

Sicherheit von Daten

Informationstechnologie ist heute global, gut ausgeprägt und progressiv. Sicherheit in der Informationstechnik, kurz IT-Sicherheit, ist nicht mehr etwas, das von Unternehmen nur als „nice to have“ eingestuft wird. Wer die Sicherheit seiner Daten nicht mehr garantieren kann, läuft Gefahr sein gesamtes Unternehmen in den Ruin zu treiben.

von WOLFGANG PRENTNER

„Amazon, Yahoo! und eBay sind bereits Opfer von Hack-Angriffen geworden, „Server des Wirtschaftsforum Davos geknackt“, „Sicherheitslücke bei Kreditkarten-Unternehmen machen Kreditkartennummern von Kunden zugänglich“. Diese Schlagzeilen stimmen nachdenklich, sie zeigen uns die Verwundbarkeit aber auch die elementare Bedeutung von Sicherheit in der Informationstechnologie.

Derzeit sind mehr als 930 Millionen Internet-User vernetzt und über 113 Millionen Internet Server weltweit aktiv. In Österreich nutzen bereits 4,6 Millionen Österreicher das Internet. Im Jahr 2006 setzten 99 Prozent der österreichischen Unternehmen mit mehr als neun Beschäftigten Computersysteme ein. Unter den Kleinunternehmen

sind es mittlerweile 98 Prozent, so die Informationen der Statistik Austria.

In 24 Prozent aller Unternehmen gibt es Beschäftigte, die über elektronische Netzwerke von außerhalb des Unternehmens mit ihrer Arbeitsstätte kommunizieren. Bei den Großunternehmen trifft dies sogar für 71 Prozent aller Unternehmen zu. 85 Prozent der Unternehmen mit Beschäftigten, die über elektronische Netzwerke mit ihrer Arbeitsstätte kommunizieren, gaben an, dass ihre Beschäftigten dies von zu Hause aus tun. Dabei ist die Datensicherheit für Unternehmen und Behörden von zentraler Wichtigkeit.

DER FAKTOR MENSCH: Mit dieser Definition der IT-Sicherheit ist man sich darüber klar geworden, dass diese Sicherheitsaspekte sehr stark auf die Gefährdung durch

äußere Angriffe abzielen. Auch heute noch wird unter Sicherheit von vielen der Schutz vor externen Angreifern verstanden. Wichtig ist jedoch auch der Schutz von unbeabsichtigten Sicherheitsverlusten. Weitaus mehr Schäden – die meisten Untersuchungen sprechen von über 80% – werden durch Fehlbedienungen, Unachtsamkeit oder aber durch vorsätzliche Handlungen der berechtigten Benutzer verursacht.

Technologie ist ein Schlüssel im Kampf gegen Missbrauch und hat eindeutig Priorität für Unternehmen und Behörden, wobei der Faktor Mensch noch immer das größte Sicherheitsrisiko darstellt, so das renommierten deutschen Fachmagazin für Informationssicherheit. Derselben Ansicht ist auch Mag. Rudolf Unterköfler vom Bundeskriminalamt zur Bekämpfung von Online-Kriminalität: „Das Sicherheitsbewusstsein ist europaweit stark gestiegen, nicht zuletzt durch die verstärkte Zusammenarbeit der Behörden auf internationaler Ebene.“

TRENDS BEI DER SICHERHEIT von Daten gehen verstärkt in Richtung IT-Risikomanagements – in Österreich und International wird dabei auf CRISAM© (www.crisam.at) hingewiesen, dem Aufbau eines Informations-Sicherheitsmanagements-Systems (ISMS) als auch dem Einsatz verbesserter Sicherheitstechnologien. Digitale Signatur und biometrische Verfahren zum Identity Management spiegeln den heutigen Stand der Technik wieder. Ein weiterer Trend der ersichtlich ist, ist die Auslagerung der IT-Services in Rechenzentren die heute Sicherheitshochburgen darstellen. Als Beispiel für die Notwendigkeit der Sicherheit von Daten kann das derzeit in Planung befindliche elektronische Urkun-

Viren, Würmer und sonstige Schädlinge

Mittlerweile ist jedes zweite E-Mail, das an österreichische Unternehmen geschickt wird ein Spam und jede fünfte elektronische Nachricht transportiert einen Virus von denen es weltweit mittlerweile über 60.000 verschiedene Arten gibt. Das Gefahrenpotential steigt weiter an, denn jeden Tag kommen mehr als ein dutzend neue Computer-Parasiten hinzu.

Hacker: Ein Hacker ist ein überaus talentierter Computer-Spezialist, der insbesondere Sicherheitsbarrieren überwinden und in fremde Systeme eindringen kann.

Viren: Ein Computervirus ist ein sich selbst vermehrendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert und auch Schaden anrichten kann.

Wurm: Ein Computervorm ist ein Computerprogramm, das sich über Computernetzwerke

verbreitet. Sie verbreiten sich zum Beispiel durch das Versenden infizierter E-Mails.

Trojaner: Als Trojanisches Pferd, auch kurz Trojaner (engl. Trojan) genannt, bezeichnet man ein Programm, welches als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine ganz andere Funktion erfüllt.

Spam: Als Spam werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt und unerwünscht zugestellt.

Phishing: Phishing versucht, den Empfänger irreführen und zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen. Dies bezieht sich in den meisten Fällen auf Online-Banking und andere Bezahlsysteme.



Foto: Archiv

derung an die Sicherheit von Daten. Gesetze sollen dabei die Innovation im Technologiebereich nicht hemmen, daher sind EU-Richtlinien zur digitalen Signatur oder das Datenschutz-, E-Commerce- oder Signaturgesetz begleitende Maßnahmen zur Datensicherheit. Derzeitige Standards sind derzeit ISO 27001, ITIL, COBIT, Common Criteria udgl.

SICHERHEITSVORKEHRUNGEN:

Virenschutz und Personal Firewall sollten zur Software-Grundausstattung jedes PCs gehören. Egal ob dieser „nur“ privat oder aber betrieblich genutzt wird. Personal Firewalls, die z. B. in den Betriebssystemen Windows XP und Vista bereits integriert sind, bieten in Verbindung mit einem Internet Security-Paket einen hohen Schutz vor Viren, Würmern, Spyware, Phishing und sonstigen Schädlingen.

Der IT-Ziviltechniker nimmt heute schon zentrale Aufgaben im Bereich der Sicherheit von Daten wie die Technologieberatung, Planung, begleitende Überwachung und die Prüfung inklusive Zertifizierung der Datensicherheit z. B. nach dem Datenschutzgesetz in den Bereichen E-Business, E-Health und E-Government wahr. Durch die Globalisierung, die internationalen Standardisierungen

und Akkreditierungen von international tätigen Konzernen im Sicherheitsbereich ist der IT-Ziviltechniker in Teilbereichen seiner Befugnis einem verstärkten Wettbewerb ausgesetzt, den er durch seine hohe Fachkenntnis, Kompetenz, Flexibilität und staatliche Reputation wettmacht. Durch die globale Vernetzung fährt der Zug aber klar ersichtlich in Richtung international anerkannten Zertifikaten von international akkreditierten Unternehmen und Organisationen ab.

Sollte berechtigter Zweifel an der Vertrauenswürdigkeit gespeicherter Daten von Computersystemen, der Sicherheit von Schutzmechanismen wie Firewalls oder ein konkreter Hinweis auf Viren, Würmer, Trojaner oder Spyware im Computer bestehen, ist der IT-Ziviltechniker der kompetente Ansprechpartner: Der IT-Ziviltechniker prüft und beurteilt Computersysteme in sicherheitstechnischen Fragen und gibt Empfehlungen ab, wie Systeme vor Angriffen effektiv geschützt werden können.

DI Dr.techn. Wolfgang Prentner

*ist Ingenieurkonsulent für Informatik und
Vorsitzender der Bundesfachgruppe
Informationstechnologie der Bundeskammer.*

denarchiv der Ziviltechniker genannt werden, bei dem die Sicherheit von öffentlichen Urkunden der Ziviltechniker groß geschrieben wird. Der Einsatz der digitalen Signatur ist dabei obligatorisch.

International wird im Sicherheitsbereich verstärkt auf Standardisierung und weniger auf rigide Gesetzgebung geachtet – frei nach dem Motto „Der Markt regelt die Anfor-