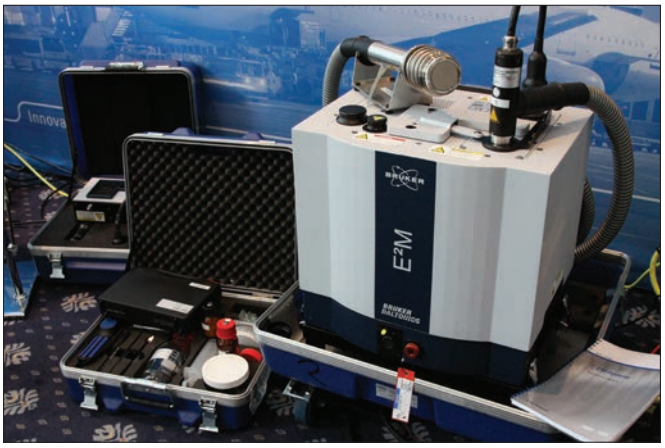
Erweiterter Dialog

Bedrohungssituationen und Abwehrmöglichkeiten waren Schwerpunkte beim VfS-Kongress 2012 in Leipzig. Dazu kamen Fachforen und eine Leistungsschau der Fachfirmen.

Mit der Sicherheitsbranche im Dialog zu sein, war der Leitgedanke des Kongresses des Verbandes für Sicherheitstechnik e. V. am 8. und 9. Mai 2012 in Leipzig. Den etwa 500 Teilnehmerinnen und Teilnehmern wurden 56 Vorträge geboten.

Die Bekämpfung des Terrorismus sei eine internationale Aufgabe. Mit einer nationalen Verfolgung könne der Friede nicht gewährleistet werden, betonte Rainer Griesbaum von der Generalbundesanwaltschaft Karlsruhe. Die Grenzen zwischen innerer und äußerer Sicherheit würden verschwimmen, wie auch die von Krieg und Verbrechen. Die Radikalisierung Einzelner erfolge zunehmend über das Internet. Der „einsame Wolf" handle außerhalb einer Organisation. Der Terrorismus habe sich verselbständigt. Der Dschihad werde auch im virtuellen Raum geführt. Angriffsziele seien die IT-Systeme von Wirtschafts- und Rüstungsbetrieben, Banken und des Verteidigungsministeriums.

Die Aufklärung des islamistischen Terrorismus, unter Einbeziehung der „Homegrown Networks", ist eine der Aufgaben des Bundesamts für Verfassungsschutz (BfV), über die Herbert Kurek vom BfV berichtet hatte. Zu diesen Aufgaben zählt die Abwehr von Cyber-Angriffen auf kritische Infrastruktur. „Die Verfügbarkeit des Cyber-Raums, die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten ist zu einer existenziellen Frage des 21. Jahrhunderts geworden." Eine weitere Aufgabe dieser Behörde ist die Abwehr von Wirtschaftsspionage. Zum Unterschied von der Konkurrenzspionage, die sich auf der Ebene einander konkurrierender Unternehmen abspielt, geht die Wirtschaftsspionage von Staaten aus. Bedroht ist der innovative Wissensvorsprung.



Massenspektrometer: Einsatz auch im Umwelt- und Gesundheitsbereich.

Schwerpunkte sind Leitindustrien wie IKT, Rüstungstechnologie, Luft- und Raumfahrt, Energie und Umwelttechnologie, Biotechnologie, Automobilbau, Automotive. Unternehmen sollten sich Gedanken machen, wo ihre „Kronjuwelen" liegen und wie diese zu schützen seien.

Die Frage, warum das Internet, das es schon seit 40 Jahren gibt, erst jetzt zum Problem wird, beantwortete Prof. Dr. Gabi Dreo-Rodosek von der Universität der Bundeswehr München damit, dass es mit Aufgaben belastet werde, für die es nie ausgelegt war. Auch Steuerungsanlagen laufen über das Internet-Protokoll, was Probleme mit den *Smart Grids* und beim *Smart Metering* aufwerfen könnte. Energie-Netze sind nicht so gut gesichert wie Datennetze. Es könnte Malware eingeschleust werden, die, etwa durch Vortäuschen einer zu großen Last zu einem Ausfall der Netze führen könnte. „Cyber-Abwehr kostet Geld; eine nicht adäquate Cyber-Abwehr kostet mehr."

Versorgungssicherheit.

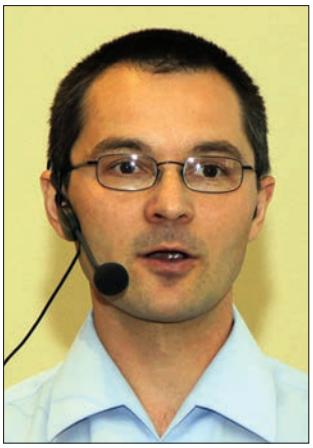
Der mögliche Ausfall der Stromversorgung und -netze („Lebensadern einer modernen Gesellschaft") war auch Thema des Vortrags von Herbert Saurugg von *Cyber Security Austria (www.cybersecurityaustria.at)*. 2010 musste jeder Stromkunde in Österreich im Durchschnitt ungeplante Stromausfälle in der Dauer von 32 Minuten in Kauf nehmen. In Deutschland waren es 19 und in der Schweiz 22 Minuten. Die längste Ausfallszeit gab es in Polen mit 386 Minuten. Die weitgehend in Erzeugung, Handel, Vertrieb, Transport und Verteilung aufgesplittete Energiewirtschaft werde durch den verstärkten Einsatz von Informationstechnologie noch angreifbarer, warnte Saurugg. Die zunehmende Vernetzung führe zu einer Steigerung der Komplexität, zu nicht linearen, instabilen Systemen und zu Rückkoppelungen, die sich verschieden auswirken könnten. Dass die europäische Energiewirtschaft die Stromversorgung in den vergangenen Jahrzehnten sehr erfolgreich betrieben habe, bedeute nicht, dass das auch in Zukunft so bleiben werde. „Fahren Sie nur mit Blick in den Rückspiegel vorwärts?", fragte Saurugg.

Das europäische Stromnetz wurde für einfach berechenbare Großkraftwerke geplant und errichtet. Nun aber sollen erneuerbare Energiequellen (Sonne, Wind) mit naturgemäß wechselnder Leistung eingebaut werden; durch den Einsatz von Informationstechnologie soll die Effizienz erhöht werden. Die aus der IKT-Welt bekannte Fehleranfälligkeit dieser Technologie könne zu einer Erhöhung der Verwundbarkeit der Stromversorgung führen. Aus den Fehlern der IKT-Welt müssten Lehren gezogen werden, wenn über *Smart Grids* die IT großflächig zum Einsatz komme. Durch erhöhte Fehlertoleranz wäre sicherzustellen, dass ein Fehler im System sich nicht auf dieses als Gesamtheit auswirkt. Die Versorgung von kritischen Bereichen sollte durch Abkoppelung vom allgemeinen Netz sichergestellt werden. In der derzeitigen Übergangsphase sollte man sich laut Saurugg auf Unsicherheiten in der Stromversorgung einstellen und Vorkehrungen für einen möglicherweise längeren Stromausfall treffen.

Christoph Unger, Präsident des Bundesamts für Bevölkerungsschutz und Katas-

FOTO: KURT HICKISCH

Jürgen Maurer: „Extremisten verfolgen Gerichtsprozesse genau und ändern dann ihre Taktik.“



Herbert Saurugg: „Kritische Bereichen sollte durch Abkoppelung vom allgemeinen Netz sichergestellt werden.“

Peter Reithmeier: „Der VfS thematisiert mit seinen 70 Mitgliedsfirmen Hochsicherheitstechnik.“

Herwig Lenz: „Die 794 Präventionsbeamten der Polizei haben 2011 337.161 Personen informiert.“

trophenhilfe (BBK), Bonn, bezeichnete einen Stromausfall von mehr als 24 Stunden als ernsthaftes Problem und bezog sich auf den Stromausfall in Italien am 28. September 2003 und den Wintereinbruch im Münsterland im November 2005. Ein Schneesturm hatte Strommasten geknickt, eine Viertelmillion Menschen waren tagelang ohne Elektrizität. In Deutschland sind die Bundesländer für den Katastrophenschutz zuständig; das Bundesamt koordiniert etwa bei Naturkatastrophen größeren Ausmaßes, Pandemien und seit 2004 auch zum Schutz kritischer Infrastruktur. Das Bundesamt ist seit 1. April 2011 in die nationale Cyber-Sicherheitsstrategie eingebunden. Zusammen mit dem BSI wurde am 30. November und 1. Dezember 2011 die IT-Notstandsübung LÜKEX (Länderübergreifende Krisenmanagementübung/Exercise) 2011 durchgeführt, bei der im Rahmen einer strategischen Stabsrahmenübung in fünf deutschen Bundesländern erstmals der Fall geübt wurde, dass durch das massive Auftreten eines IT-Schadprogramms die Telekommunikationssysteme, das Bankenwesen und die öffentliche Verwaltung lahmgelegt werden.

Cyber-Crime. Jürgen Maurer, Vizepräsident des BKA Wiesbaden, wies darauf hin, dass Extremisten Gerichtsprozesse genau verfolgen würden, was zur Aufklärung von Anschlägen geführt habe. Diese Erkenntnisse würden zur Schulung verwendet und hätten bereits dazu geführt, dass nicht mehr telefoniert, sondern Boten eingesetzt sowie Möglichkeiten der Verschleierung benützt würden. Dass in Deutschland die Vorratsdatenspeicherung noch nicht eingeführt worden sei, stelle ein Problem bei der Aufklärung von Straftaten dar.

Im Internet würden alle ein bis zwei Sekunden neue Schadprogramme auftreten; 13.000 infizierte Webseiten entstünden pro Tag neu im Netz. Zugangsdaten würden verkauft, es habe sich eine Underground Economy entwickelt. Mit Scareware werde vorgetäuscht, angebliche Fehler zu beheben.

„Botnetze sind die Schweizermesser für Kriminelle“ sagte Elmar Gerhards-Padilla, Leiter der Malware-Analyse am Fraunhofer FKIE, Bonn. Wer über ein solches Netz verfügt, könne beliebige Schadfunktionen einbringen, die in einer *Malware Economy* zu Geld gemacht werden. Der Schaden wird weltweit auf 388 Milliarden Dollar geschätzt. Die Bekämpfung der Netze wird erschwert, weil sie dezentral steuerbar sind. Die Löschung von Infektionen ist zwar im Einzelfall möglich, kann aber Auswirkungen auf die heterogene technische Landschaft haben, was Haftungsfragen aufwirft. Was passiert, wenn über einen Server in einem Krankenhaus der Rechner ausfällt?

Axel Allerkamp, Leiter der IT- und Informationssicherheit der *Axel Springer AG,* Berlin, stellte ein Computer-Programm zur Bewusstseinsbildung von Mitarbeitern für IT-Sicherheit vor. Das Programm bildet mit einer virtuellen Kunstfigur einen Tagesablauf ab, mit all den Risiken für die Sicherheit von Informationen, die als alltäglich und nicht mehr als Gefährdungen wahrgenommen werden.

Verbesserungsbedarf hinsichtlich des Datenschutzes bei sozialen Netzwerken sah Lars Konzelmann, Referent beim Sächsischen Datenschutzbeauftragten. Jedes Anklicken des „Like“-Buttons übermittelt die IP-Adresse, woraus sich in Summe Datenmuster ableiten lassen. Durch die Fülle der übermittelten Daten hat jeder Browser seinen eigenen Fingerprint. Das mit dem Anklicken verbundene Ablegen von Cookies auf dem Rechner des Nutzers sollte an eine ausdrückliche Zustimmung geknüpft werden. Datenlöschungen müssten auf Verlangen unverzüglich und vollständig erfolgen. Gesichtserkennung sollte nur nach ausdrücklicher Einwilligung des Betroffenen erfolgen dürfen.

Über datenschutzrechtliche Vorgaben beim Einsatz von Überwachungskameras referierte Rechtsanwalt Dr. Ralph Wagner vom Dresdner Institut für Datenschutz. Die derzeit im Entwurf vorliegende Datenschutz-Regelung der EU werde als direkt anwendbare Verordnung voraussichtlich die national bestehenden Datenschutzgesetze ablösen. 2014 soll die Verordnung in Kraft treten, mit einer Umsetzungsfrist von zwei Jahren.

Technik. Biometrische Erkennungssysteme wie Gesichts-, Iris-, Fingerabdruck-, Handflächen- und Venenerkennung boomen und werden allein in Deutschland bis zum Jahr 2015 einen Umsatz von über einer Milliarde Euro erreichen, bei einem jährlichen Wachstum von 25 Prozent, berichtete Dr. Xuebing Zhou vom *Center for Advanced Security Research Darmstadt (CASED).* Der

FOTOS: KURT HICKISCH

Vorteil der Biometrie liegt darin, dass sie eine direkte Verbindung zwischen dem Nutzer und seiner Identität herstellt. Biometrische Merkmale können nicht vergessen (Passwort), verloren (Token, Karte) oder weitergegeben werden. Die Daten sind einzigartig und unveränderbar – was allerdings auch bedeutet, das eine Kompromittierung dieser Daten in einer Anwendung nicht mehr rückgängig gemacht und solcherart Identität gestohlen werden kann. Ein Passwort kann gewechselt werden, ein Fingerabdruck nicht.

Technisch kann den Sicherheitsanforderungen bei Fingerabdrücken insofern entsprochen werden, als der Abdruck nicht als solcher gespeichert wird.

Über die Technik des Terahertz-Scanners und seine Anwendung zur Drogen- und Sprengstoffdetektion referierte Prof. Dr. René Beigang vom Fraunhofer IPM, Kaiserslautern. Terahertzwellen liegen der Wellenlänge nach zwischen der Mikrowelle und dem fernen Infrarot, bei einem Millimeter und darunter. In diesem Wellenbereich sind Materialien wie Kunststoffe, Papier, Keramik, Textilien, transparent. Halbleiter, Metalle und andere elektrische Leiter sind sehr starke Reflektoren. Drahtverbindungen werden erkennbar. Flüssigkeiten wie Wasser verursachen eine starke Absorption. Gesundheitlich sind diese Wellen unbedenklich. Sie bewirken keine Veränderung organischer Substanz und es sind keine besonderen Strahlenschutzmaßnahmen erforderlich.

Präventionsbus des Landeskriminalamts Sachsen.

Prävention. In Deutschland wird durchschnittlich alle zwei Minuten eingebrochen, nur jeder siebente Einbruch wird aufgeklärt. Dipl. Volkswirt Heiner Jerofsky bezifferte den für die Industrie entstehenden jährlichen Schaden durch Einbrüche mit rund 600 Millionen Euro. Dazu kommen jährlich über 13.100 vorsätzliche Brandstiftungen in Industriebetrieben, um Spuren zu verwischen. Die Sach- und Folgeschäden sind mitunter viel höher sind als der Wert der Beute. Die Prävention muss technische Vorkehrungen ebenso berücksichtigen wie organisatorische Abläufe (Einteilung in öffentliche, private und spezielle Sicherheitsbereiche) und den Einsatz professioneller Dienstleister.

Beginnend beim Perimeterschutz über die Außenhautsicherung bis ins Innere eines Gebäudes, sollte zuerst eine ausreichende mechanische oder mechatronische Sicherung erfolgen und darauf aufbauend eine elektronische Sicherung mit Einbruchs- und sonstigen Gefahrenmeldeanlagen, mit Zutrittskontrolle und Videoüberwachung.

Mag. Herwig Lenz, Leiter des Büros 1.6 (Kriminalprävention und Opferhilfe) des Bundeskriminalamts in Wien, stellte die gesetzlichen Grundlagen und den organisatorischen Aufbau der Kriminalprävention und der Opferhilfe in Österreich dar. Die 794 Präventionsbeamtinnen und -beamten der Polizei haben 2011 bei 45.687 Beratungen 337.161 Personen informiert.

Kurt Hickisch

FOTO: KURT HICKISCH

VERBAND FÜR SICHERHEITSTECHNIK

Hochsicherheit

Der 1994 gegründete Verband für Sicherheitstechnik e. V. mit Sitz in Hamburg ist eine Vereinigung von etwa 70 Unternehmen im Bereich der Sicherheitstechnik. Ziel der Verbandstätigkeit ist es, neue Bedrohungsszenarien aufzuzeigen, diese bewusst zu machen und technische Lösungsmöglichkeiten anzubieten. Angesprochen werden Anwender mit erhöhten bis Hochsicherheitsanforderungen, wie etwa Justizvollzugsanstalten, Flughäfen, Industrieunternehmen, Banken sowie öffentliche Institutionen wie Polizei und Verfassungsschutz. Durch Gesprächs- und Diskussionsrunden mit den Anwendern wird ein Dialog aufrechterhalten.

Diesem Zweck dient der jährliche Kongress mit Vorträgen über Sicherheitsthemen sowie einer Präsentation der neuesten technischen Entwicklungen der Mitgliedsfirmen. Weiters finden Fachtagungen und Fortbildungsveranstaltungen statt.

Publikationen. Der Verein ist Herausgeber der Handbücher *Elektroakustische Alarmierungseinrichtungen, Videotechnik, Gefahrenmanagement-Systeme, und Perimetersicherung*.

„Der VfS thematisiert mit seinen 70 Mitgliedsfirmen Hochsicherheitstechnik. Wir wollen jenen, die daran interessiert sind, einen Überblick über die Marktsituation geben“, erläutert VfS-Geschäftsführer Peter Reithmeier. „Dem dient die Ausstellung im Foyer während des Kongresses. In den Vorträgen soll der Blick geöffnet werden für das, was an Gefahren besteht oder noch auf uns zukommen wird, und was man dagegen tun kann.“

„Wir wollen Wissen über Hochtechnologien, über den letzten Stand der Technik, so präsentieren, dass Anwender damit etwas anfangen können. Sich für Produkte entscheiden müssen sie dann selber. Wir wollen auch helfen, Planungs- und Ausschreibungsfehler zu vermeiden, denn es kostet viel Geld, solche Fehler wieder zu beheben, die sich nachträglich herausstellen“, erläutert Reithmeier.“

Peter Reithmeier wechselt nach 20 Jahren als Geschäftsführer in den Vorsitz des VfS-Beirats. Als Geschäftsführer wird ihm Anfang 2013 Wilfried Joswig nachfolgen. „Mein Bestreben wird nach wie vor sein, die Anwender noch näher an den Verband heranzuführen und dessen Tätigkeit verstärkt nach Österreich, in die Schweiz und nach Luxemburg auszuweiten“, betont Reithmeier.

www.vfs-hh.de