



IT-Sicherheitsmesse it-sa 2010 in Nürnberg: 304 Aussteller und 7.100 Besucher.



Bundesamt für Sicherheit in der Informationstechnik: Präsentation des neuen Personalausweises in Scheckkartenformat.

# Umfassende Information

**Sicherheit bei der Anwendung der Informations- und Kommunikationstechnologie muss auch kommuniziert werden – bei der IT-Sicherheitsmesse it-sa in Nürnberg war das der Fall.**

**K**ommunikation war großgeschrieben bei der it-sa, die vom 19. bis 21. Oktober 2010 in der Halle 12 der Messe Nürnberg stattfand. Neben dem bewährten Konzept, in einem *Forum Blau* technisch orientierte Fachvorträge anzubieten und im *Forum Rot* eher solche mit strategischem und ökonomischem Hintergrund der IKT-Sicherheit, waren ein Auditorium für einen breiteren Zuhörerkreis ansprechende Themen eingerichtet sowie im Rahmen der Sonderfläche „Das perfekte Rechenzentrum“ ein *Forum Orange* speziell für Fragen der Sicherheit von Rechenzentren. Ferner fanden im angrenzenden Kongresszentrum 14 weitere Fachveranstaltungen statt. Insgesamt wurden 320 Fachvorträge abgehalten – sie können unter [www.it-sa/Programm](http://www.it-sa/Programm) als Videostream im Internet abgerufen werden samt den Handouts. Die Benutzerdaten erhält man bei Angabe von Namen und Adresse zugesendet.

**Speichermedien.** In Laptops werden die auf Magne-

tisierungseffekten beruhenden Festplatten als Datenspeicher zunehmend durch elektronische Speicherbauteile (Flash-Speicher) ersetzt. Diese aus mehreren Chips aufgebauten *Solid State Drives (SSD)* haben eine Speicherkapazität bis zu 250 GB, sind schneller, kleiner und durch den Wegfall mechanisch bewegter Bestandteile gegen mechanische Belastungen unempfindlicher als Festplatten. Sie verbrauchen weniger Strom. Allerdings sind sie noch deutlich teurer als Festplatten mit gleicher Kapazität, auch ihre Lebensdauer ist geringer.

Die unter den Ausstellern vertretene, auf Datenrettung spezialisierte österreichische Firma *Attingo* ([www.attingo.at](http://www.attingo.at)) ist in der Lage, auch auf solchen Speichermedien verloren gegangene Daten wiederherzustellen, indem einzelne Speichereinheiten entnommen und ausgelesen werden.

**Neue Produkte.** *Kensington* ist Marktführer darin, tragbare elektronische Geräte wie Laptops oder Notebooks mit einem Schloss

über ein flexibles Stahlkabel vor Diebstahl zu schützen. Das elektronische Buch verbreitet sich rasch und bietet beispielsweise gegenüber Loseblatt-Ausgaben oder bei Schulungsunterlagen den Vorteil, rasch und kostengünstig aktualisiert werden zu können. In Anbetracht der leichten Verbreitbarkeit steigen aber auch die vom Standpunkt des Urheberrechts her zu stellenden Ansprüche.

Ein *Digital Rights Management (DRM)* muss regeln, wer wie viele E-Books besitzen darf, ob er Kopien anfertigen oder Ausdrücke machen darf und wie lange Berechtigungen gelten.

Die *OEM GmbH*, Saarbrücken ([www.oem.de](http://www.oem.de)), hat einen Buchstick entwickelt, der als USB-Stick kopiergeschützt und verschlüsselt den Inhalt eines Druckwerks gespeichert enthält und das über elektronische Medien lesbare Buch darstellt – mit dem Vorteil, online aktuell gehalten werden zu können. Weitergabe und Nutzung können individuell festgelegt werden. Dazu kommen komfortable Suchfunktionen und

Verlinkungen ([www.buchstick.de](http://www.buchstick.de)).

**Social Media Guidelines.** Rechtsanwalt Andreas Crone von *Rödl & Partner*, Nürnberg, referierte über rechtliche Herausforderungen bei der Nutzung von „Social-Media-Diensten“ in Unternehmen. Zwei Drittel der deutschen Internetnutzer bewegen sich in sozialen Netzwerken wie *Facebook*, *Xing*, *LinkedIn* und *Twitter* – auch während der Arbeitszeit. Es stellt sich die Frage, wie Unternehmen damit umgehen. Immerhin können sie von solchen Kontakten auch profitieren, und beispielsweise bei *Xing* oder *LinkedIn* stehen geschäftliche Kontakte im Vordergrund. Personalberater („Headhunter“) suchen in diesen Netzwerken und umgekehrt kann man in diesen auch ein positives Bild von sich selbst entwickeln.

Nicht übersehen werden darf, dass Mitarbeiter allenfalls ein negatives Image des Unternehmens vermitteln und soziale Netzwerke dazu benützt werden können, vertrauliche Informationen abzuschöpfen. Letztlich geht es

# Produkte für den Sicherheitsbereich

Alarmanlagen Videüberwachung

Beratung • Planung • Verkauf • Montage • Service

Ing. **Witke** Ges.m.b.H

**01 / 769 83 50**

1110 Wien • Simmeringer Hauptstraße 257  
office@witke.com • www.witke.com

## WIR PRÜFEN, WAS DAHINTER STECKT



Asphalttechnologie / Straßenbau  
und Flugplatzbau



Zement

Bituminöse Bindemittel

STAATLICH AKKREDITIERTE  
PRÜF- UND ÜBERWACHUNGSSTELLE

Umweltechnik

Asphalt für Wasserbau und  
Deponiebau

**OQS** Zertifiziert gem. ISO 9001

Recycling Bauweisen,  
Stabilisierungen

Erd- und Grundbau

**OIB** Landesrechtlich  
akk. Prüf- u.  
Überwachungsstelle

Sonderbau / Baucheimie

Technische Gesteinskunde

Bemessung von Straßen und  
Flugplätzen

Betontechnologie

Pavement Management

TPA Gesellschaft für Qualitätssicherung und Innovation GmbH

A – 1220 Wien  
Polgarstraße 30  
Tel. +43 (0)1 / 21 728 – 312  
Fax +43 (0)1 / 21 728 – 112

A – 9710 Feffernitz  
Werkstraße 17 a  
Tel. +43 (0)4245 / 2670  
Fax +43 (0)4245 / 4527

A – 4021 Linz  
Salzburgerstr. 323 a  
Tel. +43 (0)732 / 3731 – 509  
Fax +43 (0)732 / 3731 – 400

A – 8644 Mürzhofen  
Wiener Str. 15  
Tel. +43 (0)3864 / 5515 – 20  
Fax +43 (0)3864 / 5515 – 26

A – 6170 Zirl  
Salzstraße 3 a  
Tel. +43 (0)5238 / 52169 – 20  
Fax +43 (0)5238 / 52169 – 24

**schiekmetall**



TSE - Türschloss Elektronik  
Immer auf der sicheren Seite!

Schiekmetall Handels-GmbH  
Albert Schweitzer-Gasse 9  
1140 Wien

Tel.: 0043/1/97-026-0  
Fax: 0043/1/97-026-55

info@schiekmetall.at

www.schiekmetall.at



„Solid State Drives“ ersetzen Festplatten.

auch um die Bindung von betrieblichen Ressourcen und den Verlust an Arbeitszeit. Es sind ähnliche Probleme wie bei der privaten Nutzung von Telefon und E-Mail am Arbeitsplatz: Es steht dem Arbeitgeber frei, eine derartige Nutzung generell zu verbieten und die Einhaltung zu überwachen. Auch bei nur stillschweigender Duldung ist eine generelle Überwachung nicht mehr zulässig. Es gilt, Vor- und Nachteile der Nutzung sozialer Netzwerke abzuwägen. Crone empfiehlt, im Zusammenwirken mit dem Betriebsrat den Mitarbeitern „Social Media Guidelines“ als Leitfaden an die Hand zu geben, in denen beispielsweise der zeitliche Umfang der Nutzung dieser Netzwerke geregelt ist, Beschränkungen auf „Business Networks“ wie *Xing* oder *LinkedIn* erfolgen und auch auf die Verschwiegenheitspflicht, die Grenzen zulässiger Kritik und die Unterlassung unternehmensschädlicher Äußerungen hingewiesen wird.

### Neuer Personalausweis.

Auf Grund der am 1. November 2010 in Deutschland erfolgten Einführung des neuen Personalausweises hat das deutsche *Bundesamt für Sicherheit in der Informationstechnik (BSI)* in Vorträgen und am Messestand einen seiner Schwerpunkte auf die elektronische Identität gelegt. Der neue Personalausweis hat das Format einer Scheckkarte und kann anhand der lesbar aufgedruckten Daten über den Inhaber sowie dessen Foto als her-



Kensington Lock: Diebstahlsicherung für Notebooks.

kömmlicher Ausweis verwendet werden. Der im Ausweis integrierte, berührungslos auslesbare Chip enthält diese Daten überdies in elektronischer Form, was seinen Inhaber in die Lage versetzt, sich im Internet auszuweisen. Damit können beispielsweise Behördengänge erledigt oder personalisierte Internet-Services (Online-Shops, Banken, soziale Netzwerke) genutzt werden. Das hierzu erforderliche Basis-Lesegerät – sofern ein solches nicht in der Tastatur integriert ist – kostet zwischen 10 und 15 Euro. Auf Wunsch können zur Erhöhung der Sicherheit gegen Missbrauch bei Verlust oder Diebstahl auch zwei Fingerabdrücke zusätzlich gespeichert werden.

Der Benutzer, der zur Nutzung der elektronischen Ausweisfunktion neben dem Ausweis die sechsstellige geheime PIN einsetzen muss, kann bestimmen, ob und welche Daten er im Internet übermittelt. Für den Umgang beispielsweise in sozialen Netzen kann eine pseudonyme Kartenkennung verwendet werden, ohne dass persönliche Daten preisgegeben werden. Eine Abfrage, ob ein bestimmtes Alter erreicht ist (Jugendschutz), wird nicht mit der Weiterleitung des Geburtsdatums, sondern mit einem Ja oder Nein beantwortet. Zudem können Anbieter von Internet- oder Automaten Diensten nur dann auf Ausweisdaten zugreifen, wenn sie dafür ein staatlich ausgestelltes Zertifikat besitzen, sodass auch die Identität der Gegenseite feststeht. Zu

dieser von vornherein gegebenen eID-Funktion kann sich der Inhaber – ähnlich der Funktion Bürgerkarte in Österreich – ein (kostenpflichtiges) Zertifikat auf den Ausweis laden und hat mit dieser QES-Funktion (Qualifizierte Elektronische Signatur) die Möglichkeit, elektronische Dokumente und Willenserklärungen rechtssicher elektronisch zu unterschreiben. Dazu ist als Zusatzgerät ein Lesegerät mit der Möglichkeit zur PIN-Eingabe und einem Display erforderlich.

Die biometrischen Daten können durch die Verschlüsselung und die beim Lesevorgang ablaufenden kryptografischen Protokolle nur von berechtigten Behörden (Polizei, Zoll Grenzkontrolle, Meldebehörden) ausgelesen werden, und das nur auf eine Entfernung von wenigen Zentimetern. Der Ausweis muss auf ein Lesegerät gelegt oder in ein solches hineingeschoben werden. Ein unbemerktes Auslesen ist nicht möglich.

Der neue Personalausweis wird zentral von der Bundesdruckerei in Berlin hergestellt und ist für Personen unter 24 Jahren sechs Jahre gültig, sonst zehn Jahre. In der Regel wird das Dokument für Personen ab 16 Jahren ausgestellt. An Gebühren sind 28,80 Euro zu entrichten, für den Ausweis mit sechsjähriger Gültigkeit 22,80 Euro. Alte Personalausweise behalten bis zum Ablaufdatum ihre Gültigkeit. Ein vorzeitiger Austausch ist jederzeit möglich.

**IKT an Schulen.** Der Arbeitskreis *Schule des Berufsverbandes der Datenschutzbeauftragten Deutschlands e.V.* ([www.bvdnet.de](http://www.bvdnet.de)) hat die Aktion „Datenschutz geht zur Schule“ ins Leben gerufen, die nach zweijährigem Testlauf in den Bundesländern Nordrhein-Westfalen, Hessen und Bayern auf ganz



„it-sa“ Nürnberg: Stand des Landeskriminalamts Bayern.

Deutschland ausgeweitet werden soll. Laut dem Initiator und Leiter des Arbeitskreises Thomas Floß gehe es darum, bei Kindern und Jugendlichen der 6. und 7. Schulstufe mehr Sensibilität im Umgang mit den neuen Medien und mit Kommunikationsplattformen zu schaffen und auch die Schattenseiten wie Cybermobbing und Abzocke aufzuzeigen. So bemerkten zwei Schülerinnen, dass die Kontrollleuchte der Webcam an ihrem Laptop fallweise aufleuchtete, ohne dass sie diese aktiviert hatten. Ein Hacker hatte über eine als Bildschirmschoner getarnte Schadsoftware die Kontrolle über die Rechner erlangt, die Internetkameras ferngesteuert aktiviert und damit freie Sicht ins Kinderzimmer erhalten. Die Adressen der Mädchen hatte er sich über den Messenger-Zugang eines Mitschülers geholt. Sichere Passwörter, ein aktueller Virenschutz und ein sen-

siblerer Umgang mit unbekannter Software hätten diese Zugriffe verhindert. „Sei misstrauisch, glaub nicht alles“, ist einer der Ratschläge.

**Hochschulstudien.** In einem eigenen Themenbereich, dem *Campus@it-sa*, präsentierten deutsche Hochschulen ihre Möglichkeiten für die akademische Ausbildung von Sicherheitsingenieuren und -managern. Die Hochschule Furtwangen (Baden-Württemberg) bietet seit dem Wintersemester 2007/08 ein siebensemestriges Bachelor-Studium an, das sowohl Security als auch technische Sicherheit (Safety) umfasst.

Auf dem Gebiet der Sicherheit sollen Generalisten herangebildet werden, mit der Möglichkeit zur Spezialisierung, beispielsweise einer Zusatzausbildung als Brandschutz- oder Strahlenschutzbeauftragter. Im fünften Semester ist ein Berufspraktikum vorgesehen. 2011 ist eine Erweiterung

auf ein Master-Studium geplant ([www.SecurityandSafetyEng.de](http://www.SecurityandSafetyEng.de)).

Die Hochschule Albstadt-Sigmaringen (Baden-Württemberg) startete im Wintersemester 2010/11 einen berufsbegleitenden, auf E-Learning aufgebauten sechssemestrigen Master-Studiengang „Digitale Forensik“. Voraussetzungen sind ein mit dem Bachelor abgeschlossenes Studium sowie ein Jahr Berufserfahrung ([www.digitaleforensik.com](http://www.digitaleforensik.com)). Ziel ist die Heranbildung von Ermittlern und Kriminologen im Cyberspace.

An der FH Brandenburg wird der dreisemestrige, Sicherheit ganzheitlich betrachtende Masterstudiengang Security Management angeboten. Zulassungsvoraussetzung ist ein Hochschul- bzw. Fachhochschulabschluss. Neben Information-Security und Forensik werden Gebäude- und Personen- sowie Anlagen- und Reaktorsicherheit und Kenntnisse in Unternehmensführung und Personalwesen vermittelt ([www.security-management.de](http://www.security-management.de)).

Für Absolventen eines zumindest dreijährigen Informatik-Studiums wurde an der Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit – if(is), der viersemestrige Masterstudiengang Internet-Sicherheit eingerichtet ([www.internet-sicherheit.de](http://www.internet-sicherheit.de)).

Die *International School of IT Security AG* bietet mit der Ruhr-Universität Bochum den berufsbegleitenden Fernstudiengang „Applied IT Security“ an. Das Studium dauert mindestens vier Semester. Zulassungsvoraussetzungen sind ein abgeschlossenes Studium und ein Jahr Berufserfahrung. Der akademische Titel „Master of Science“ wird von der Ruhr-Universität Bochum verliehen ([www.is-its.org](http://www.is-its.org)). Kurt Hickisch

## IT-SA

Die aus einem Teilbereich der ehemaligen *Systems* in München hervorgegangene, vom *Secumedia-Verlag* seit 2009 im Kongresszentrum in Nürnberg veranstaltete IT-Sicherheitsmesse *it-sa* konnte im zweiten Jahr ihres Bestehens die Zahl der Aussteller von 257 auf 304

steigern und die Zahl der Besucher von 6.600 auf 7.100. Die Messe bündelt das Angebot an Produkten und Dienstleistungen auf dem Gebiet der IT-Sicherheit.

Die nächste *it-sa* wird vom 11. bis 13. Oktober 2011 in Nürnberg stattfinden.