Internationale Anti-Spam-Strategie

Sicherheit in der Informationstechnik war ein Schwerpunkt auf der CeBIT 2005 vom 10. bis 16. März 2005 in Hannover. Die weltgrößte Messe war Schauplatz zukunftsweisender Technologien.

Mehr als 40 Millionen Deutsche und vier Millionen Österreicher nutzen regelmäßig das Internet. Täglich werden weltweit 30 Milliarden E-Mails versendet, 60 Prozent davon sind Spam-Mails, unerwünschte Werbemails. Die Informationstechnologie habe Schattenseiten, die bekämpft werden müssten, sagte Deutschlands Bundesinnenminister Otto Schily bei der Eröffnung des „Public Sector Parks“ bei der diesjährigen CeBIT in Hannover. „Der wirtschaftliche Erfolg hängt nicht zuletzt davon ab, ob es gelingt, diese Technik in jeder Weise sicher zu machen“, betonte Schily und forderte eine umfassende nationale und internationale Anti-Spam-Strategie durch rechtliche, wirtschaftliche und technische Maßnahmen. Diese müssten bereits bei den Providern ansetzen, etwa, dass an Hand von Blacklists Spam-Mails ausgefiltert werden. Durch Spam und Netzattacken geht in Deutschland mehr Produktivität verloren als durch Streiks.

Dem Schutz vertraulicher Informationen im öffentlichen Dienst und in der Wirtschaft soll verstärktes Augenmerk zugewendet werden, wobei der Biometrie und der Kryptografie besondere Bedeutung zukommen wird. Biometrische Verfahren können Dokumentenmissbrauch entscheidend einschränken oder Unberechtigten den Zugang zu geschützten Räumen verwehren.

Das Ziel, 376 Dienstleistungen der Verwaltung als E-Government über das Internet anzubieten, werde bis Jahresende erreicht werden, kündigte Schily an. Es werde dabei nicht nur Information auf diesem Weg angeboten, sondern es soll zu echter Transaktion kommen. Deutschland startet eine Breitbandoffensive, kündigte der Minister für Wirtschaft und Arbeit, Wolfgang Clement, an. Die Einführung der elektronischen Gesundheitskarte ab 1. Jänner 2006 erfordere leistungsfähige Netze, ebenso Telemedizin und E-Learning. Letztlich gehe die technische Entwicklung in Richtung des „Triple-Play“: Fernsehen, Telefon und Daten-übertragung (Internet) wachsen zusammen.

„Sicheres Rechenzentrum“: Lösungen für Brandschutz, Stromversorgung und mehr.

Datenausspähung. Virenschreiben ist out, Spyware ist in. Virenschreiber dürften erkannt haben, dass es lukrativer ist, Daten auszuspähen und zu Geld zu machen, als sie bloß sinnlos zu zerstören. Eine brauchbare Internet-Adresse wird um 15 bis 20 Euro gehandelt. Ein Drittel aller Unternehmen ist nach den Feststellungen des auf Spyware spezialisierten Unternehmens *Webroot (www.webroot.com)* von derartigen Programmen befallen – mit der Folge, dass sie im harmlosen Fall mit Spam überhäuft werden. Schlimm ist, wenn Geschäftsdaten ausspioniert werden. Gegen Antispam-Software wurden Rootkits entwickelt, Programme, die Spyware verstecken und dadurch unangreifbar machen.

Webroot unterhält einen eigenen Rechnerverbund, der alle auf der Welt ans Internet angeschlossenen Rechner nach dem Vorhandensein von Spyware und neuer Formen dieser Software untersucht. Ein Überprüfungszyklus dauert acht Tage.

CefIS. Die mit Sicherheit in der Informationstechnik befassten Firmen waren bei der CeBIT wieder im Centrum für Informationssicherheit (CefIS) der „von zur Mühlen GmbH“ zusammengefasst. Im Mittelpunkt stand auch heuer das „Sichere Rechenzentrum“. Hier wurde erläutert, wie sicherheitstechnisch optimale Lösungen getroffen werden können – auf den Gebieten des Brandschutzes, der (unterbrechungsfreien) Stromversorgung, der Klimaanlage, des Schutzes vor austretendem Wasser und der Zutrittskontrolle.

Kostenlos CDs über Sicherheit im Internet gab es beim Ausstellungsstand des *Bundesamts für Sicherheit in der Informationstechnik (BSI).* Das BSI veranstaltete eine Reihe von Fachvorträgen. BSI-Präsident Dr. Udo Helmbrecht überreichte auf der Messe Grundschutz-Zertifikate, durch die nach Überprüfung bestätigt wird, dass ein damit ausgezeichnetes Unternehmen das IT-Grundschutzhandbuch und die dort angeführten Sicherheitsempfehlungen anwendet.

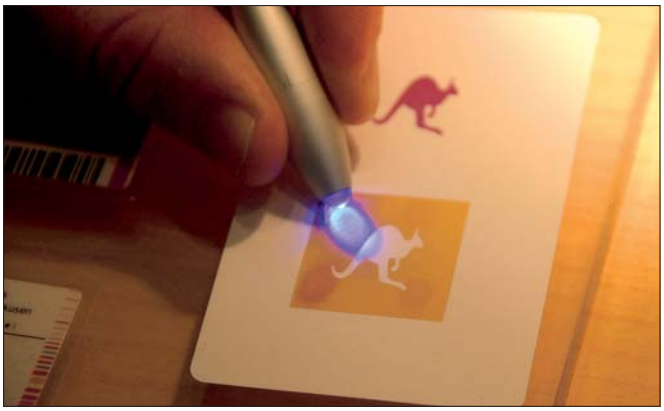
Neues Löschsystem. Die Firma Kidde-Deugra stellte im CefIS ein Löschsystem auf der Basis des Löschmittels *Novec™ 1230* von *3M* vor. Das bei Raumtemperatur flüssige Löschmittel ist elektrisch nicht leitend – ein in die Flüssigkeit eingetauchtes Handy blieb funktionsfähig. In der Atmosphäre löst sich das Gas nach Herstellerangaben spätestens nach fünf Tagen ohne Gefahr für die Ozonschicht auf.

Die Flüssigkeit steht in Behältern durch Stickstoff unter einem Druck von etwa 40 bar und wird bei einem Brand über spezielle Düsen verdampft. Die brandlöschende Wirkung entsteht da-

FOTO: KURT HICKISCH

CeBIT 2005
6.000 Stände

Die jährliche CeBIT in Hannover ist mit einer Netto-Ausstellungsfläche von 309.000 Quadratmetern die größte Messe der Welt. Sie gilt als Leitmesse der internationalen ITK-Industrie. Es herrschte großer Andrang: 2005 präsentierten 6.270 Aussteller ihre Produkte und Dienstleistungen; 2004 waren es 6.109.



Dokumentensicherheit: Mit einer Bakterienfarbe können Dokumente und Banknoten fälschungssicher gemacht werden.

durch, dass dem Feuer eine seiner Komponenten, die Wärme, entzogen wird. Es findet also nicht, wie beispielsweise bei Inertgasen, eine Sauerstoffverdrängung statt, mit der damit verbundenen Erstickungsgefahr für Menschen und der Gefahr des Überdrucks.

Dokumentensicherheit. Die Philipps-Universität Marburg hat die Anwendungsmöglichkeiten des aus einem Bakterium gewonnenen Pigments Bakteriorhodopsin weiterentwickelt. Es handelt sich um eine fotochromatisches Protein, das unter Einwirkung sichtbaren Lichts seine Farbe sehr augenfällig von Violett auf Gelb ändert. Diese Eigenschaft kann genützt werden, um Dokumente (Banknoten) fälschungssicher zu gestalten. Ändert sich die Farbe unter Lichteinfluss nicht, liegt eine Kopie vor. Die Herstellung des Farbstoffs erfordert hohes biotechnologisches Wissen. Außerdem können, ohne die grundlegenden Eigenschaften zu verändern, Sequenzen der Aminosäuren verändert werden; das Material kann dadurch codiert werden, mit 2010 Kombinationsmöglichkeiten, sodass eine Rückführbarkeit auf den Ursprungsort gewährleistet werden kann.

Bei Einwirkung sehr hoher Lichtenergie, wie sie durch Laserpulse in Pico- bis Nanosekundenbereich erzielt wird, wird der Farbwechsel irreversibel, was zur Datenspeicherung im Bereich von 1 MB/cm^2 benützt werden kann (www.chemie.uni-marburg.de/hampp).

Unfallübungs-Software. Mit der aus den Niederlanden kommenden Software *diabolo*VR können Unfälle virtuell durchgespielt werden (www.e-semble.com). Der Kursteilnehmer wird über den Bildschirm in ein Szenario versetzt und kann sich mit dem Joystick in dieser virtuellen Welt bewegen, in der sich ein Verkehrsunfall, ein Brand in einem Tunnel oder in einer petrochemischen Anlage oder ein sonstiger Feuerwehreinsatz ereignen. Er hat die Lage zu beurteilen und Entscheidungen zu treffen, deren Folgen mitverfolgt werden können.

Datenarchivierung. E-Mails müssen nach handels- und steuerrechtlichen Bestimmungen bis zu sieben Jahre lang aufbewahrt werden, wenn über sie Geschäftsverkehr abgewickelt wird. Wer hat eigentlich noch 5 1/4-Zoll-Laufwerke, wie sie vor dieser Zeit noch gang und gäbe waren? Da sammelt sich, bei der Schnelllebigkeit der technischen Entwicklung, allein zum Zweck der Archivierung im Keller ein Computer-Museum an, und es stellt sich für die Archivierung die Frage, inwieweit die heute gebräuchlichen Formate zur Datenspeicherung in 10 oder 20 Jahren hard- und softwaremäßig noch gelesen werden können. *K.H.*

FOTO: KURT HICKISCH