

Sicherheitsexpertenpool

Parallel zur „Security“ in Essen hat der Security-Kongress stattgefunden, der erstmals von der SecuMedia GmbH mit einem neuen Konzept veranstaltet wurde.

Themenschwerpunkte des Kongresses waren Unternehmenssicherheit, neue Sicherheitstechnologien, Technologien gegen den Terror, Feuerwehr- und Löschtechnik sowie Brandschutz und Sicherheitsdienstleistung.

Sicherheitspartnerschaften. Angesichts der Bedrohung durch den Terrorismus wurde in einer Podiumsdiskussion die Frage von Sicherheitspartnerschaften diskutiert; sie wurden – mit unterschiedlichen Argumenten – einhellig als unverzichtbar bezeichnet. „In anderen Staaten neigt man zur Bildung einer Superbehörde“, meinte etwa der Vizepräsident des deutschen Bundeskriminalamts (BKA), Prof. Dr. Jürgen Stock. „In Deutschland errichten wir zu einer Problemstellung Netzwerke von selbständigen Einheiten.“

Konrad Freiberg, der Vorsitzende der Gewerkschaft der Polizei, sieht ebenfalls keine Alternative zur Zusammenarbeit, zumal sich die Polizei auf ihre gesetzlichen Prioritäten zurückziehen müsse. Verwechslungsmöglichkeiten zwischen Polizei und privaten Sicherheitsdiensten, etwa durch eine sich annähernde Art der Uniformierung oder bei den Dienstfahrzeugen, müssten allerdings verhindert werden.

Als Aufgaben der privaten Sicherheitsdienste im Rahmen einer sinnvollen Zusammenarbeit mit der Polizei bezeichnet Wolfgang Waschulewski, Präsident des BDWS, „Beobachten, Erkennen, Melden“. Carl Heinrich von Bauer, leiten-



Security-Kongress 2006: Experten referierten unter anderem über neue Möglichkeiten zur Bekämpfung des Terrors.

der Ministerialrat im Innenministerium Nordrhein-Westfalen, forderte die Verwaltung auf, sich auf die Wünsche der Wirtschaft einzustellen. Eine Messzahl sei die Inanspruchnahme der Beratungsstellen durch die Wirtschaft; diese Zahl sei im Steigen begriffen.

Wirtschaftskriminalität.

Von den rund 6,4 Millionen Delikten, die in Deutschland 2005 angezeigt wurden, sind zwar nur knapp 90.000 oder 1,5 Prozent der Wirtschaftskriminalität zuzuordnen. Der durch diese Delikte verursachte Schaden, mehr als vier Milliarden Euro, beträgt allerdings rund die Hälfte der gesamten erfassten Schadenssumme – was die Bedeutung dieser Art von Kriminalität deutlich macht.

Nach einer 2006 durchgeführten Studie der Wirtschaftsprüfungsgesellschaft KPMG zur Wirtschaftskriminalität in Deutschland waren in Deutschland in den letzten drei Jahren Unternehmen mit einem Umsatz bis 100 Millionen Euro in 19 Prozent der Fälle von

wirtschaftskriminellen Handlungen betroffen, Unternehmen mit einem Umsatz von 100 bis 500 Millionen zu 31 Prozent und solche mit mehr als 500 Millionen bereits zu 55 Prozent. Das ist das Hellfeld; die Unternehmen selbst schätzen, dass auf einen entdeckten Fall fünf unentdeckte kommen. Bei der Aufdeckung spiele der Zufall eine große Rolle; kriminalpräventiven Strategien komme große Bedeutung zu, erklärte Dieter John, Leiter des Bereichs Forensik bei KPMG.

Über jene Bereiche der Wirtschaftskriminalität, in denen Detekteien beauftragt werden, berichtete die Präsidentin des Bundesverbandes Deutscher Detektive, Eveline Wippermann. Dies reiche von Verletzungen des Patentrechts und Markenrechtes, Produkt- und Markenpiraterie, Diebstahl geistigen Eigentums oder von Know-how, Anlage- und Subventionsbetrug bis zu Computerkriminalität und Versicherungsbetrug. Einen breiten Raum nimmt die Aufklärung von Mitarbeiterdelikten ein, wie Verstöße

gegen Wettbewerbsverbote, Verrat von Geschäfts- und Betriebsgeheimnissen, Betriebsabotage oder un gerechtfertigte Fehlzeiten („Krankfeiern“). Werden Mitarbeiterdelikte von Angehörigen des Managements begangen, ist der Schaden wesentlich größer. Dazu kommt, dass diese Ebene von Kontrollmechanismen kaum erfasst wird. Bekannt werden solche Fälle eher durch die eifersüchtige Ehefrau, die verlassene Geliebte, missgünstige Kollegen oder dann, wenn krankheits- oder urlaubsbedingt eine Vertretung einspringen muss.

Dem Verkauf von gestohlenen Waren oder gefälschter Markenartikel im Online-Handel, rückt die r.o.l.a. Business Solutions GmbH (www.rola-solutions.de) unter anderem mit eigenen Analysemethoden und eigener Datenbank zu Leibe. Wenn Waren mit dem Zusatz „Keine Papiere“ angeboten werden, liegt der Verdacht auf gestohlenen Gut nahe, ebenso, wenn unter dem Einstandspreis angeboten wird.

Wenn leere Schachteln von Medikamenten wie *Via-gra* angeboten werden, wird das Verbot des Medikamentenhandels umgangen: Bei hergestelltem Kontakt werden die vollen Packungen verkauft. Von Markenprodukten wie teuren Uhren oder Parfüms kommen Fälschungen auf den Markt; der Missbrauchsumsatz bei Parfüms wird mit über 11 Millionen Euro oder 37 Prozent pro Jahr angegeben. Hinweise auf „fehlerhafte Produktion“ oder „Duftabweichungen möglich“,

„Kratzer, fehlerhafte Produktion“ sollten ebenso zu denken geben wie in Osteuropa angemeldete Nicknames, Schreibfehler oder bloß auf einen oder drei Tage beschränkte Laufzeiten der Angebote. Auch falsche Packungsgrößen kommen vor. Durch das automatisierte Auswerten relevanter Daten der Angebote lassen sich die unter verschiedenen Bezeichnungen und auf verschiedenen Plattformen auftretenden Anbieter letztlich auf einige wenige zurückführen, gegen die dann vorgegangen werden kann.

Unternehmenssicherheit.

Mitunter können intelligente Einfälle Probleme lösen, belegte Dkfm. Rainer von zur Mühlen durch Beispiele. Dem überhand nehmenden Ladendiebstahl in einem großen Einkaufszentrum in Nordrhein-Westfalen wurde durch den Einbau einer sich langsam drehenden Karuseltür als Eingangstür begegnet: Die Täter haben sich dadurch in ihrem Fluchtverhalten beeinträchtigt gefühlt; die Häufigkeitsquote beim Ladendiebstahl, zuvor die höchste im Land, ist daraufhin stark gesunken. Punker, die sich in Einkaufspassagen niedergelassen hatten, wurden durch Berieselung mit klassischer Musik gewaltfrei vertrieben; desgleichen Fixer aus Toiletten, in denen Licht mit hohem Blauanteil das Setzen der Nadeln erschwert hatte.

Auch Krisenbewältigung gehört zur Unternehmenssicherheit. Die Notwendigkeit zu entsprechenden Vorkehrungen kann sich auch insofern ergeben, als von der Versicherung bei Fehlen solcher Vorkehrungen Obliegenheitsverletzung geltend gemacht werden könnte. Oftmals stellt ein Problem auch die Wahrnehmung einer Krise dar, da in



Jürgen Stock plädiert für Sicherheitspartnerschaften.

Hierarchien die Tendenz besteht, Schwächen nach oben in immer abgeschwächter Form zu berichten, wogegen Stärken verstärkend kommuniziert werden. Ein Risk-Scanning soll helfen, Micro-Trends, die Risikopotenzial in sich bergen, möglichst frühzeitig zu entdecken.

Die Video-Überwachung

wird durch das Erkennen von Bewegungs- und Verhaltensmustern von Objekten (etwa Abstellen von Koffern oder Ansammlung von Personen) noch intelligenter werden; es wird durch entsprechende Bildanalyseverfahren und lernfähige Systeme möglich werden, unbedenkliche Objekte beispielsweise grün zu markieren, kritische gelb, alarmrelevante rot. Der Trend geht vom Bildverarbeiten zum Bildverstehen mit dem Ziel, Sicherheitspersonal vom bloßen Beobachten zu entlasten und für Entscheidungstätigkeiten freizuhalten.

Warensendungen können, bei entsprechender Ausstattung, mit den Möglichkeiten der Satellitenortung (GPS) auf ihrem Weg über Land mitverfolgt und mit Hilfe der vom Handy her bekannten GSM-Technologie auch in Räumen geortet werden. Die intelligente Transportbox (SmartBox) der Deutschen Post AG, die dies er-



Wolfgang Waschulewski: „Beobachten und melden.“

möglicht, weiß auch über ihren Inhalt Bescheid, überwacht dessen Zustand (etwa permanente Kühlung von Arzneimitteln), kommuniziert mit einem Control Center und schlägt sofort Alarm, wenn sie unautorisiert geöffnet wird.

IT-Sicherheit.

„Im Internet befindet man sich in einem Haifischbecken“, sagte der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Dr. Udo Helmbrecht, und verwies auf die vielfältigen Bedrohungen aus dem Netz.

Die organisierte Kriminalität bediene sich dieser Möglichkeiten bereits; „Dienstleistungen“ wie das Verschicken von Trojanern oder gezielte Attacken könne man bereits kaufen. Allerdings würden Schäden nur selten angezeigt: Von 5.000 Unternehmen, an die hierzu Anfragen gerichtet worden waren, antworteten 616; von diesen gaben lediglich 25 Prozent an, Anzeige erstattet zu haben.

An die 80 Prozent der Bedrohungen der IKT-Sicherheit können mit dem vom BSI entwickelten Grundschutz abgedeckt werden. Das Angebot des BSI, einer 1991 gegründeten Behörde mit etwa 500 Mitarbeitern, ist vielfältig und umfasst neben dem ständig aktualisierten Grundschutzhandbuch

(GSHB) den „Leitfaden IT-Sicherheit“ für Einsteiger, einen Kurs zur Anwendung des GSHB sowie die Software „GSTOOL“ zur Unterstützung bei der Anwendung des IT-Grundschutzes, ferner Musterrichtlinien und Beispielkonzepte. Online-Informationen werden über www.bsi-fuer-buerger.de und www.buerger-cert.de angeboten.

Bei Angriffen auf die Kommunikation und damit auf die Vertraulichkeit von Informationen müssen alle Abschnitte des Verlaufs der Kommunikation beachtet werden, vom Sender über das Kommunikationsmittel (Sprache, Licht, Luft, Leitungen, Papier) bis zum Empfänger.

Die modernen Kommunikationsmittel

bergen besondere Risiken, denen organisatorisch (Security Policies, Zutritts- und Besucherregelung, Verbot von Foto-Handys, Kontrolle von Datenträgern und anderes) und technisch (Verschlüsselung von Nachrichten und Netzwerken, physische Schutzmaßnahmen für gefährdete Räume, Firewalls, Filter u. a.) begegnet werden kann.

Mit der fortschreitenden Verbreitung der RFID-Technik könnte sich das Pervasive Computing zu einem Problemfeld entwickeln, weil über sie Prozesse in der Außenwelt direkt gesteuert werden können. Pervasive Computing ist die Vernetzung des Alltags mit Objekten, in die Mikroprozessoren „eingebettet“ sind. Wenn der Kühlschrank von selbst merkt, dass das Joghurt ausgegangen ist, und gleich nachbestellt, mag das als Erleichterung empfunden werden; anders schaut es etwa bei Implantaten für Tiere oder automatischen Identifikationssystemen für Menschen aus.



Postfach 190
1092 Wien
Tel.: 01/315 70 10 (Fax: DW 4)
www.iwoe.at

ALLGEMEIN BEEIDETER UND GERICHTLICH ZERTIFIZIERTER DOLMETSCHER UND ÜBERSETZER
(DEUTSCH, KROATISCH, BOSNISCH UND SERBISCH)

←····· ÜBERSETZUNGSBÜRO ·····→

Mag. Ivan MALČIĆ

A-4601 Wels, Maria-Theresia-Straße 9/2, Postfach 132
Mobil-Tel: 0664 / 402 46 07
Fax: 0 72 42 / 25 22 38
e-mail: mag.malacic@aon.at

MITGLIED DES ÖSTERREICHISCHEN VERBANDES DER GERICHTSDOLMETSCHER

RECHTSANWALT
DR. MICHAEL MATHES

Marc Aurel-Strasse 6
1010 Wien

Telefon: 01-512 51 51
Telefax: 01-513 87 71



Udo Helmbrecht: „Haifischbecken Internet.“



Rainer von zur Mühlen: „Mozart gegen Punker.“

TAT-Congress. Dem Thema „Technology Against Terror“ war eine eigene Sonderschau auf der Messe und ein ganztägiger Kongress gewidmet. Berichtet wurde unter anderem über das europäische Forschungsprogramm „Research for Security“, über die Detektion von terroristischen Kampfstoffen und Maßnahmen zum Schutz kritischer Infrastrukturen sowie zum Schutz von Gebäuden. Erstmals wird von der *Extremus Versicherungs AG*, Köln, eine Versicherung gegen Terroranschläge angeboten. Bei dieser Versicherungsanstalt handelt sich um einen Zusammenschluss von 16 namhaften deutschen Versicherungsunternehmen mit Unterstützung der deutschen Bundesregierung, um Großrisiken in Deutschland wieder versicherbar zu machen.

Nur für Insider. Eine Abendveranstaltung des Kongresses unter dem Titel „Hacker, Knacker und Spione“ am 11. Oktober war darauf angelegt, dass Referenten unter der Zusicherung der Vertraulichkeit der weitergegebenen Informationen, „Klartext“ sprechen konnten – der Saal war bis auf den letzten Platz gefüllt. Zugelassen waren nur hauptberuflich im Sicherheitswesen Beschäftigte.

Pressevertreter hatten zuvor eine Verpflichtungserklärung zu unterfertigen und sich bei einem Verstoß gegen diese zu einer an den Deutschen Kinderschutzbund zu zahlenden Vertragsstrafe von 5.000 Euro zu verpflichten.

Erörtert wurden unter der Moderation von Peter Hohl, dem Geschäftsführer der *SecuMedia Verlags GmbH*, die im Zusammenhang mit Funknetzen (WLANs) wieder zu bemerkende Renaissance der Gaunerzinken, dass man sich also beim „Wardriving“ durch Zeichen an Hausmauern auf nicht verschlüsselte Hot Spots aufmerksam machen kann. Von der *Deutschen Telekom AG* wurde demonstriert, wie Lausch- und Spähangriffe abgewehrt werden können. Sebastian Schreiber, Geschäftsführer der *SySS GmbH*, führte vor, mit welchen Tools und sonstigen Hilfsmitteln wie *Google*-Anfragen in fremde Netze eingedrungen werden kann und beispielsweise Preise von Online-Shops manipuliert oder drahtlose Kommunikationsverbindungen abgehört werden können. Steffen Wernéry von den „Sportsfreunden der Sperrtechnik“ zeigte die „nur relative Sicherheit“ mechanischer Schlösser auf.

Kurt Hickisch