhebung, Erfassung, Aufbereitung, Nutzung, Speicherung, Übermittlung, programmgesteuerten Verarbeitung, internen Darstellung, Ausgabe und Wiedergewinnung von Daten.

KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) Das seit 1998 rechtskräftige Gesetz verpflichtet Aktiengesellschaften zur Durchführung eines angemessenen Risikomanagements, um alle relevanten Schwachstellen, die bedrohlich für ein Unternehmen werden könnten, transparent zu machen. Nach herrschender Meinung gilt das Gesetz auch für große GmbHs.

Phishing Wortschöpfung aus den Wörtern ‚password‘ und ‚fishing‘ die sinngemäß ‚nach Passwörtern fischen‘ bedeutet. Mit gefälschten E-Mails und Webseiten werden Nutzer getäuscht und zur Preisgabe von vertraulichen und sensiblen Daten veranlasst, die dann missbraucht werden können.

Spyware Unerwünschte Programme, die vom Nutzer häufig unbemerkt installiert werden und dessen Verhalten ohne sein Wissen ausspionieren und die gewonnenen Informationen an Dritte (häufig Werbefirmen und Softwarehersteller) weiterleiten.

Trojanisches Pferd/ Trojaner Kombination eines (manchmal nur scheinbar) nützlichen Anwendungsprogramms mit einer versteckt arbeitenden Spyware zum Ausspionieren persönlicher Daten oder der Öffnung einer Backdoor.

Wurm Vollständiges, lauffähiges Programm, das sich selbstständig (ohne Nutzeraktion) vervielfältigen kann und sich in IT-Systemen und vor allem in Netzen ausbreitet. Würmer enthalten häufig Schadfunktionen.

► **Dok.-Nr. 16871**

► **Der Feldversuch** einer Beraterfirma lässt IT-Sicherheitsbeauftragten die Haare zu Berge stehen: Auf dem Firmenparkplatz eines Betriebes wurden wie zufällig hundert infizierte USB-Sticks fallen gelassen. Nur wenige Stunden später konnte über das Netzwerk ihre Nutzung an Firmencomputern nachgewiesen werden – trotz der eindeutigen Vorgabe durch die EDV-Abteilung, auf keinen Fall fremde Datenträger zu verwenden.

Noch nie war es so einfach für Datendiebe, Sicherheitslücken zu missbrauchen. Riesige Datenmengen lassen sich in Sekundenschnelle überspielen. USB-Sticks sind mittlerweile sogar in Uhren und Taschenmessern untergebracht – und auch Foto-Handys mit USB-Schnittstelle und hoher Speicherkapazität eignen sich zum Datenklau.

Mitarbeiter eines Unternehmens müssen zum Thema Datensicherheit aufgeklärt und sensibilisiert werden, denn selbst triviale Vorgänge auf der untersten Sachbearbeiter-Ebene können eine Datenschutz-Katastrophe auslösen. Das bestätigt auch Lutz Hausmann, Technischer Geschäftsführer beim Sicherheitssoftware-Hersteller Securepoint aus Lüneburg: „Gerade kleine und mittlere Unternehmen müssen sich mehr mit dem Thema IT-Sicherheit beschäftigen, damit ihnen nicht das gleiche passiert wie den Großen.“ Für kleine Unternehmen und den Mittelstand empfiehlt Hausmann maßgeschneiderte Komplettlösungen durch Drittanbieter, denn die eigenen EDV-Fachkräfte sind durch das Alltagsgeschäft meist so weit ausgelastet, dass ihnen die Zeit fehlt, sich fortzubilden. Vorkonfigurierte Geräte vereinen verschiedene Sicherheitslösungen auf nur einer Hardware-Plattform. Vorteile: einfache Installation, niedrige Kosten, geringere Komplexität beim Gerätemanagement. Der Software-Experte schlägt drei wesentliche Mechanismen vor,



Gerade kleine und mittlere Unternehmen müssen sich mehr mit dem Thema IT-Sicherheit beschäftigen, damit ihnen nicht das gleiche passiert wie den Großen.

Lutz Hausmann

Technischer Geschäftsführer beim Sicherheitssoftware-Hersteller Securepoint, Lüneburg

um Sicherheitslücken zu schließen: Intelligenter Sicherheits-Software, Aufklärung und automatisierte Eskalationsstufen als Frühwarnsystem.

Abgestufte Sicherheitsmaßnahmen hätten nach Hausmanns Einschätzung auch die spektakuläre und systembedingte Datenpanne bei der Telekom verhindern können. Übrigens: Für den Diebstahl der T-Mobile-Kundendaten übernahm Deutschland-Chef Philipp Humm die Verantwortung und zog Konsequenzen: Am 7. November 2008 trat er von seinem Posten zurück.



VW-Wolfsburg Volkswagen setzt im IT-Kontrollzentrum eine LCD-Monitorwand zur Überwachung und Steuerung seiner weltweiten Datenströme sowie Informations- und Kommunikationssysteme ein.