

„Kriminalität 2.0“

Das gemeinsame Vorgehen gegen „Kriminalität 2.0“ und die „Underground Economy“ war der Leitgedanke des VfS-Kongresses 2014.

Mensch, Organisation und Technik sollen für sich und in ihrer Wechselbeziehung dargestellt werden“, umriss der Vorsitzende des *Verbandes für Sicherheitstechnik e.V.* (VfS; www.vfs-hh.de), Wilfried Joswig, das Ziel des VfS-Kongresses 2014, der am 8. und 9. April 2014 in Leipzig stattfand und von rund 400 Teilnehmern besucht wurde.

Andreas Baumann, Inspekteur der sächsischen Polizei, wies darauf hin, dass sich klassische Deliktfelder auch in der digitalen Welt wiederfinden, allerdings in veränderter Qualität. Straftäter nutzen die über *Skype* und soziale Netzwerke gegebenen vielfältigen Kommunikationsmöglichkeiten, Verschlüsselungsverfahren und die Anonymität über Internetcafés oder Anonymisierungsdienste.

Bei beinahe jeder Straftat werden IKT-Systeme eingesetzt. Die Sicherstellung und Auswertung dieser Systeme sei grundsätzlich erforderlich. Auch einfache Sachverhalte könnten zu komplexer Spurenlage führen.

„**Cyber-Kriminalität** hat das Potenzial zu Massendelikten und ist die perfekte Plattform dafür“, sagte der Präsident des deutschen Bundeskriminalamts, Jörg Ziercke. Cybercrime ist profitabel, erfordert wenig eigene Infrastruktur und es gibt entsprechende Tools.

Der Cyber-Raum ermöglicht Anonymität und die Trennung von realer und digitaler Identität. Gruppen können sich vernetzen; das Entdeckungsrisiko ist gering. Neue Tatbegehungsweisen



Mobiler Überwachungscontainer: Die Videoüberwachungsanlage wird mit Solarenergie betrieben.

haben sich entwickelt – etwa Flashmobs, um Opfer zu überfallen. Die Statistik verzeichnet in Deutschland 64.000 Fälle von Cybercrime im engeren Sinn, und in weiteren 34.000 Fällen war der Computer Tatmittel. Die Fallzahlen steigen stetig; das Dunkelfeld kann kaum erfasst werden, was mit der mangelnden Anzeigebereitschaft zusammenhängt.

Die Schätzungen des durch Cybercrime weltweit verursachten Schadens bewegen sich zwischen 100 bis 500 Milliarden Dollar jährlich. In der deutschen Statistik sind 43 Millionen Euro ausgewiesen. Zu dieser Zahl merkte Ziercke allerdings an, dass nach einer vom LKA Niedersachsen durchgeführten Befragung von 20.000 Personen über 16 Jahren nur 8,5 Prozent der Straftaten



Visierbeschlag: Schutz vor Manipulation des Schlosses.

angezeigt werden. Die Fall- und Schadenszahlen müssten wohl um den Faktor 10 erhöht werden. Nach einer Internet-Befragung der *IHK* melden nur sechs Prozent der Unternehmen auf sie verübte Angriffe. Das größte Schadenspotenzial haben Infrastruktursysteme, wobei nicht mehr die Frage ist, ob Angriffe erfolgen, sondern ob sie abgewehrt wurden. Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* verzeichnet auf Regierungsebene bis zu 2.000 Angriffe täglich.

Die Tätertypen reichen vom jugendlichen Einsteiger bis zu organisierten Kriminellen, Nachrichtendienstlern und Extremisten.

Die Angriffe von Nachrichtendiensten lassen sich anfänglich nicht von allgemeinen kriminellen Angriffen unterscheiden. Finanzagenten stellen ihr Privatkonto gegen eine Prämie für Geldwäsche zur Verfügung.

„Haktivisten“ geht es um zivilen Ungehorsam. Sie gehen virtuell auf die Straße und kämpfen gegen in ihren Augen bestehende Unge-

rechtigkeit. Sie dringen in Datenbanken ein und blockieren Unternehmen durch dDOS-Angriffe. Es geht ihnen darum, möglichst großen Schaden anzurichten.

Bei Betrug werden fremde Identitäten verwendet, um damit Barabhebungen und Einkäufe zu tätigen, oder nach Vorkasse die bestellten Waren nicht zu liefern. Erpressung erfolgt mit „Ransomware“ wie dem BKA-Trojaner, der den Computer sperrt und ihn erst nach Bezahlung eines „Lösegeldes“ (Ransom) freigibt. Ein Einzeltäter hatte mehr als 200.000 solcher Angriffe versucht, von denen über 32.000 erfolgreich waren. Derartige Schadprogramme werden wie im Franchising vertrieben.

Nachdem Unbekannte in die Abrechnungssysteme von Kreditkartenfirmen in zwei arabischen Staaten eingedrungen waren und die Limits von Bezahlkarten hinaufgesetzt hatten, wurden im Februar 2014 in einer weltweiten Aktion mit Blankokarten innerhalb von zwei Tagen 40 Millionen US-Dollar erbeutet. Zeitgleich wurden in 23 Staaten 17.000 Aktionen durchgeführt. In Deutschland betrug der Schaden bei 1.000 Abhebungen 2,5 Millionen Euro.

Ein Online-Schwarzmarkt für den illegalen Handel mit Drogen und Waffen hatte sich über das Portal „Silk Road“ entwickelt. Zahlungen wurden in Bitcoins geleistet, die vom Kunden auf ein Treuhandkonto eingezahlt wurden und erst nach der Lieferung dem Verkäufer übermittelt wurden. Bis zur Abschaltung des Systems Anfang Oktober 2013

betrug der Umsatz 1,2 Milliarden Dollar. Über 300 Kilogramm Suchtmittel und über 500.000 Ecstasy-Tabletten wurden gehandelt.

Virtuelle Zahlungsmittel eignen sich zur Geldwäsche, wobei das nationale Recht an seine Grenzen stößt. Bei „Liberty Reserve“ konnte man sich einkaufen, wobei ein Prozent der Transaktionssumme einbehalten wurde. Von 2006 bis zur Schließung des auf Costa Rica etablierten Unternehmens durch US-Behörden im Mai 2013 wurden 55 Millionen Transaktionen getätigt, mit einem Volumen von sechs Milliarden Dollar.

Das Internet ist das wichtigste Mittel zur Verbreitung ideologischer Propaganda. Indoktrinierung in Hinterzimmern oder mit Literatur, die unter der Decke gehalten wird, hat sich überlebt. Man wird mit Daten zugeschüttet – von Festplatten, Smartphones usw.

Die Polizei braucht Big-Data-Technologien, um mit dieser Fülle und auch mit fremdsprachigen Dateien umgehen zu können. Automatisierte, intelligente Sortierung ist gefragt, etwa durch Extraktion von Kfz-Kennzeichen oder Währungsbeträgen. Es muss die Möglichkeit geben, Daten zu spiegeln, damit Unternehmen während der Ermittlungen weiterarbeiten können. Zusätzliche Probleme schaffen Anonymisierungsdienste wie „Tor“ oder die Verlagerung von Daten in die Cloud.

Auf Geldwäsche und die Verlagerung von Delikten, speziell im Bereich der Suchtgiftkriminalität, sowie die in diesem Bereich verwendeten Bezahlsysteme Bitcoin und Liberty Reserve gingen auch Kriminaldirektor Dr. Michael Dewald vom BKA Wiesbaden sowie



Bitcoins: Die virtuelle Währung wird auch von Kriminellen genutzt.

Frank Dickel und Thomas Buortmes vom Landeskriminalamt Hessen ein. In Online-Spielen (*Second Life; World of Warcraft*) haben sich Währungen etabliert, die auf Börsen im realen Leben gehandelt werden.

Volker Wagner von der Deutschen Telekom AG referierte im Speziellen über Wirtschaftskriminalität. Wer Einblick in die Preispolitik eines Unternehmens erhält, in beabsichtigte Übernahmen von Unternehmen oder von Partnerschaften, über Top-Personalentscheidungen und neue Produkte, kann sich einen Wettbewerbsvorteil verschaffen. Als den „Juwelierladen der digitalen Welt“ bezeichnete Wagner Handy-Shops: Bei kleiner Masse haben Smartphones hohen Wert. Raubüberfälle auf Shops oder Lkws mit solcher Ladung könnten sich häufen.

Die Funktionsweise von Bitcoins erläuterte Joerg Platzer von der *Crypto Economics Consulting Group*. Dieses digitale Zahlungsmittel basiert auf einer verteilten Buchhaltung (Peer-to-Peer): Jeder weiß von jeder Zahlung jedes anderen, ohne Dazwischentreten anderer Instanzen wie etwa einer Bank. Bei einer Transaktion wird nach Überprüfung der digitalen Signatur des Zahlers über den Netzwerknoten allen anderen kryptogra-

fisch verschlüsselt, mitgeteilt, welcher Betrag an wen überwiesen wurde. Die Bitcoin-Menge ist mit 21 Millionen BTCs begrenzt. Eine zentrale Notenbank, die die Geldmenge reguliert, existiert nicht. Bitcoins werden bis zur achten Stelle nach dem Komma geteilt. (www.bitcoin.de; www.bitcoinkiez.de).

Sicherheitstheorie. „Was ist Sicherheit eigentlich?“ Diese Frage stellte Prof. Dr. Rita Haverkamp von der Eberhard-Karls-Universität Tübingen. Kann Sicherheit nur, wie es dem Wortsinn entspricht (se: ohne; cura: Sorge) negativ als frei von Sorgen definiert werden? Spielen nicht Lebensqualität, Lebenszufriedenheit, Glück und Vertrauen, also positive Werte, auch eine Rolle? Haverkamp ging auf die Diskrepanz zwischen der gefühlten und der gegebenen, in der Kriminalstatistik messbaren Sicherheit ein, wobei sie sich auf die vom Max-Planck-Institut 2012 durchgeführte Befragung von 2.525 Personen über Sicherheit und Lebensqualität in Deutschland bezog.

Die Entwicklung der Kriminalität in Deutschland macht 48 Prozent der Bevölkerung große Sorgen. Höher liegen nur die Sorgen um schadstoffbelastete Lebensmittel (52 %) und die zuneh-

mende Kluft zwischen Arm und Reich (73 %). Hinsichtlich der persönlichen Sorgen liegt mit 41 Prozent die Sorge, im Alter ein Pflegefall zu werden, an der Spitze. Opfer einer Straftat zu werden, macht 14 Prozent der Bevölkerung große Sorgen; Opfer eines Terroranschlags zu werden, liegt mit 10 Prozent am Ende der Skala. Vereinsamung (15 %), Unfall (16 %), Arbeitslosigkeit (21 %), finanzielle Situation (22 %), Kontaktverlust zu einer wichtigen Person (24 %), eine schwere Erkrankung (28 %), unzureichende finanzielle Altersversorgung (37 %) machen dem Einzelnen viel mehr Sorgen. Daraus lässt sich ableiten, dass im persönlichen Bereich Gefahren anders gesehen werden als auf der gesellschaftlichen Ebene.

„Unsicherheit empfinden und Furcht stehen in Abhängigkeit von den Maßnahmen, die man selbst treffen kann.“ Sicherheit wird dabei zunehmend als Ware gesehen, die man kaufen kann, sich aber auch leisten können muss. „Wir müssen lernen, mit Unsicherheit zu leben“, sagte Haverkamp vor allem im Hinblick auf eine vergreisende Gesellschaft und das mit zunehmendem Lebensalter steigende Unsicherheitsgefühl.

Dass die Gesellschaft verlernt habe, mit Risiko umzugehen, stellte auch Dr. Niklaus Oberholzer vom Schweizerischen Bundesgericht in Lausanne fest. Es bestehe die Tendenz, die Lösung gesellschaftlicher Probleme dem Strafrecht zu übertragen und dieses dadurch zu einer stumpfen Waffe zu machen.

Nach einer Phase des Zurückdrängens des Strafrechts bis etwa in die 1970er-Jahre scheine sich der Zeitgeist zu wandeln. Um dem Unsicherheitsgefühl in der Bevölkerung entgegenzutreten, wür-



Jörg Ziercke: „Cyber-Kriminalität hat das Potenzial zu Massendelikten.“

den in einer Form des Aktivismus neue Strafbestimmungen geschaffen. Je komplexer der Sachverhalt, umso mehr werde nach einfachen Lösungen gerufen. Polizei und Justiz sollten Sicherheit schaffen, die es aber so nicht geben würde. Im Straßenverkehr habe man sich auch nicht für eine Null-Toleranz entschieden. „Sicherheit ist nicht nur ein polizeitechnisches, sondern ein gesellschaftliches Problem.“ Strafrecht solle nur dort eingesetzt werden, wo es tatsächlich nötig ist und nicht andere, ganzheitliche Lösungen gefunden werden können.

Sicherheitspraxis. Auch die Architektur kann zur Hebung des Sicherheitsgefühls beitragen, schilderte DI Thomas Eckert (*Dömges Architekten AG, Regensburg*). Im öffentlichen Raum sind Übersichtlichkeit, Helligkeit und über diesen Raum ausgeübte soziale Kontrolle von Bedeutung. Angsträume sind Unterführungen und dunkle U-Bahn-Haltestellen, noch dazu, wenn diese Anlagen einen ungepflegten und verwahrlosten Eindruck machen. Lange und dunkle Autobahnunterführungen können vermieden werden, wenn zwischen den Richtungsbahnen Platz gelassen wird.

Parkhäuser sollten in das draußen ablaufende Leben



Thomas Eckert: „Architektur kann zur Hebung des Sicherheitsgefühls beitragen.“

eingebunden sein, sodass die Umgebung wahrgenommen und Geräusche von außen gehört werden können. Läden im Erdgeschoß vermitteln den Eindruck, nicht isoliert zu sein. Bei Gebäuden sollten frühzeitig die vor fremdem Eindringen zu schützenden Bereiche festgelegt werden, da nachträgliches Aufrüsten teuer werde.

Dass man sich neben der Kriminalität auch auf Extremwetterlagen, Hochwasser und Überschwemmungen einstellen wird müssen, machte Uwe Rogler vom TÜV Nord deutlich. Nach Prognosen wird die Niederschlagsmenge bis zum Jahr 2100 um bis zu 30 Prozent steigen. Rückschlagklappen der Abwasserkanalisation sollten überprüft und mobile Schutzwände vorgesehen werden.

Auch gegen Engpässe in der Stromversorgung sollte vorgesorgt werden, angesichts der Tatsache, dass es in Deutschland 2012 über 190.000 Versorgungsunterbrechungen ab einer Dauer von drei Minuten gegeben hat, wobei die durchschnittliche Nichtverfügbarkeit etwa 16 Minuten betragen hat.

Eine unterbrechungsfreie Spannungsversorgung sollte gewährleistet und Anschlüsse an eine zweite Netzeinspeisung geschaffen sowie Notstromaggregate bereitge-



Volker Wagner: „Handy-Shops sind die Juwelieläden der digitalen Welt.“

stellt werden. Eine Risikoanalyse sollte zu einem ganzheitlichen Schutzkonzept führen.

Was allerdings nützt ein Brandschutzkonzept, wenn der von einem Brandmelder ausgehende Alarm auf Personen weitergeleitet wird, die nicht mehr aktiv sind? Thomas Redmer vom LKA Sachsen berichtete über Erfahrungen aus der Brandursachenermittlung. Wegen nicht geschlossener Brandschutztüren brennen Hallen trotz Brandschutzmauern ab. „Brandgefährlich“ ist auch die Lagerung von Kartonaugen an der Außenseite von Supermärkten.

Produkte. Die in vier Vortragsreihen parallel laufenden, rund 60 zeitlich abgestimmten Vorträge waren von einer im Foyer abgehaltenen Produktschau mit 60 Anbietern von Sicherheitstechnik und -dienstleistern begleitet.

Mit dem mobilen Überwachungscontainer *Motibox* (www.motibox.de) war im Freigelände eine über Solarenergie betriebene, autarke und interaktive Videoüberwachungsanlage aufgestellt. Dallmeier präsentierte auch die Kameras zum Videoüberwachungssystem *Panamera* (www.panamera.com). Beim *KABA TouchGo* Schließsystem genügt es, den



Andreas Baumann: „Bei fast jeder Deliktsart werden IKT-Systeme eingesetzt.“

Transponder am Körper zu tragen. Das passende mechanische Schloss wird durch bloßes Berühren geöffnet. Somit können auch Zutrittsberechtigungen vergeben werden. Das System ist beispielsweise für Krankenanstalten geeignet.

Das GPS-Handy von *Soft-Clean* (www.softclean.net) ist nicht nur äußerst robust, sondern gibt im Notfall auch die GPS-Koordinaten durch, ebenso wie *TimeTrack* als kleinstes Ortungsgerät seiner Klasse.

Bei den manipulationsgeschützten Visierbeschlägen der Firma *Eckhardt Stedler & Partner OHG* (www.stedler-ohg.de) wird das zu schützende Schloss mit einem Beschlag umgeben und ist erst dann zugänglich, wenn eine Art Lade geöffnet wird. Die Besonderheit des vorgestellten Systems liegt darin, dass der Öffnungsmechanismus für diese Abdeckung nach außen keine beweglichen Teile aufweist. Die Steuerung erfolgt über Permanentmagnete, die sich sowohl im „Schlüssel“ als auch im Schloss befinden.

Das System wurde für Justizvollzugsanstalten entwickelt, um mutwillige Beschädigungen von Schlössern zu verhindern. Derzeit ist es in über 100 Justizvollzugsanstalten im Einsatz

Kurt Hickisch