Information – aber sicher

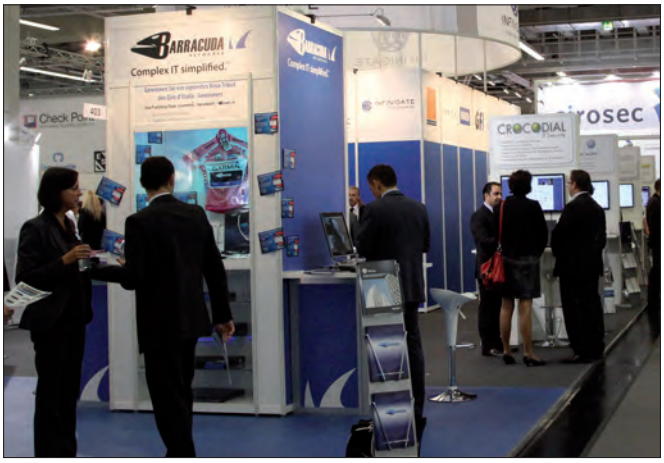
Von Abhörsicherheit bis Zutrittskontrolle reichte das Angebot der Aussteller bei der IT-Sicherheitsmesse IT-SA vom 16. bis 18. Oktober 2012 im Messezentrum Nürnberg.

Vierzig Prozent der Wertschöpfung basieren weltweit auf der Informations- und Kommunikationstechnologie“, sagte die Beauftragte der deutschen Bundesregierung für Informationstechnik, Staatssekretärin Cornelia Rogall-Grothe, am 16. Oktober 2012 bei der Eröffnung der IT-SA 2012 in Nürnberg. „In Deutschland sind die Hälfte der Unternehmen quer durch alle Branchen schon jetzt vom Internet abhängig.“

Die zunehmende Digitalisierung und Vernetzung habe zu faszinierenden Möglichkeiten geführt, aber auch zu neuen Abhängigkeiten. Die Chancen müssten genützt und die Risiken so gering wie möglich gehalten werden. Die Cyber-Kriminalität entwickle sich in besorgniserregendem Maße. Alle zwei Sekunden werde ein neues Schadprogramm installiert. An die 60.000 Webseiten würden täglich mit Schadprogrammen infiziert und damit Ansteckungspunkte bilden.

Von 2006 bis 2011 hätten sich die Fälle von Internetkriminalität in Deutschland von rund 30.000 auf 60.000 verdoppelt. Die registrierten Schäden seien um 70 Prozent angestiegen und beliefen sich im Jahr 2011 auf über 71 Millionen Euro.

Täglich würden auf Regierungssysteme fünf gezielte Spionageangriffe stattfinden. Der Staat habe die Aufgabe, die Cyber-Sicherheit auf einem angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen, und habe kritische Infrastrukturen zu schützen. Je höher der Grad an Cyber-Sicherheit sei, umso attraktiver seien der Markt und das Interesse, in diesem Markt wirtschaftlich tätig zu werden. Cyber-Sicherheit sei ein Standort- und strategischer Wettbewerbsvorteil. „IT-Sicherheit ist der Schlüssel zum Erfolg für unsere Zukunft. Auf jeden Einzelnen von uns kommt es an.“



334 Aussteller aus 50 Ländern und 6.100 Besucher auf der größten IT-Sicherheitsmesse im deutschsprachigen Raum.

FOTO: KURT HICKISCH

Allianz für Cyber-Sicherheit. Der Vizepräsident des *Bundesamtes für Sicherheit in der Informationstechnik (BSI; www.bsi.bund.de)*, Horst Flätgen, betonte, dass Vertrauen in die neuen Technologien die Grundvoraussetzung für deren Anwendung sei. Die Angriffe seien professioneller geworden. Mittlerweile stehe auch die Zertifikats-Infrastruktur im Fokus der Angreifer.

Die im März auf der *CeBIT 2012* angekündigte Allianz für Cyber-Sicherheit *(www.allianz-fuer-cybersicherheit.de)* habe den Echtbetrieb aufgenommen und habe bereits 35 Partner. Ziel der Allianz sei es, eine Verknüpfung mit der Wirtschaft herzustellen und einen offenen Erfahrungsaustausch über Best-Practice-Beispiele herzustellen. Da die Angriffe zumeist über automatisierte Verfahren erfolgen, sei die rhetorisch gemeinte Frage, „Wer will schon etwas von mir?“, für die Unterlassung von IT-Sicherheitsmaßnahmen kein stichhaltiges Argument mehr.

Die Allianz wurde vom *BSI* zusammen mit dem *Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.; www.www.bitkom.org)* gegründet. Dessen Präsident Prof. Dieter Kempf hob bei der Eröffnung der IT-SA hervor, dass das BSI im Gegensatz zur Polizei nach einem gemeldeten Angriff nicht verpflichtet sei, Ermittlungen aufzunehmen. Eine Steigerung der Meldung von IT-Sicherheitsvorfällen aus der Wirtschaft sei anzustreben, ohne allerdings eine Meldepflicht einzuführen. Dies könnte zu einer Abwehrhaltung führen. Eine Art „digitale Babyklappe“, bei der Meldungen anonym erfolgen, könnte helfen zu vermeiden, dass auch andere Unternehmen in die gleiche Falle tappen. Die Meldungen aus der Wirtschaft sollten sich letztlich zu einem Lagebild verdichten lassen, das vom *BSI* als zentralem staatlichen Träger ausgewertet werde. Umgekehrt stelle diese Behörde im Wege des *Bitkom* der Wirtschaft Abwehrmittel zur Verfügung.

Nach einer Studie des *Bitkom* haben 39 Prozent der befragten 810 Unternehmensverantwortlichen Cyberattacken, zwei Prozent sogar öfter als 20-mal. 57 Prozent der Befragten sahen Angriffe auf ihre IT-Systeme, etwa von Hackern, Konkurrenten, Kriminellen oder ausländischen Geheimdiensten, als reale Gefahr; 45 Prozent haben keinen Notfallplan vorbereitet. 53 Prozent verzichten aus Sicherheitsgründen auf Transaktionen im Internet – und nehmen sich die Chancen, die in der Nutzung dieses Mediums liegen. 43 Prozent der IT-Unternehmen erlauben die Nutzung privater Geräte wie Laptops, Smartphones oder Tablets für die Arbeit, wobei als Hauptgrund dafür die höhere Zufriedenheit der Mitarbeiter und eine Steigerung der Effizienz angeführt wurden.

„Bring Your Own Device“. Die Vermischung von Beruf und Privatleben, die ständige Erreichbarkeit und die Möglichkeit, Arbeit nach Hause mitzunehmen, wirft bei der betrieblichen Nutzung von eigenen Endgeräten und der Vermischung von privater und geschäftlicher IT Probleme organisatorischer, rechtlicher und technischer Art auf: Wem gehören dann eigentlich Hardware, Software, Lizenzen? Welcher Datentarif findet Anwen-

IT-Sicherheitsmesse: Stand des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Verschlüsselungssystem für abhörsicheres Telefonieren mit Smartphones.

dung? Die Bezuschussung privater Geräte durch den Arbeitgeber stellt steuerlich einen geldwerten Vorteil dar, dem Werbungskosten des Arbeitnehmers gegenüberstehen. Wer haftet bei Schäden oder Verlust der Hardware oder von Daten oder bei Lizenzverstößen? Wie wird die Endgerätesicherheit hergestellt (Firewall, Virenschutz, installierte Applikationen)? Wie kann das Unternehmen bei privater Festplattenverschlüsselung auf seine Daten zugreifen? Was geschieht mit den Daten beim Ausscheiden des Mitarbeiters?

Laut Stefan Strobel, Geschäftsführer der Firma *Cirosec (www.cirosec.de)* bedarf es in diesen Fällen einer eingehenden Risikoanalyse und der Entwicklung von Konzepten.

Sichere Smartphones. Ein Lösungsmodell für die aufgezeigten Probleme, vor allem, was die sichere Trennung von betrieblichen und privaten Daten auf Smartphones betrifft, hat nach *T-Systems* mit *SiMKo3* vorgestellt *(www.tsystems.de/-simko)*.

Für Smartphones mit dem Betriebssystem Android wurde ein *Linux* basiertes Betriebssystem mit L4-Mikrokern (Hyperviser Typ 1) entwickelt, das eine virtuelle Welt von mehreren parallel arbeitenden Android-Systemen auf dem Smartphone darstellt.

Mit diesem Gerät wird eine gesicherte verschlüsselte Verbindung auch mit Sprachverschlüsselung aufgebaut und es können nach Personalisierung durch das Unternehmen sensitive Daten gesichert mobil synchronisiert, bearbeitet und abgelegt werden. Der offene Bereich steht nach wie vor mit Zugang zum Internet, sozialen Netzwerken sowie im App-Store zur Verfügung.

Für abhörsicheres, verschlüsseltes Telefonieren mit Smartphones bietet die Firma *Rohde&Schwarz* das hardware basierte Verschlüsselungssystem *TopSec Mobile* an. Als „Telefonhörer" fungiert ein etwa daumengroßes Gerät, das als Headset ausgestattet werden kann.

Dieses Gerät verschlüsselt die aufgenommene Sprache in sich und sendet die verschlüsselten Daten über eine Bluetooth-Verbindung zum Smartphone, das etwa durch eine Schutzhülle schallsicher abzudecken ist. Das Smartphone dient zum Verbindungsaufbau und zur Gesprächsabwicklung, wobei der Gesprächspartner in gleicher Weise mit dem Krypto-Gerät ausgestattet sein muss. Gegenüber einer Software-Verschlüsselung ist die Hardware-Lösung wesentlich sicherer.

Webseiten-Check. Eco, der *Verband der deutschen Internetwirtschaft e.V.,* hat mit der „Initiative-S" einen kostenlosen Webseiten-Check entwickelt, der vor allem für kleine und mittelständische Unternehmen gedacht ist, die sich keinen eigenen IT-Sicherheitsbeauftragten leisten können. Das Unternehmen meldet sich mit der zu überprüfenden Internet-Adresse und Bekanntgabe der eigenen E-Mail-Adresse unter *www.initiative-s.de* an, worauf der Webauftritt des Unternehmens

IT-SA 2012

IT-Sicherheitsmesse

Die IT-Sicherheitsmesse IT-SA ist die größte IT-Sicherheitsmesse im deutschsprachigen Raum und wird mittlerweile mit derartigen Messen in London *(Infosec)* und San Francisco *(RSA-Conference)* verglichen.

Es waren 334 Aussteller aus 50 Ländern vertreten. 6.100 Fachbesucher, dem Charakter einer B2B-Messe entsprechend, wurden gezählt.

Auf Fachforen (Forum Rot für IKT-Management; Forum Blau für Technik; allgemeine Sicherheitsfragen Auditorium) wurden rund 250 Vorträge geboten, die im Internet unter *www.IT-SA.de,* Forenprogramm, als Videostream und/oder Handouts abrufbar sind. In Live-Hackings wurde die Notwendigkeit aufgezeigt, sich entsprechend vor Angriffen zu schützen. Für den eiligen Besucher waren Handzettel mit Topic Routes vorbereitet: Auf Hallenplänen waren jeweils jene Aussteller markiert, deren Geschäftsfeld sich im Besonderen unter bestimmten Schwerpunkten wie etwa Datenschutz, Authentifizierung, Cloud/Mobile Security, Awareness, bewegt. *Campus@IT-SA* bot Hochschulen und Bildungseinrichtungen Gelegenheit, sich zu präsentieren.

Als Neuheit wurde der dreitägige *Congress@IT-SA* mit seinen fünf Themenkreisen angeboten, bei dem mit unabhängigen Fachleuten Themen wie Cloud Computing, Mobile Security oder BYOD erörtert wurden.

FOTOS: KURT HICKISCH

von Sicherheitsexperten des Vereins auf Schadprogramme untersucht wird. Das erfolgt automatisiert in regelmäßigen Abständen, im Schnitt etwa einmal in der Woche.

Wird eine Infektion entdeckt, wird per E-Mail darüber informiert und es werden Informationen zur Beseitigung des Schadprogramms und Hilfestellung dabei durch Anweisungen und Tools geboten. Ferner stehen Experten für Rückfragen zur Verfügung. Wenn der Schadcode beseitigt wurde, erhält das Unternehmen eine Bestätigung darüber, verbunden mit Hinweisen zur weiteren Prävention. Besteht die Infektionsgefahr weiter, wird das Unternehmen darüber ebenfalls verständigt und zugleich auch der Provider.

Mit dieser Initiative, die in den ersten drei Wochen bis zur *IT-SA* schon 3.500 Registrierungen verzeichnen konnte, soll erreicht werden, dass Webseiten von Unternehmen nicht ihrerseits zur Gefahr für andere werden, sei es durch die Verbreitung von Viren oder Trojanern, oder dass sie Teil eines Botnetzes werden, von dem aus Spam- und Phishing-Mails versendet oder andere Rechner lahmgelegt werden (dDOS-Attacken). Es geht auch um Haftungsfragen. Weiterhin angeboten wird von *eco* auch das DE-Cleaner-Rettungssystem mit der Anti-Bot-CD.

Cyber-Awareness. Mit „Datenschutz geht zur Schule“ hat der Berufsverband der *Datenschutzbeauftragten Deutschlands (BvD) e.V. (www.bvdnet.de)* eine Initiative ins Leben gerufen, die Kinder und Jugendliche für die Chancen und Risiken der Nutzung der Informations- und Kommunikationstechnik sensibilisieren soll. Etwa 40 Mitglieder des Vereins halten ehrenamtlich an Schulen

Cornelia Rogall-Grothe: „In Deutschland ist die Hälfte der Unternehmen vom Internet abhängig.“

Dieter Kempf: „Das BSI ist nicht verpflichtet, nach einem gemeldeten Angriff Ermittlungen aufzunehmen.“

Horst Flätgen: „Vertrauen in die neuen Technologien ist die Grundvoraussetzung für deren Anwendung.“

Vorträge unter anderem zum sicheren Umgang mit Daten in sozialen Netzwerken. Kinder und Jugendliche sind zwar bestens vertraut mit der Bedienung der Oberflächen ihrer PCs und Smartphones, ihnen fehlt aber das nötige Hintergrundwissen.

Bewusst gemacht werden sollen die Folgen davon, dass das Internet nichts „vergisst“ und dass immer Spuren zurückbleiben; dass auch andere mitlesen können; dass Identitätsdiebstahl möglich ist und dass durch Fehler in der Konfiguration ungewollte Effekte eintreten können. Die Vorträge sind kostenlos. Bisher wurden 25.000 Schüler in fast allen deutschen Bundesländern erreicht. Hingewiesen wurde in diesem Zusammenhang auf den für Lehrer unter *www.internauten.de* entwickelten Medienkoffer.

Kurzvorträge. Beim *DsiN MesseCampus* schlug der Verein *Deutschland sicher im Netz e.V. (DsiN; www.sicher-im-netz.de)* unter anderem vor, dass zehn Prozent der Vorlesungszeit an Hochschulen dem Thema IT-Sicherheit gewidmet sein sollten.

Prof. DI Udo Kalinna der Hochschule Emden/Leer erörtete die Sicherheit von Passwörtern aus mathematischer Sicht, wobei sich ergibt, dass es vor allem auf die Länge von Passwörtern ankommt und weniger auf den verwendeten Zeichenvorrat. Bei einem gegebenen Zeichenvorrat steigt die Anzahl der möglichen Kombinationen mit der Länge des Passworts. Die Vergrößerung des Zeichenvorrates, etwa durch Einfügung von Sonderzeichen, bringt in Bezug auf die Sicherheit gegenüber Wörterbuch- oder Brute-Force-Angriffen weniger als die Verlängerung des Passwortes.

Sogar die „Höchstlebensdauer“ eines Passwortes lässt sich, unter der Annahme eines in Kauf zu nehmenden Risikos, berechnen *(http://zuse.et-inf.fho-emden.de/rechne.php)*. Kalinna empfiehlt, einen selbst gewählten Satz entweder zur Gänze als Passwort zu verwenden, oder die Anfangsbuchstaben eines jeden Wortes dieses Satzes, unter Berücksichtigung der Groß- und Kleinschreibung sowie enthaltener Sonderzeichen. Selbst bei großer Rechenleistung würde dann die Entschlüsselung durch kombinatorische Methoden rasch in den Bereich von Milliarden von Jahren kommen. Wörterbuch-Attacken scheitern bei Verwendung von Dialektwörtern als Passwörter.

Facebook wäre mit einer Milliarde Menschen nach China und Indien das drittgrößte „Land“, erläuterte Prof. Dr. Norbert Pohlmann vom *Institut für Internet-Sicherheit – if(is) (www.internet-sicherheit.de)* der Westfälischen Hochschule Gelsenkirchen. Im Durchschnitt hat jeder User 229 Freunde, davon 7 Unbekannte. 300 Millionen Fotos werden pro Tag hochgeladen.

Facebook kann auch als Angriffstool verwendet werden, etwa durch gefälschte Fan-Seiten, die zu externen Webseiten führen, die Malware verbreiten. E-Mails, die sich als solche von *Facebook* ausgeben, können ebenfalls zu manipulierten Webseiten führen. Gegenüber „tollen“ Apps ist Misstrauen angebracht. Sie könnten den Zweck haben, persönliche Informationen (E-Mail-Adressen, Freundesliste) zu gewinnen und ein Profilbild zu erstellen. Ebenso sind Misstrauen und persönliche Nachfrage angebracht, wenn ein „Freund“ die Zusendung von Geld verlangt, weil er sich in einer Notlage befinden würde. Seine Identität könnte von einem Betrüger übernommen worden sein. *Kurt Hickisch*

Fotos: Kurt Hickisch