16th European Police Congress

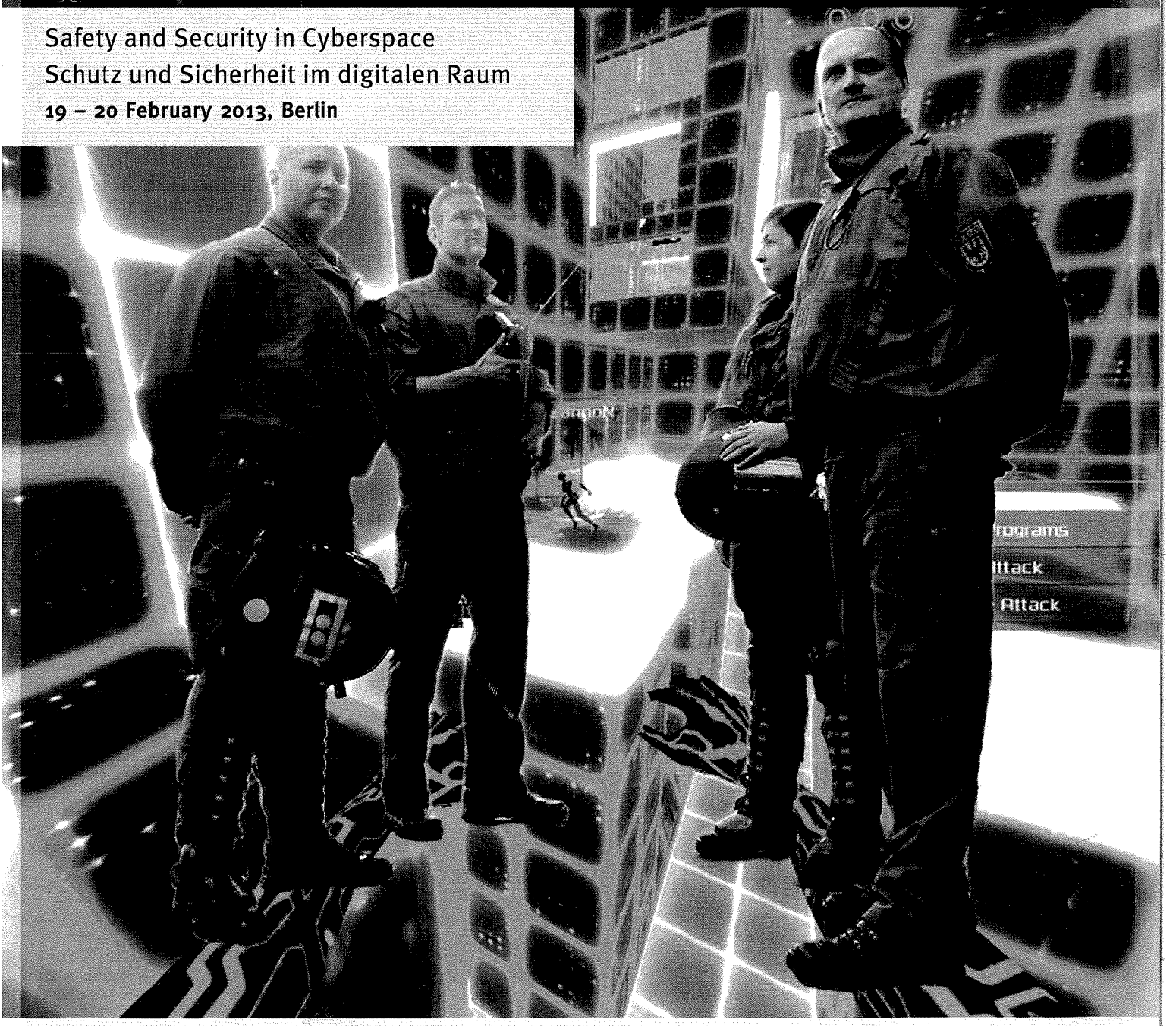
February 2013 7 Euro

EUROPEAN POLICE

MAGAZINE of the 16th EUROPEAN POLICECONGRESS

Safety and Security in Cyberspace
Schutz und Sicherheit im digitalen Raum

19 – 20 February 2013, Berlin



Europe's leading Conference for internal Security

ProPress Publishing Group
Berlin / Bonn / Vienna / Brussels

www.european-police.eu

Content / Inhalt 2013

Titelfoto: EP/Behörden Spiegel-Gruppe/verwendete Fotos: Kerstin Ginsberg, morguefile.com

Imprint

"European Police Magazine" is published by the ProPress Publishing Group Bonn/Berlin, Germany.
Editorial Director: Patricia B. Linnertz
Publisher: R. Uwe Proll
Editorial Board: Martin Jung, Patricia B. Linnertz
Publishing House: ProPress Verlagsgesellschaft m.b.H.

Headquarter Bonn:
Friedrich-Ebert-Allee 57, D-53113 Bonn
Phone: +49/228/97097-0
Fax: +49/228/97097-75

Berlin Office: Kaskelstr. 41, D-10317 Berlin
Phone: +49/30/557412-0
Fax: +49/30/557412-33
Brussels Office: Hartmut Bühl,
Avenue des Celtes, 30, B-1040 Brussels
Phone/Fax: +32/2732 3135
Austria Office: Salzburg Management Business School, Schloss Urstein, Schlossallee 9, A-5412 Puch/Salzburg
E-Mail: anmeldung@european-police.eu
Layout: SpreeService- und Beratungsgesellschaft m.b.H. Berlin, Birte Schulz

Print: SZ Offsetdruck-Verlag, Sankt Augustin
The European Police Magazine is published by the ProPress Publishing Group, who organizes the European Police Congress (contact: Martin Jung), the Congress on European Security and Defence (contact: Reimar Scherz) and the European Congress on Civil Protection and Disaster Management (contact: Verena Müller).
For further information about the magazine and the congress please visit www.european-police.eu
Copyprice is 7 Euro.

3M Deutschland GmbH
Government Markets · Behörden & Bundeswehr

Öffentliche Sicherheit

Details entscheiden

Innovative Schutzlösungen für Ausbildung und Einsatz

- **Elektroakustischer Gehörschutz:**
  ProTac II, Tactical XP und ComTac XP sind nach der Technischen Richtlinie der Polizei (TR) "Gehörschützer für das Schießen" zertifiziert und vom Polizeitechnischen Institut (PTI) der Hochschule der Polizei (DHPol) für den Polizeieinsatz freigegeben. Sie bieten erstklassigen Tragekomfort, Gehörschutz und Kommunikationsfähigkeit.
- **Nichtlinearer Gehörschutz:**
  Impulsschallgehörschutzstöpsel (ISGS) - garantiert verbale Verständigung, neutralisiert gleichzeitig Lärmspitzen.
- **Passiver Gehörschutz:**
  der bewährte EAR Classic II Hörstöpsel oder verschiedene Kapselgehörschutz-Lösungen.
- **ComTac XP + EAR Classic II im Plug Modus:**
  Höchste Dämmung bei voller Kommunikationsfähigkeit.
- **Ballistische Schutzbrillen:**
  die Maxim Ballistic, 180° verzerrfreie Scheiben, beidseitige DX-Beschichtung gegen Beschlagen und Verkratzen.
- **Ballistischer Körperschutz:**
  Borcarbid von ESK – Superleichte Keramikplatten zum Schutz von Einsatzkräften.

3M-Technologie: Alles hören außer Lärm

www.3M-Behoerden.de

3M Deutschland GmbH · Government Markets
Behörden & Bundeswehr
Carl-Schurz-Straße 1 · D-41453 Neuss
Tel.: +49 (0) 2131/14-24 41 · Fax: +49 (0) 2131/14-12 24 41
E-Mail: Behoerden@mmm.com

3M

Der digitale Tatort

R. Uwe Proll
Herausgeber und Chefredakteur,
Behörden Spiegel

Fast alle Formen der Kriminalität finden sich heutzutage im Netz wieder: Warenbetrug, Diebstahl, Spionage, Angriffe auf Kritische Infrastrukturen (KRITIS). Hinzu kommen neue, also Internet-genuine, Kriminalitätsformen wie etwa Botnetz- und DDoS-Attacken, das Abgreifen und Ausspionieren von Daten und Informationen im E-Mail-Verkehr, Phishing oder auch das Verbreiten von Schadsoftware.
Mit den veränderten, digitalisierten wie auch neuen Kriminalitätsformen entstehen auch neue Aufgabenfelder für die Polizei. Dieser Entwicklung wurde bereits Rechnung getragen. In einigen Landeskriminalämtern (LKAs) sind bereits Cyber-Abteilungen entstanden und eigene Strategien werden entwickelt. Aber reicht das aus? Verlangt die digitale Bedrohung nicht neue Strukturen anstatt nur einfach einer neuen Aufgabenverteilung?
Und wo ist die Gefahr aus dem Cyber-Raum, die nicht nur auf polizeiliche Bedrohungslagen zu reduzieren ist, adäquat ressortiert?
Auf Bundesebene existiert das Bundesamt für Sicherheit in der Informationstechnik (BSI). Werden solche Strukturen auch auf Landesebene benötigt, also Landesämter für IT-Sicherheit (LSI)?

Plattform für Verbrechen – mit oder ohne die Polizei?

Wie keine andere Kriminalitätsform kennt die Cyber-Kriminalität keine Grenzen. Wo also sollte der Kampf gegen den digitalen Tatort geführt werden? Europa und Interpol haben eine Antwort bereits gegeben. Mit dem European Cybercrime Centre (EC_3) bei Europol und dem Interpol Global Complex for Innovation (IGCI) wurden neue Instrumente geschaffen, die sich auf dem 16. Europäischen Polizeikongress erstmals in Deutschland vorstellen.
Doch welche Instrumente, sowohl personell als auch technisch, braucht die Polizei, um im Kampf gegen die Cyber-Kriminalität auf digitaler Augenhöhe zu sein?
Zudem bietet das digitale 21. Jahrhundert nicht nur neue Bedrohungen und neue Herausforderungen, sondern auch neue Chancen, etwa der Kommunikation via Facebook. Soziale Netzwerke sind heute aber auch eine Plattform für Verbrechen. Wo Menschen zusammenkommen, gibt es Verbrechen. Doch einen fahndungsfreien Raum darf es nicht geben! Das Internet ist ein Raum für viel Informationen, eben auch krimineller Aktivitäten, aber daher auch eine enorme Quelle. Wir brauchen die Fahndung per Facebook. Doch welcher Rechtsrahmen ist für die verdeckte Aufklärung in Facebook notwendig?

Diesen und anderen Fragen sowohl der Sicherheit und des Schutzes im digitalen Raum widmet sich der 16. Europäische Polizeikongress, den der Behörden Spiegel auch in diesem Jahr wieder mit Unterstützung des Bundesministeriums des Innern (BMI), des Bundeskriminalamtes (BKA), des Bundesamtes für Verfassungsschutz (BfV), der Cyber Akademie (CAk) und anderer internationaler Partner durchführt.

Zukunft bauen und Exzellenz fördern

Der Europäische Polizeikongress richtet seinen Blick in diesem Jahr verstärkt in die Zukunft. Die Cyber Akademie wird vorgestellt. Sie bildet in verschiedenen Seminaren zukünftige Experten für den Cyber-Raum aus und weiter. Daneben wird erstmalig in diesem Jahr auch die Nachwuchsarbeit der Polizei gefördert.
Mit dem 1. Zukunftspreis Polizeiarbeit "Soziale Netzwerke" werden herausragende Abschlussarbeiten von Studenten ausgezeichnet, die innovative Ideen und Lösungen für die polizeiliche Arbeit bieten.

Wir wünschen nicht nur angenehme Tage in Berlin, sondern auch vor allem gute Gespräche und – das Wichtigste: neue Erkenntnisse und Kontakte.

R. Uwe Proll
Herausgeber und Chefredakteur, Behörden Spiegel

The Digital Crime Scene

Virtually every form of crime has an online pendant these days: fraud, theft, espionage, attacks on critical infrastructures. And then there are new forms of crime that are unique to the internet such as botnet and DDOS attacks, the tapping and spying out of data and information in email traffic, phishing, or also the distribution of malware.
These changed, digitalized and new forms of crime also open up new task areas for the police. This development has been addressed. A number of State Offices of Criminal Investigation have already established cyber departments with their own specific strategies. But is that enough? Doesn't the digital threat call for new structures, instead of simply reallocating the tasks?
And which department is adequately responsible for cyber threats that are not only reducible to the kinds of threat usually handled by the police?
On a federal level, there is the Federal Office for Information Security. Are structures such as this also required on a "Länder"- level, i. e. State Offices for IT Security?

The highlight is every year the discussion with the Ministers of Interior from the German Länder.

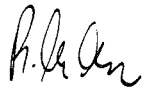
A Platform for Crime – With or Without Police?

Cybercrime knows even fewer boundaries than other forms of crime. So where exactly should a campaign against the digital crime scene be fought? Europe and Interpol have already provided an answer. The newly created European Cybercrime Centre (EC3) at Europol and the Interpol Global Complex for Innovation (IGCI) are new instruments that will be introduced in Germany for the first time at the 16th European Police Congress.
But what would be the right instruments for the police, in staffing as well as technical terms, to ensure an equal digital footing in the fight against cybercrime?
The digital 21st century not only harbours new threats and challenges, however, but also new opportunities, for example in the communication on facebook. Social networks have also become a platform for crime these days, alas.
Crime will occur wherever people congregate. But there must be no such thing as an unpoliceable space! The internet has room for plenty of information, but also for criminal activities, as it were, and is hence an enormous source. We do need policing on facebook. But what would the regulatory framework for undercover policing on facebook need to look like?

These and other questions concerning safety as well as protection in cyberspace will be addressed this year by the 16th European Police Congress, once again organized by Behörden Spiegel with the assistance of the Federal Ministry of the Interior, the Federal Criminal Police Office, the Federal Office for the Protection of the Constitution, the Cyber Akademie, and further international partners.

Building a Future and Promoting Excellence

This year's European Police Congress will place a greater focus on looking ahead to the future. Cyber Akademie will be training future cyberspace experts in many different seminars. Besides this, the promotion of young talent for the police force will also receive a boost for the very first time this year.
The 1st Police Work Future Prize "Social Networks" is being awarded to honour outstanding final student papers advancing innovative ideas and solutions for police work.
We wish you a pleasant stay in Berlin, but even more so a lively exchange, and most importantly: new insights and contacts.



R. Uwe Proll
Publisher and Chief Editor, Behörden Spiegel

PAN AMP®

INTERNET | SECURITY | SOLUTIONS

16th European Police Congress

INTERNET & DEEP INTERNET® FORENSIC

PAN AMP AG, panamp.de

19.- 20. February 2013,
bcc, 4b, Berlin, Germany

INTERNET & DEEP INTERNET® FORENSIC

ROBOT TECHNOLOGY® die automatische Fahndung und Recherche nach relevanten Datensätzen durch selbständig agierende Robots, die das Internet und das DEEP INTERNET® analysieren.

REPORT TECHNOLOGY® analysiert automatisch System - und Servereigenschaften im Internet und DEEP INTERNET® und erstellt automatisiert einheitliche Dossiers für Fall-Bearbeitungs-Systeme.

ONLINE EVIDENCE® dient der Sofortsicherung von flüchtigen Beweisen in Datennetzen und dem DEEP INTERNET®. Im Observer-Modus überwacht die ONLINE-EVIDENCE® fortlaufend Standort-, Inhalts- und Konfigurationsveränderungen des Zielsystems.

PANTRACK TECHNOLOGY® beinhaltet Systeme zur Ortung von Internet-PC`s und Online-Devices, die durch eine Rückverfolgung der Datenströme die verwendete Hardware lokalisieren kann.

PAN AMP AG

PAN AMP ist als Hersteller von Hochleistungs-Filter und Forensik-Technologie ein weltweit tätiges Unternehmen mit hoher Technologiekompetenz im Bereich der Daten-Filterung und der Forensik. Von dem Tor zur Welt, der Hansestadt Hamburg aus entwickelt und vertreibt PAN AMP wegweisende Lösungen für die sichere Nutzung und das Management von Inhalten in Datennetzen und Forensik-Technologien mit künstlicher Intelligenz. PAN AMP verfügt über eine weltweit einzigartige technische Lösung zur automatisierten Lokalisierung im Internet und DEEP INTERNET® von Extreminhalten, Extremismus, Terrorismus und Bombenbauanleitungen.

PAN AMP entwickelt Technologien und Systeme zur Verteidigung des virtuellen Raums. Der Schwerpunkt in der weiteren Forschung und Entwicklung liegt in der Absicherung nationaler Teilnetze und in der Beratung zur Weiterentwicklung von staatlicher IT und Infrastruktur. Hierdurch unterstützt PAN AMP Staaten, die effektive Gegenmaßnahmen zur Verteidigung des virtuellen Raumes aufbauen.

Europas Antwort auf Cybercrime

Schutz und Sicherheit im digitalen Raum

(EP/lin) "Cybercrime ist eigentlich nichts Neues. Es ist nur eine neue Definition von Kriminalität, die mit anderen Mitteln verübt wird." Peter Vahrenhorst, Cybercrime-Kompetenzzentrum des Landeskriminalamtes (LKA) Nordrhein-Westfalen, eröffnete im September letzten Jahres das Diskussionsforum "Herausforderung Cybercrime" des Behörden Spiegel in Kooperation mit BITKOM auf der security essen 2012.

Cybercrime, die neue Dimension der Kriminalität, stellt die Polizei vor große Herausforderungen. Foto: EP/MIK NRW

Delikte wie Warenkreditbetrug, Beleidigung, Mobbing, Kinderpornografie, Schutzgelderpressung und Wirtschaftsspionage würden im Internet nur "anders" ausgeführt. Das Internet habe aber auch neue Deliktsfelder entstehen lassen: Skimming, Phishing, Carding, Schadsoftware, Botnetze, DDoS-Attacken, Account Takeovers und die Underground Economy seien hierfür nur einige Beispiele.

"Diese neuen Phänomene entwickeln sich stetig weiter, sie sind flexibel, dynamisch und vor allem anonym", so Vahrenhorst. Außerdem hätten sich mit dem Internet neue Tätertypologien ergeben. "Im Internet herrscht ein großes Gefahrenpotenzial. Es herrscht aber leider auch ein hohes Dunkelfeld über begangene Straftaten und Delikte", so Vahrenhorst weiter. Daher sei der optimale Informationsaustausch sowie Zusammenarbeit und Kooperation zwischen der Wirtschaft und Industrie sowie den Behörden und Organisationen mit Sicherheitsaufgaben das Ziel zur Bekämpfung der Internetkriminalität.

Die Polizei stehe dabei vor zwei großen Herausforderungen: "Wir brauchen eine flächendeckende Grundkompetenz hinsichtlich Cybercrime bei der Polizei, aber eben auch spezielle Fachkompetenz", so Vahrenhorst.

Kriminalität und vor allem auch Organisierte Kriminalität im Internet sind dabei allerdings keine nationalen Probleme und Herausforderungen. Cybercrime kennt keine Landesgrenzen.

Europas Antwort auf Cybercrime

Cyber-Kriminalität, wie der Diebstahl von Kontodaten, falsche Onlineshops, das Hacken von Smartphones und groß angelegte koordinierte Angriffe auf öffentliche Infrastrukturen, nimmt verstärkt zu. Kreditkarteninformationen lassen sich über scheinbar von der Bank stammende E-Mails einholen und werden dann unter organisierten kriminellen Vereinigungen für einen Euro pro Karte weiterverkauft. Hacker starten Angriffe gegen Unternehmen, um an Geschäftsgeheimnisse zu gelangen.

"Nur wenige Straftaten dieser Art werden der Polizei gemeldet und noch weniger werden aufgeklärt. Die einzelnen Mitgliedsstaaten der Europäischen Union haben unterschiedliche Erfahrungen gesammelt, aber grenzübergreifende Zusammenarbeit findet nur selten statt. Daher macht die Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyber-Kriminalität Sinn", sagt die EU-Kommissarin für Inneres, Cecilia Malmström.

Als Antwort auf die stetig steigende Kriminalität im Internet wurde das European Cybercrime Centre (EC3) bei der europäischen Polizeiagentur Europol in Den Haag eingerichtet. Seit Anfang Januar 2013 hat das EC3 seine Arbeit aufgenommen. Das Zentrum soll der Fokus der Europäischen Union im Kampf gegen Cyber-Kriminalität werden. Es soll die Mitgliedsstaaten der Union und deren Einrichtungen durch den Aufbau operativer und analytischer Kapazitäten für Ermittlungen und Kooperationen mit internationalen Partnern unterstützen. Zudem soll das EC3 als Informationsbasis über Cybercrime in der Europäischen Union dienen. Daneben soll auch ein Netzwerk von Experten aus verschiedenen Sektoren aufgebaut werden, das gegen Cybercrime und Kinderpornografie kämpfen und präventiv vorgehen soll. Die Einrichtung des Zentrums werde im Kampf gegen Cyberkriminalität der EU einen Meilenstein setzen, sagte Rob Wainwright, Executiv Direktor Europol.

Angesichts der technischen Möglichkeiten des 21. Jahrhunderts sei es nun an der Zeit, dass die Sicherheitsbehörden einen Schritt voraus seien. Mit der Unterstützung der Mitgliedsstaaten, der Einrichtungen der EU, internationalen Partnern und des Privaten Sektors werde das European Cybercrime Centre die Europäische Union im Kampf gegen die Internetkriminalität mit den Worten Wainwrights "schlauer, schneller und stärker" machen.

Globales Zentrum für Innovationen

Aber nicht nur die deutschen Sicherheitsbehörden und die europäische Polizeiagentur Europol reagieren auf die zunehmende Bedrohung aus dem Cyber-Raum. Internetkriminalität ist ein globales Phänomen und Problem. Gegen die neuen Bedrohungen des 21. Jahrhunderts braucht die Polizei auch neue Instrumente. Sie braucht Echtzeit-Zugang zu Informationen, die über ihre eigenen Grenzen hinausgehen.

Mit dem INTERPOL Global Complex for Innovation (IGCI) will INTERPOL der Polizei weltweit Werkzeuge und Fähigkeiten im Kampf gegen die neue Bedrohungslage zur Verfügung stellen. Das IGCI ist eine Forschungs- und Entwicklungseinrichtung für die Ermittlung von Kriminalität und Kriminellen, innovativem Training, operativer Unterstützung und Kooperation. Es wird derzeit in Singapur aufgebaut und soll 2014 operativ werden.

Zu den vier Komponenten des IGCI zählt das INTERPOL Digital Crime Centre. Zwei Kernelemente des Zentrums sind das Forensische Labor und das Cyber Fusion Centre.

Im Forensischen Labor wird der Fokus auf Technologie gelegt, die Ermittler werden mit der Fähigkeit einer besseren Koordination und Durchführung nationaler und regionaler Ermittlungen ausgestattet. Die vier Hauptthemen des Labors sind dabei: Trend-Analyse, Test von Forensischen Werkzeugen, Entwicklung von Best Practice, Ausbildung und Fortbildung.

Das Cyber Fusion Centre wird ähnlich dem INTERPOL Command and Coordination Centre in Echtzeit das Netzwerk überwachen und schadenbringende Aktivitäten im Internet analysieren. Die Analyse und Überwachung wird in zwei Hauptgebieten erfolgen: nachrichtendienstlich und polizeilich.

3M Cogent Fusion Handheld

Neue mobile Technologie zur Personenerkennung in Echtzeit

(EP) Der Einsatz von Geräten zur biometrischen Personenerkennung hält neben dem militärischen Bereich zunehmend Einzug in den behördlichen Raum. Besonders im Rahmen der Strafverfolgung bieten mobile biometrische Geräte Polizeibeamten zahlreiche Nutzungsmöglichkeiten. Mit dem 3M Cogent Fusion Handheld bietet das Multi-Technologieunternehmen 3M eine innovative Lösung zur mobilen Identitätsüberprüfung in Echtzeit.

Der technische Fortschritt im Bereich der automatisierten Erkennung übereinstimmender Muster eröffnet Polizeibeamten vielfältige neue Einsatzmöglichkeiten. Ob für kriminalistische Ermittlungen, zu forensischen Zwecken oder zur Wahrung der öffentlichen Sicherheit – insbesondere mobile Technologien zur Personenerkennung bringen hier einen großen Nutzen. In Deutschland werden diese technischen Möglichkeiten jedoch bislang kaum genutzt. Lediglich im Bereich der biometrischen Gesichtserkennung laufen erste Versuche, u. a. auf Bahnhöfen, Flughäfen oder bei Demonstrationen. Dabei werden Aufnahmen von Personen mit den biometrischen Bilddaten im Reisepass und Personalausweis verglichen. Diese Daten werden seit November 2005 über einen Chip in deutschen Ausweisdokumenten gespeichert.
In den USA wird das 3M Cogent Fusion Handheld mit großem Erfolg bereits von drei US-amerikanischen Polizeieinheiten eingesetzt. Mittels Abgleich von Fingerabdrücken, Gesichtserkennung und Iris-Scan lassen sich Personen schnell identifizieren, zum Beispiel wenn sie keine Ausweispapiere bei sich tragen oder Opfer eines Unfalls sind. Die aufgenommenen Daten werden in Echtzeit via WLAN, GPS, UMTS oder Bluetooth mit einer Online-Datenbank abgeglichen, sodass die Beamten noch vor Ort eine zuverlässige Auskunft über die zu überprüfende Person erhalten. Alle gesammelten Daten können zudem über GPS lokalisiert werden.

Der 3M Cogent Fusion Handheld: Mobile Identitätsprüfung in Echtzeit

Foto: EP/3M

Maximale Zeitersparnis dank mobilem Fingerabdruckabgleich

Bisher mussten latente Fingerabdrücke an Gegenständen zunächst auf Trägermaterial aufgenommen, ins Labor geschickt und dort ausgewertet sowie mit den Fingerabdrücken in der Datenbank abgeglichen werden. Der Prozess kann durchaus mehrere Tage in Anspruch nehmen. Durch den Einsatz des 3M-Cogent-Fusion-Gerätes wird die Ermittlungszeit deutlich verkürzt und die Handlungsfähigkeit der Beamten schon am Tatort gesteigert. Darüber hinaus werden Ressourcen und damit Kosten bei der Ermittlung eingespart.
Die Erfassung der Fingerabdrücke erfolgt über zwei unterschiedliche Wege: Latente Fingerabdrücke auf Beweismitteln werden mithilfe einer integrierten Hochleistungskamera aufgenommen, während direkte Fingerabdrücke über einen Scanner übertragen werden. Eine Systemmeldung gibt umgehend Auskunft über die Verwertbarkeit der Aufnahme. Ist die Qualität ausreichend, werden die Daten in Echtzeit an ein automatisiertes Fingerabdruckidentifizierungssystem (AFIS) gesendet und mit der zentralen Datenbank der Polizeidienststelle abgeglichen. Zusätzlich lassen sich die Daten auch mit einem internen Speicher mit bis zu 15.000 Fahndungseinträgen abgleichen.

Hochleistungskamera ermöglicht sofortige biometrische Gesichtserkennung

Zur Identifikation von Personen mittels biometrischer Gesichtserkennung werden Gesichtsmerkmale erfasst, analysiert und mit bestehenden Daten abgeglichen. Voraussetzung für eine mögliche Identifikation ist eine hochwertige biometrische Frontalaufnahme. Die Hochleistungskamera des 3M-Cogent-Fusion-Gerätes erfasst das Gesicht in einer Auflösung von bis zu 1.000 dpi. Anschließend lokalisiert eine Erkennungssoftware das Gesicht und berechnet seine charakteristischen Eigenschaften. Dieses sogenannte "Template" wird mit anderen gespeicherten Gesichtsbilder-Templates in Echtzeit über ein mobiles Netzwerk verglichen.

Zunehmende Anwendung der Iriserkennung

In den USA hat sich die von den 3M-Cogent-Fusion-Geräten unterstützte Iriserkennung als eine ebenfalls hochpräzise Methode zur Personenidentifikation erwiesen. Hierfür wird der Iris-Scanner an das Auge herangeführt und leicht an die Gesichtshaut gedrückt. Der Blick der zu identifizierenden Person muss gerade nach vorne gerichtet sein. In nur wenigen Sekunden ist die Iris gecannt und kann mit existierenden Iris-Scans abgeglichen werden.
Ein zusätzlicher Vorteil des Cogent Fusion Handheld ist seine mobile Handhabung in kompakter Größe (Länge 22,2 cm, Breite 11,7 cm, Höhe 7,4 cm). Der nützliche Helfer ist mit 0,5 Kilogramm ein Leichtgewicht und passt in jede Tasche.

Cybercrime:

Forensik und Sicherheit

(EP) Definitorisch werden alle Staftaten unter dem Begriff "Cybercrime" subsumiert, bei denen der Computer als Tatmittel eine zentrale Rolle spielt. Jörg-Uwe Hesse, Vorsitzender der Justizministerkonferenz, brachte es im November 2012 im ZDF-"Morgenmagazin" treffend auf den Punkt: "Das Internet ist der größte Tatort der Welt, aber dort sind auch die größten Informationen zu holen." Das Internet birgt also aus Sicht der Sicherheitsbehörden Risiken und Chancen.

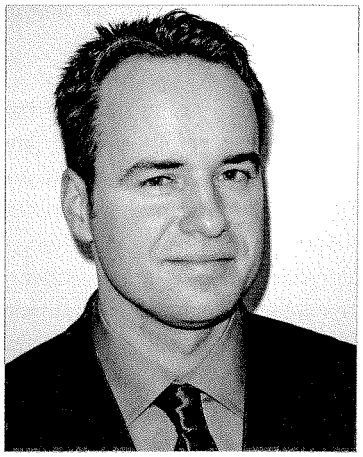
Zunächst zu den Risiken: Radikale Islamisten schöpfen das Potenzial des Web 2.0 intensiv und intelligent aus. Webauftritte von Terrorgruppen lassen sich zwar relativ schnell vom Netz nehmen, aber Diskussionsforen, die anonym oder mit Tarnnamen funktionieren, sind sehr schwer zu identifizieren und zu überwachen. Das Internet wird zur viralen Informations- und Rekrutierungsbasis von Terroristen.

Es gibt täglich tausende Hackerangriffe auf Kritische Infrastrukturen in Deutschland, die große materielle Schäden anrichten und auch Menschen töten können (z. B. durch Stromausfälle). Auch computergestütze Spionage und Sabotage sowie Datendiebstahl bei Behörden und Industrieunternehmen sind an der Tagesordnung. Selbst gewöhnliche, international operierende Cyber-Kriminelle werden aktiver: Für 40 Euro pro Karte werden gültige Kreditkartendaten im Internet zum Kauf angeboten. Der damit verbundene Schaden wird allein in Europa auf mehrere Milliarden Euro jährlich geschätzt.

Deutsche Sicherheitsbehörden stellen sich diesen Risiken und haben eigene Organisationseinheiten, die sich ausschließlich mit Cybercrime befassen. Sie nehmen das Internet gleichzeitig aber auch als Chance wahr: Sie starten Fahndungen per Facebook oder über spezielle eigene Webseiten und sie betreiben aktive Informationsrecherche im Internet, in Kombination mit den üblichen Fahndungsmechanismen. Beispielsweise in der Projektinitiave "White IT", in der sich Oracle engagiert, geht es um den weltweiten Kampf gegen Kinderpornografie im Internet, an dem sich bereits 48 Länder beteiligen.

Technisch, infrastrukturell und personell stellen diese geschilderten Sachverhalte hohe Anforderungen an die IT-Expertise der Sicherheitsbehörden: Zum einen müssen sie ihre eigenen IT-Systeme wirksam gegen Angriffe von außen abschotten. Das ist bislang hauptsächlich dadurch gelungen, dass die Polizeiverfahren in separaten physischen Netzen arbeiten, komplett entkoppelt vom Internet. Die elektronische Verzahnung zwischen den Behörden (z. B. Polizeien mit der Staatsanwaltschaft, Polizeien mit dem Zoll) sowie die zunehmende Internetpräsenz der Polizeien erzwingen eine gewisse Öffnung, die dann ein Einfallstor für Hackerangriffe darstellt. Auch der Datendiebstahl hinter bzw. innerhalb der Firewall muss verhindert werden, zumindest durch massive Limitierung der Zugriffe auf hochvertrauliche Daten. Zusätzlich können alle Zugriffe exakt auditiert werden, um nachzuweisen, wer wann welche Dateninhalte gesehen hat. Nur wenige deutsche Sicherheitsbehörden haben derartige Technologien schon im Einsatz. Oracle hat für all diese Sicherheitsanforderungen die notwendigen Komponenten verfügbar, u. a. kryptografische Verschlüsselung der Datenbankinhalte und/oder Verschlüsselung dieser Daten auf dem Übertragungsweg von der Quelle zum Ziel oder auch die Auditierung der Datenbankzugriffe selbst. Mit Oracle-Technologien kann sichergestellt werden, dass keinerlei unerlaubte Zugriffe auf sensible Daten möglich sind.

Zum anderen ist der aktive Blick nach außen sowohl für die laufende Fahndung als auch für die gezielte Prävention wichtig. Einschlägige Studien belegen, dass sich die Polizeiarbeit der Zukunft massiv auf die Prävention konzentrieren muss, da damit die Deliktzahlen nachhaltig sinken. Nur so kann in Zeiten massiv abnehmender personeller Kapazitäten (Pensionierungswelle, Kostendruck wegen der Schuldenbremse) die Innere Sicherheit in Deutschland auf dem bestehendem Niveau gehalten werden. Nach Analystenschätzung werden sich bis zum Jahr 2020 die Datenbestände international um den Faktor 50 vermehren. Dieser unstrukturierten Massendaten (neuer IT-Megatrend "Big Data") in Form von Webseiten, sozialen Foren, Textdokumenten, Messages aller Art etc. gilt es Herr zu werden. In Deutschland weder juristisch zulässig noch technisch möglich und auch politisch nicht gewollt ist eine vollständige Internetüberwachung. Pragmatisch gefordert ist eine flexible technische Möglichkeit, alle möglicherweise relevanten Quellen auf definierte Kriminalitäts- oder Terrorphänomene zu überwachen und aktive Signale zu bekommen, wenn sich auffällige Muster ergeben. Diesen kann dann gezielt (manuell) nachgegangen werden. Auch für diese Domäne des Informationsmanagements, die sich um den Bereich Wissensmanagement, unscharfe Suche und umfassende Analyse rankt, bietet Oracle ein vollständiges Lösungsportfolio, das bei Bedarf alle notwendigen Hard- und Softwarekomponenten aus einem Guss liefert. Dazu gehört neben der Massendatenakquise und -verarbeitung die gezielte Filterung dieser semi- oder unstrukturierten "Schmutzdaten", auch deren Verdichtung und/oder tiefergehende Analyse.



Oliver Röniger, Oracle Deutschland, Accountmanager Öffentliche Auftraggeber Foto: EP/Oracle

Auf dem Oracle-Stand im Rahmen des 16. Europäischen Polizeikongresses in Berlin stellen wir Ihnen gerne die hier skizzierten Möglichkeiten vor.

"Wir stellen uns der Verpflichtung!"

Polizeiliche Bekämpfung von Cybercrime

(EP) Am Rande des Polizeitages 2012 in München sprach European Police mit dem Münchner Polizeipräsidenten Prof. Dr. Wilhelm Schmidbauer über die Herausforderung der Bekämpfung von Cybercrime für die Polizei. Das Gespräch führte Behörden Spiegel-Chefredakteur R. Uwe Proll.

European Police: *Cyberkriminalität ist ein zunehmendes Polizeithema. Wie hoch ist die Anforderung an Ihre Behörde, den Bürgern hier beizustehen?*

Schmidbauer: Höher denn je! Das Polizeipräsidium München ist nicht nur gefordert, eine jährlich steigende Zahl an Betrugsstraftaten im Internet, Datenausspähungen, Sabotageakten an EDV-Infrastruktur oder Urheberrechtsverstößen aufzuklären – wir von der Münchner Polizei stellen uns auch der Verpflichtung, die in den letzten Jahren massiv eingeschränkten Möglichkeiten der Gefahrenabwehr und der Strafverfolgung in der virtuellen Welt anzuprangern.
Eingeschränkte Möglichkeiten, die de facto die Rechte der Verbraucher im World-Wide-Web beschneiden! Wir stellen uns der Forderung, die Bürger im Netz nicht alleine zu lassen.

European Police: *Für die Bekämpfung der Cyber-Kriminalität braucht man Spezialisten. Wie reagieren Sie darauf?*

Schmidbauer: Seit 02.07.2012 arbeitet im Polizeipräsidium München die Task Force Cyber Crime. Wir reagieren, indem wir Spezialisten ausbilden und einstellen! Das heißt, wir machen beides: Wir bilden erfahrene Kriminalbeamte in EDV-Wissen fort und wir stellen ausgewiesene EDV-Fachleute ein und bilden sie zu Kriminalbeamten aus. Und zwar ganzheitlich: So sind unsere Ermittler echte EDV-Fachleute, die alle Tricks und Fallen des Internets, von Hard- und von Software kennen. In der Prävention und Beratung haben wir Kommunikationsexperten, die – in die Computersprache übersetzt – als "Interface" zwischen dem bisweilen mit den neuen Medien überforderten Menschen und den hochspezialisierten Cyber-Cops fungieren.
Wir haben dort Beamtinnen und Beamte, die mit den Menschen in ihrer Sprache sprechen, Probleme und Gefahren entsprechend aufzeigen und Lösungen an die richtige Stelle bringen. Auch durch Profis zur Bekämpfung des Wirtschaftbetrugs oder durch Fahnder gegen Kinderpornografie.

European Police: *Ihre Cyber-Sondereinheit wird regulär in der Organisation geführt und alle Mitarbeiter erhalten die reguläre Besoldung oder mehr?*

Schmidbauer: Unsere Spezialisten auf allen Gebieten, ob Rauschgiftfahnder, Mordermittler oder Experten für die Terrorismusbekämpfung werden gleich alimentiert. Da sind auch die Cyber-Cops keine Ausnahme. Aber zum finanziellen Aspekt tritt bei Polizeibeamten immer auch noch der Lohn in Form des Bewusstseins, gesellschaftlich Wichtiges zu leisten, Menschen, die Opfer geworden sind, zu helfen und für ein Mehr an Gerechtigkeit auf unserer Welt zu sorgen.
Entsprechend sind die Ermittler gegen Cyber-Kriminalität auch ganz ordentlich in unsere Aufbauorganisation eingebunden. So unterstützen sie auch einmal außerhalb ihres originären Aufgabenbereichs ihre Kollegen, wenn es heißt, in anderen Ermittlungsfällen ausgesprochene EDV-Probleme anzugehen.

Info

ePolice: Prävention & Strafverfolgung in Sozialen Netzwerken
Moderiert von Bernhard Egger, Dezernatsleiter Fahndung, Bayerisches Landeskriminalamt, diskutieren am Dienstag, 19. Februar 2013, von 11:00 Uhr bis 12:30 Uhr u. a. Dr. Markus Hellenthal, Vice President IBM, Geschäftsleiter Public Sector, Savas Gel, Niedersächsisches Ministerium für Inneres und Sport, Helmut Picko, Dezernatsleiter Kompetenzzentrum Cybercrime, Landeskriminalamt Nordrhein-Westfalen, und Thomas-Gabriel Rüdiger, Fachhochschule des Landes Brandenburg, über Prävention und Strafverfolgung in Sozialen Netzwerken.

DEEP INTERNET Forensic

Gefahrenlagen schneller feststellen

(EP/Bert Weingarten/PAN AMP) In Deutschland wird der effektive Einsatz von automatisierter Internet-Forensik-Technologie bereits seit 2003 durch die PAN AMP AG vorangetrieben. Dadurch wurde es möglich, mehr Untersuchungen durchzuführen, die Analysezeit erheblich zu reduzieren und Gefahrenlagen schneller festzustellen und aufzuklären.

Technologie

Die Erkenntnis, dass vollautomatisierte Prozesse wesentlich effizienter sind als die Suche per Hand, führte bereits Ende der neunziger Jahre zur Entwicklung der PAN AMP Technologie zur automatischen URL-Analyse. Hierdurch wurde es erstmals möglich, Internetinhalte fortlaufend zu überprüfen, inhaltliche Veränderungen automatisch zu erfassen und auszuwerten. Im Jahre 2000 wurde das Angebot durch Entwicklungen ergänzt, die selbständig Datennetze durchsuchten. Seither werden umfassende Systeme zur automatisierten Internet und DEEP INTERNET Forensic entwickelt, die Inhalte, Computer und Netzwerke voll automatisiert analysieren, identifizieren und lokalisieren.

Forensik

Beflügelt durch eine umfassende Verfügbarkeit, immer schnellere Anbindungen und eine immer weitergehende Verbreitung des Internets, erreicht die jederzeit für jedermann verfügbare Menge an Informationen und Daten ständig neue Dimensionen. Doch nicht nur legale Netzbetreiber, die lizenzierte und rechtlich einwandfreie Inhalte vertreiben, stellen immer größere Datenmengen in das Internet ein. Auch Kriminelle haben das Internet voll erschlossen; mit dem Effekt, dass in vielen Konzernen, Kanzleien und staatlichen Einrichtungen bereits heute die Personalkapazitäten für die Abwehr und die Verfolgung von Straftaten bis an die Grenze ausgeschöpft sind. Die noch immer verbreitete Recherche und Beweissicherung per Einzelplatz-PC mit Webbrowser und Handarbeit wird der heutigen Herausforderung bei weitem nicht mehr gerecht.

In- und Ausländische Strafverfolgungsbehörden stellten in den vergangenen Jahren eine weitere Zunahme von Straftaten fest, die per Computer begangen worden sind. Das Spektrum der Straftaten reicht vom Betrug mit Phishing, über die Verbreitung von illegalem Material wie Kinderpornografie, bis zur Verbreitung von Computerviren und dem Einbruch oder der Manipulation fremder Rechnersysteme.

Bislang galt die goldene Regel schnellstmöglich der zur Straftat verwendeten Computer habhaft zu werden, um einen technischen und kriminalistischen Prozess, den man als Digitale Forensik bezeichnet, durchzuführen. Doch wie sichert man "flüchtige Beweise", Beweise, von denen man erwarten muss, dass sie in kürzester Zeit nicht mehr verfügbar oder rekonstruierbar sein werden? Eine weitere Problematik war die Gegebenheit, dass die zur Straftat verwendeten Rechnersysteme oftmals ihren physikalischen Standort in einem anderen Bundesland oder im Ausland haben, oder es sich gar um weltweit verteilte Rechnersysteme handelt.

Peter Altmaier (l.) im Gespräch zur DEEP INTERNET Forensic mit Bert Weingarten (r.) Foto: EP/PAN AMP

Aus diesen Überlegungen heraus entwickelt PAN AMP®, basierend auf der bereits von seit 1998 entwickelten Hochleistungs-Filtertechnologie, umfassende Systeme zur automatisierten Internet und DEEP INTERNET Forensic, die verdächtige Computer und Netzwerke voll automatisiert identifizieren, analysieren, Dossiers erstellen und die Online-Beweissicherung leisten.

Zur vollständigen Beantwortung der juristischen Frage der so genannten "7-Goldenen-W" (wer? was? wann? wo? womit? wie? warum? reicht der PAN AMP Technologie ein einziger Mausklick. Hierdurch werden z.B. Ergebnisse der DEEP INTERNET Forensic, der Online-Beweissicherung und das dazugehörige Dossier mit allen Ergebnissen online zugestellt bzw. auf Datenträgern zur Übergabe gespeichert. Vor Gericht kann der Vorfall so nicht nur angesehen sondern durch die vorliegende Online-Beweissicherung vorgeführt werden.

Ich freue mich auf Ihre Teilnahme an meinem Vortrag auf dem 16. Europäischen Polizeikongress:

Info

DEEP INTERNET FORENSIC - Entwicklungsstand der automatisierten Lokalisierung von Cybercrime

⇢ **Mittwoch, den 20. Februar 2013, 10:40 Uhr**

IT und Polizei

Der Zwang des Faktischen

(EP/lin) Unter dem Titel "IT und Polizei: Anforderungen an die Informationstechnologie und Herausforderung Cybercrime" fand in Wiesbaden die Abschlussveranstaltung der Reihe "Polizeitage 2012", einer Kooperation der Gewerkschaft der Polizei (GdP) und des Behörden Spiegel, statt.

In seiner Eröffnung stellte Horst Westerfeld, Staatssekretär im Hessischen Ministerium der Finanzen sowie Bevollmächtigter der Hessischen Landesregierung für E-Government und Informationstechnologie, zunächst die auch von der Ständigen Konferenz der Innenminister und Innensenatoren der Länder (IMK) geforderte Kompetenz gegen Internetkriminalität in den Vordergrund. "Es müssen Kompetenzen zusammengelegt werden, damit die Polizei ihre Aufgaben im Cyber-Raum erfüllen kann", so der Staatssekretär.
Das Netz sei ein Raum, der viele verschiedene Angriffspunkte biete. Es gebe dort schon jetzt viel Kriminalität, der die Polizei entgegentreten müsse. "Dabei stehen wir jedoch noch am Anfang der Möglichkeiten von Cybercrime. Wir brauchen mehr Ressourcen und mehr Kompetenz, diesem entgegenzutreten", so Westerfeld. Das Netz biete aber eben auch riesige Chancen. Ohne das Netz sei keine Wirtschaftsentwicklung mehr möglich. Die physikalischen Netze seien für die Wettbewerbsfähigkeit eines Wirtschaftsstandorts wichtig. Daher müsse der Sicherung der Netze auch Priorität gelten.
Bernhard Lammel, Abteilungsleiter 3 "IuK-Einsatz und Cybercrime" im Landeskriminalamt Hessen (HLKA), betonte, dass Cybercrime kein Nischenthema mehr sei und auch kein exklusives Spezialistenthema. Cybercrime sei Alltag, der jeden betreffe.
Nach der Neuorganisation im HLKA arbeiteten in der neuen Abteilung IuK Einsatz und Cybercrime derzeit 80 Personen. Unter dem Motto "Vernetzte Kompetenz im Team" sei die neue Abteilung gut gestartet. Dennoch plane man in Hessen bereits weiter. Mit dem Projekt "System 120" wolle man die Kompetenz im Landeskriminalamt personell aufstocken und die guten Einzelaktionen in Hessen systematisch zusammenbringen. "Wir müssen eine gemeinsame Linie in Hessen finden", so Lammel. Dazu bedürfe es u. a. der Fachkompetenz in der polizeilichen Fläche und des Ausbaus vertikaler und horizontaler Kompetenz. "Eine Grundkompetenz, Cybercrime schon in der polizeilichen Ausbildung zu erlernen, ist zwingend notwendig. Da müssen wir ran", sagte Lammel.

Der Polizei nichts wegnehmen

Moderiert von Behörden Spiegel Chefredakteur R. Uwe Proll diskutierten Nancy Faeser, Innenpolitische Sprecherin der SPD-Fraktion im Hessischen Landtag, Alexander Bauer, MdL, Innenpolitischer Sprecher der CDU-Fraktion im Hessischen Landtag, Dr. Frank Blechschmidt, MdL, FDP, Mitglied im Innenausschuss, und Jörg Bruchmüller, Landesvorsitzender Hessen der Gewerkschaft der Polizei, in Wiesbaden über die Herausforderungen der Internetkriminalität für die Polizei.
Nach Nancy Faeser seien die Möglichkeiten und Gefahren des Netzes in der Gesellschaft angekommen. So würde etwa an Schulen bereits frühzeitig an der Medienkompetenz gearbeitet. In der Polizei sei die Herausforderung Cybercrime dagegen noch nicht unbedingt angekommen. Es seien hier erweiterte Möglichkeiten für die Polizei bei Facebook notwendig. "Die Polizei muss sich hinsichtlich der Fahndung und der Strafverfolgung dem Cyber-Raum anpassen. Die Politik rennt dort noch hinterher", so Faeser. Doch der Bürger komme bei Straftaten als erster zur Polizei. Daher sei eine breite Fortbildung in der polizeilichen Facharbeit notwendig. Dies gelte aber auch bei Richtern. Viele Verfahren würden aus Kapazitätsmangel bei Richtern eingestellt. Zudem werde eine Partnerschaft mit Privaten gebraucht.
"Wir laufen der Lage derzeit hinterher. Es ist eine Ohnmacht vorhanden. Dennoch können wir vieles verbessern. Außerdem machen wir noch nicht alles, was wir machen könnten", so die einstimmige Meinung der Diskussionsrunde.

Freiheit und Sicherheit im Netz

Eskalation von Facebook-Partys

(EP/lin) Facebook ist für manch einen regelrecht Teil seines täglichen Lebens geworden. Man unterhält sich auf Facebook, man hat Freunde auf Facebook und man teilt die täglichen Situationen seines Lebens. Man verabredet sich zu einem gemeinsamen Kinobesuch oder lädt zur Geburtstagsfeier ein.

Immer öfter, fast täglich, eskalieren aber solche Facebook-Partys in einem zumeist unkalkulierbaren Chaos: Gewalt, Zerstörungen, Alkohol-Exzesse, unkontrollierbare Menschenmassen. Erste Todesfälle infolge ausgearteter Facebook-Parties in Frankreich und den Vereinigten Staaten führten bisher zu keinerlei Umdenken.

Die Eskalation von Facebook-Partys erfordert regelmäßig den Eingriff von Einsatzkräften der Polizei und Feuerwehr, die sich jedoch einer unsicheren Rechtslage gegenübersehen. Besteht in diesen Fällen das Grundrecht auf Versammlungsfreiheit? Ist für eine Facebook-Party die Vorlage von Sicherheitskonzepten notwendig? Wer haftet für die entstandenen Schäden? Trägt Facebook eine Mitschuld?

Bislang kann die Polizei nur präventiv gegen ausufernde Facebook-Partys vorgehen. Die Gewerkschaften fordern daher auch die Schaffung rechtlicher Voraussetzungen.

Immer häufiger eskalieren Facebook-Partys und erfordern ein Eingreifen der Sicherheitsbehörden. Diese sehen sich jedoch einer unsicheren Rechtslage gegenüber.

Foto: BS/Rainer Sturm/Pixelio.de

Was geht eigentlich ab im Netz?

Polizei in der Pflicht gegen Cybercrime

(EP/Patricia B. Linnertz) Das Motto der letztjährigen CeBIT trägt noch immer über die Veranstaltung hinaus: "Managing Trust" ist ein Bekenntnis zur Stärkung von Vertrauen und Zuverlässigkeit der technischen Innovationen im Hinblick auf Ihre Akzeptanz in Unternehmen und Behördenlandschaft. So stellen etwa Cyber-Kriminalität und vor allem die Underground Economy die Polizei vor erhebliche Herausforderungen.

Oliver Stock, Polizeidirektion Hannover, stellte im Rahmen des Fachforums "Cybercrime – eine Herausforderung für Polizei und Gesellschaft" auf der CeBIT 2012 zunächst die Akteure und Phänomene der Kriminalität im virtuellen Raum sowie Risiken und Bedingungen des Cybercrimes anhand von Erfahrungen aus polizeilichen Ermittlungen im Bereich der Cyber-Schattenwelt dar. Die Ermittlungserfolge der Sicherheitsbehörden im Bereich sogenannter "Carderforen" aus der Welt des Cybercrimes wurden von der allgemeinen Öffentlichkeit bislang kaum wahrgenommen. Es war nur eine kurze Meldung, die in Fachmedien über den Online-Ticker lief: "Polizei legt "Carder"-Forum still."

Oliver Stock kann das gut nachvollziehen: "Die Öffentlichkeit ist für diese Phänomene noch nicht sensibilisert. Was sich im Schatten der Netzwelt abspielt, ist auch für die meisten normalen Internet-Nutzer nicht zu überschauen", sagte Stock in Hannover. Längst aber habe die alltägliche Kriminalität ins Internet Einzug gehalten.

Stock machte deutlich, dass gerade die illegalen Handelsplattformen inzwischen weltweit verbreitet seien. Allein in Deutschland dürfte es nach Einschätzung der Ermittler über 20 sogenannte "Schattenforen" geben. "Dort ist inzwischen die gesamte Breite der Kriminalität vertreten. Schwerpunkt ist nach wie vor der Betrug mit fremden Zahlungskartendaten, aber inzwischen auch der Vertrieb von Betäubungsmitteln, Waffen oder falschen Identitätspapieren", machte Stock deutlich.

Im Rahmen des Fachforums nahmen die Ermittler der Polizeidirektion Hannover ihr Publikum mit auf eine "Einkaufstour". Die Sprache war zwar grundsätzlich deutsch, gleichwohl war der Inhalt ohne anschließende Übersetzung kaum nachzuvollziehen. "In der Szene hat sich längst eine Subkultur mit einer eigenen Sprache etabliert, die aus der öffentlichen Diskussion gelernt hat, dass das Internet als polizeifester Raum unangetastet bleiben soll", ist sich Stock sicher. Aus Ermittlersicht ist der "Lebensraum Internet" nicht nur ein Raum voller kreativer und innovativer Chancen, sondern auch ein Risikoraum, der für viele Menschen nicht mehr antizipierbar ist.

Die Zeit der "Digitalromantik" mit "moralischen Hackern" und experimentierfreudigen "Skript Kiddies" scheint längst vorbei. Aus diesen Gruppen rekrutieren sich inzwischen auch Kriminelle, die für Bereiche des Cybercrimes zur Verfügung stehen. Darunter finden sich "Cyber-Dealer", die als Läufer arbeiten, um virtuelle Gewinne in echtes Geld umzusetzen, sowie "Experts" und "Professionals", von denen die Prozesse der Cyber-Kriminalität gesteuert werden.

Jeder könne durch Kriminalität im oder durch das Netz betroffen sein und habe dann bisweilen große Mühe, seine Reputation wieder herzustellen. Das Motto "Managing Trust" hält Stock daher für ein wichtiges Signal an die Branche, aber auch an Teile der Politik, die Augen vor Risiken und Kriminalität im Internet nicht zu verschließen. "Wir haben im Moment eher noch das Problem, dass viele Besorgnisträger der Offline-Welt längst vorhandene Realitäten der Online-Welt nicht zur Kenntnis nehmen", glaubt Stock.

Das Internet habe einen Parallel-Raum geschaffen, in dem digitale Beziehungen bestünden. Gerade in dem "Raum" des Internets stoße die Polizei an ihre Grenzen.

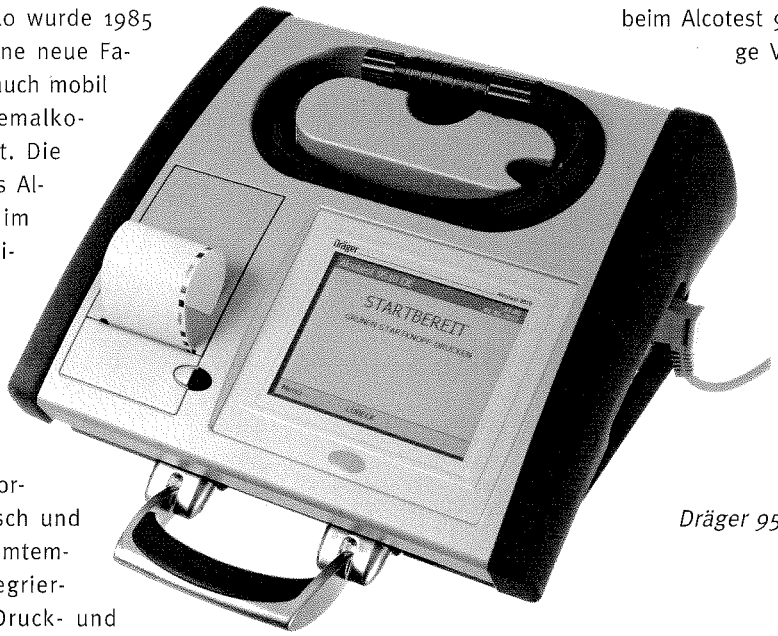
"Die Polizei ist lokal zuständig. Das Internet hat aber eben keine lokale Begrenzung auf einen kriminal-geografischen Raum", sagte Stock weiter.

Das Dräger 9510 DE

Die neuste Generation der beweissicheren Atemalkoholtests

(EP) Seit Jahrzehnten sind Atemalkoholmessungen ein etabliertes und effizientes Mittel gegen Alkohol im Straßenverkehr. Das 1953 bei Dräger entwickelte "Pusteröhrchen" zur Bestimmung von Atemalkohol bei Verkehrsteilnehmern fand sofort hohe Akzeptanz bei der Polizei. Es ermöglichte eine objektive Vor-Ort-Messung, die als Basis für die Anordnung weiterer Beweissicherungsmaßnahmen diente. Der damals entstandene und für Dräger geschützte Markenname "Alcotest" wurde weltweit gleichbedeutend für Atemalkoholmessungen.

Mit der Einführung der ersten Generation des Alcotest 7110 wurde 1985 der Grundstein für eine neue Familie stationär, aber auch mobil zu verwendender Atemalkoholmessgeräte gelegt. Die Weiterentwicklung des Alcotest 7110 gipfelte im Alcotest 7110 Evidential, das seit 1998 einen Meilenstein in der Atemalkoholmessung darstellt. Als mobil oder stationär verwendbares Gerät mit Doppelsensorsystem (infrarot-optisch und elektrochemisch), Atemtemperaturmessung, integriertem Drucker sowie Druck- und Volumensensoren erfüllen seine Messergebnisse die weltweit strengsten Anforderungen und wurden in vielen Ländern zum Standard. In Deutschland sind die Messungen dieses Gerätes nach dem Straßenverkehrsgesetz und dem Urteil des Bundesgerichtshofes vor Gericht den Ergebnissen der Blutprobe gleichgestellt.



Dräger 9510 DE

Foto: EP/Dräger

Im Jahr 2013 feiert Dräger das Jubiläum von 60 Jahren Alcotest. Dräger-Alcotest-Geräte finden heute in den unterschiedlichsten Ausführungen weltweit Verwendung. Was mit dem Alcotest-Röhrchen begann, reicht heute bis zu computergesteuerten Messgeräten, die Fremdeinflüsse oder Manipulationen bei der Bestimmung der Atemalkoholkonzentration ausschließen. So helfen Dräger-Alcotest-Geräte, die Verkehrssicherheit zu erhöhen. Die Technik hat sich im Laufe der Jahre verändert und die Qualität der Ergebnisse sowie die Einfachheit der Anwendung haben sich kontinuierlich weiterentwickelt. Dafür steht seit 60 Jahren der Name Alcotest.

Das Dräger Alcotest 9510 DE ist die neueste Entwicklung im Bereich der beweiskräftigen Atemalkoholmessung aus dem Hause Dräger. Es erfüllt die Anforderungen der DIN VDE 0405, die Zulassung bei der Physikalisch-Technischen Bundesanstalt wird in Kürze abgeschlossen. Dann kann das Alkoholmessgerät von der Polizei zur Überwachung des Straßenverkehrs eingesetzt werden und seine Testergebnisse werden im Bereich der Ordnungswidrigkeiten vor Gericht anerkannt.

Die Bestimmung der Atemalkoholkonzentration erfolgt auch beim Alcotest 9510 DE durch die gleichzeitige Verwendung zweier voneinander unabhängiger Messsysteme mit unterschiedlicher analytischer Spezifität: einem elektrochemischen und einem infrarot-optischen Sensor. Durch dieses duale Sensorkonzept werden Fremdeinflüsse erkannt und Fehlmessungen ausgeschlossen. Neben den Messsystemen für die Alkoholbestimmung sind auch die Messsysteme für die Atemtemperatur und das Exspirationsvolumen redundant ausgelegt. Beide Messgrößen werden durch jeweils zwei Sensoren bestimmt. Durch den internen Vergleich dieser Sensordaten sind die Messungen nicht manipulierbar und liefern höchst zuverlässige Ergebnisse.

Die selbsterklärende Benutzeroberfläche führt den Bediener durch die einzelnen Test- und Handhabungsschritte. Diese werden durch akustische Signale und vollständige Textanweisungen ergänzt. Das große Display stellt dabei alle Schritte übersichtlich dar. Alle Daten werden individuell über das Touchscreen-Display oder eine externe Tastatur direkt in das Gerät eingegeben.

Der lange, flexible und temperierte Atemschlauch des Alcotest 9510 DE verhindert die Atemkondensation. Der obere Teil des Atemschlauchs, in den die Atemtemperatursonden integriert sind, ist auswechselbar, um den Austausch der empfindlichen Atemtemperatursensoren zu erleichtern.

Mit seiner hohen Robustheit gegen äußere Einflüsse eignet sich das Alcotest 9510 DE auch für den mobilen Einsatz. Das Gerät arbeitet entweder mit 230-Volt-Wechselspannung oder mit 12-Volt-Gleichspannung, ohne auf einen Umschalter, Adapter oder Stromumwandler angewiesen zu sein.

Das Gerät kann wahlweise horizontal oder vertikal aufgestellt genutzt werden, da das Touchscreen-Display die Möglichkeit bietet, die Anzeige um 180° zu drehen. Dadurch kann der Platzbedarf auf ungefähr eine DIN-A4-Fläche reduziert werden.

40 Jahre GSG 9

Sonderpublikation zum 40-Jährigen Bestehen der deutschen Antiterroreinheit

» Was ich mir für die Zukunft wünsche? Mein einziger Wunsch ist jeden Tag, dass meine Leute heil aus dem Einsatz zurückkommen! «

Olaf Lindner, Kommandeur der GSG 9

40 Jahre GSG 9 ist eine Geschichte über revolutionäre Gedanken, Meilensteine der Inneren Sicherheit und das Aushängeschild deutscher Sicherheit in der Welt.
Anlässlich des Jubiläums der deutschen Antiterror-Einheit hat der Behörden Spiegel eine Sonderpublikation erstellt, die mit einer formlosen E-Mail an verlag@behoerdenspiegel.de erhältlich ist.

Fallentwicklung und Aufklärung

Cybercrime und Tatmittel Internet

(EP/Patricia B. Linnertz) Nach der Polizeilichen Kriminalstatistik wurden im Jahr 2011 insgesamt 84.981 Fälle von Computerkriminalität erfasst. Dies bedeutete einen leichten Anstieg von 0,7 Prozent (604 Fälle) gegenüber dem Jahr 2010.

24.923 Straftaten wurden im Bereich Betrug mittels rechtswidrig erlaubter Debitkarten mit PIN verübt, im Bereich Computerbetrug nach § 263 a StGB wurden in 2011 insgesamt 26.723 Fälle registriert. Das illegale Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen wurde in insgesamt 15.726 Fällen erfasst.

Die größte Veränderung gegenüber der statistischen Erhebung des Jahres 2010 ließ sich im Bereich Datenveränderung und Computersabotage feststellen. Hier stieg die Zahl der erfassten Fälle um 84 Prozent von 2.524 auf 4.644 an.

Die geringste Aufklärungsquote lag 2011 mit 21,3 Prozent im Bereich des Ausspähens und Abfangens von Daten, die höchste mit 92,8 Prozent bei der Softwarepiraterie in Form gewerbsmäßigen Handelns.

Eine bundesweite vergleichende Darstellung der Sonderkennung "Tatmittel Internet" in der Polizeilichen Kriminalstatistik ist erst seit 2011/2010 möglich. Im Bundesgebiet wurden 2011 insgesamt 222.267 Straftaten mit dem Tatmittel Internet erfasst, was einen Rückgang gegenüber 2010 von 9,9 Prozent bedeutet. Unter diese Straftaten fallen die Verbreitung pornografischer Schriften/Erzeugnisse, Betrug (einschließlich sonstiger Warenkreditbetrug, Warenbetrug, Leistungsbetrug, Leistungskreditbetrug, Computerbetrug sowie sonstige weitere Betrugsarten) und Straftaten gegen Urheberrechtsbestimmungen.

Als Tatort bei Straftaten mit Tatmittel Internet gilt Ort der Handlung durch den Tatverdächtigen, der bei dieser tatmittelspezifischen Form in einer Vielzahl von Fällen nicht identisch sein dürfte mit dem Ort, an dem das strafrechtlich relevante Ereignis eintritt.

Bei den registrierten Schäden ist 2011 ein Anstieg gegenüber 2010 um rund 16 Prozent auf rund 71,2 Millionen Euro zu verzeichnen. Davon entfallen rund 50 Millionen Euro auf den Bereich Computerbetrug und rund 21,2 Millionen Euro auf den Betrug mit Zugangsdaten zu Kommunikationsdiensten.

Die Tatsache, dass zu lediglich zwei Deliktsbereichen eine statistische Schadenserfassung erfolgt, lässt keine belastbaren Aussagen zum tatsächlichen monetären Schaden im Bereich Cybercrime zu.

Eine Einschätzung des Phänomens Cybercrime allein auf Basis statistischer Zahlen ist nicht möglich. Einzelne bzw. besonders relevante Phänomene, wie z. B. Phishing im Bereich Onlinebanking, Straftaten im Zusammenhang mit gezielten DDoS-Attacken oder auch die vielfältigen Ausprägungen der digitalen Erpressung, werden in der PKS nicht unter dem Begriff Cybercrime, sondern vielmehr unter den PKS-Schlüsseln der einzelnen Tathandlungen erfasst. Dies führt dazu, dass keine auf validen Daten basierenden Aussagen zum tatsächlichen Ausmaß in diesen von den Strafverfolgungsbehörden als relevant wahrgenommenen Segmenten des Bereichs Cybercrime möglich sind.

Hinzu kommt das vermutete große Dunkelfeld, insbesondere bei den Deliktsfeldern Computersabotage und Datenveränderung,

- da Straftaten durch den Geschädigten nicht erkannt werden (die Infektion des Computers bleibt unentdeckt),
- der Geschädigte (häufig ein Unternehmen) die erkannte Straftat nicht anzeigt, um beispielsweise im Kundenkreis die Reputation als "sicherer und zuverlässiger Partner" nicht zu verlieren, und/oder
- eine große Anzahl der Straftaten aufgrund immer weiter verbreiteter technischer Sicherungseinrichtungen über das Versuchsstadium nicht hinauskommt und von den Geschädigten nicht angezeigt wird, zumal kein finanzieller Schaden entsteht.

"Was uns nachts nicht schlafen lässt"

Herausforderung Cybercrime

(EP/lin) Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Januar 2013 den ersten Cyber-Sicherheitstag für Teilnehmer der Allianz für Cyber-Sicherheit ausgerichtet. Im Wissenschaftszentrum in Bonn informierten sich mehr als 100 Gäste über die Ziele und Angebote der bundesweit agierenden Initiative.

Zudem bestand die Möglichkeit, aktuelle Themen der Cyber-Sicherheit mit BSI-Experten und Partnern der Allianz zu diskutieren sowie eigene Erfahrungen in diesem Bereich auszutauschen. Das BSI präsentierte unter anderem aktuelle Informationen und erste Ergebnisse der Allianz für Cyber-Sicherheit. So seien beispielsweise erste Informations- und Erfahrungsaustausche auf lokaler Ebene initiiert worden, etwa von der Industrie- und Handelskammer NRW. Seit Beginn der Pilotphase im Mai 2012 konnten bereits mehr als 50 Unternehmen und Institutionen gewonnen werden, die die Allianz als Partner unterstützen.

Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) gegründet wurde. Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, aktuelle und valide Informationen flächendeckend bereitzustellen. Die Allianz für Cyber-Sicherheit baut hierfür eine umfangreiche Wissensbasis für Teilnehmer auf und unterstützt den Informations- und Erfahrungsaustausch. Die Allianz hat sich u. a. das Ziel gesetzt, ein aktuelles Lagebild zu erstellen und zu pflegen, um Informationen für potenziell betroffene Organisationen zur Verfügung zu stellen.

Vor welchen Herausforderungen nicht nur die Behörden und Organisationen mit Sicherheitsaufgaben (BOS), sondern auch die Wirtschaft hinsichtlich der zunehmenden Spionage und Kriminalität im Internet steht, verdeutlichte ein Fachforum des Behörden Spiegel auf der security essen 2012.

Alexander Geschonneck, KPMG, betonte dort, dass sich das Jahr 2012 als das Jahr des Passwortes gezeigt habe. Der Anstieg an Passwortdiebstählen sei enorm angestiegen. "Das Problem dabei ist ganz einfach. 60 Prozent der Anwender verwenden ihre Passwörter mehrfach. So können die Täter auch mehrfach und an verschiedenen Punkten zugreifen", sagte Geschonneck. Neben dem Passwortdiebstahl seien aber auch Phänomene wie "Bring your own Device", Soziale Medien, Kommunikation über Skype und Messenger sowie nicht geschützte Smartphones Umstände, "die den Forensiker nachts nicht schlafen lassen".

"Unternehmen und Behörden müssen sich hinsichtlich des Potenzials der Internetkriminalität selbst fortbilden. Sie müssen in der goldenen Stunde die richtige Maßnahme ergreifen können", so Geschonneck weiter.

Wie Thorsten Scharmatinat, itWatch, betonte, müsste gegen die Gefahren im Netz vor allem eine Akzeptanz der Bürger für Sicherheits-Lösungen geschaffen werden. Die Möglichkeiten hierfür seien vielseitig. "Es geht darum, die faulen Eier im Netz, also die Angreifer, zu finden. Dazu müssen Leckagepunkte beobachtet werden, Problematisches ist zu monitoren und Ungewolltes zu identifizieren", so Scharmatinat. Auch müssten neue Technologien und Verfahren im Netz zuvor ausführlich geprüft werden. Eine Lösung liege auch in der Kontrolle. "Auch dabei sind die Möglichkeiten vielfältig. Es geht um die Kontrolle über Devices und Apps. Diese können durch Sperren, Monitoring oder auch die Anwendung von Filtern kontrolliert und so gegen die Gefahren im Internet geschützt werden", sagte Scharmatinat.

Diesen Punkt unterstrich auch Joachim Mahlstedt, Bundesdruckerei: "Der Nutzer ist arglos, vor allem hinsichtlich seiner Passwörter, und steht zudem vor raffinierten Methoden, komplexen Systemen und gravierenden Folgen. Wir müssen die Technik der Sicherheit im Internet näher an den Bürger bringen."

Innovative GIS-Produkte

Lösungen für den Schutz der öffentlichen Sicherheit

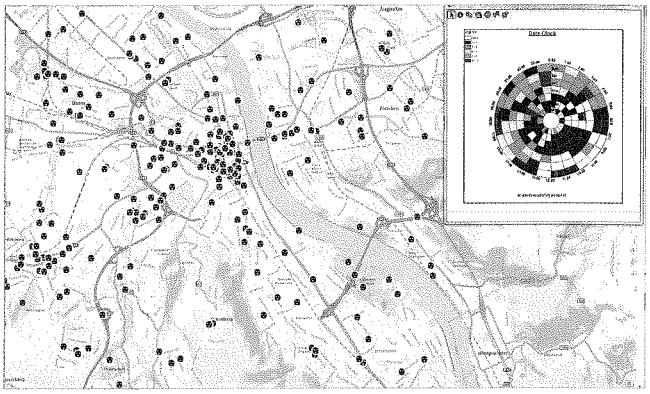
(EP) Der Schutz der Bevölkerung und die Aufrechterhaltung der öffentlichen Sicherheit gehören zu den zentralen Aufgaben der Polizei. Der Erhalt der Inneren Sicherheit wird von unterschiedlichen Faktoren beeinflusst. Als auslösende Ursachen gelten zum einen naturbedingte Auswirkungen und zum anderen Ereignisse, die gewollt oder ungewollt durch Menschenhand verursacht werden.

Während in unseren Breiten die Gefährdung der Bevölkerung durch Naturkatastrophen weniger häufig ist, so hat insbesondere die Zunahme terroristischer Bedrohungen mittlerweile in Europa zu höchster Wachsamkeit geführt. Die Sicherheitsansprüche der Bevölkerung, aber auch die Wahrnehmung von Bedrohungen in der Öffentlichkeit haben sich in den letzten Jahren deutlich verändert – und somit auch die Anforderungen an die Sicherheitsbehörden.

Die Bürgerinnen und Bürger erwarten bestmögliche Prävention und eine schnelle Aufklärung von Delikten. Zugleich möchten sie umfassend und leicht verständlich über komplexe Sachverhalte, wie z. B. Evakuierungsmaßnahmen, informiert werden. Um diesen Anforderungen gerecht zu werden, ist es entscheidend, verschiedene Informationen thematisch, zeitlich und räumlich in einen Gesamtzusammenhang zu bringen. Durch die Einbindung der ArcGIS Lösungen von Esri in bestehende polizeiliche Prozesse bei der Planung oder dem Einsatz lassen sich personelle Ressourcen optimieren, die Reaktionsfähigkeit deutlich erhöhen und die Kriminalitätsbekämpfung unterstützen. Die große Herausforderung ist die gleichzeitige Einbindung und Auswertung unterschiedlicher Informationsquellen sowie die Verfügbarkeit von Schnittstellen zu bestehenden Systemen, wie Vorgangsbearbeitungs-, Fallbearbeitungs- oder Analysesystemen. Egal, ob es sich um den Einsatz in einem Lagezentrum handelt oder um mobile Einsatzkräfte vor Ort: Esri liefert die notwendige Technologie, diesen Herausforderungen zu begegnen, und stellt sich mit dem Geoinformationssystem ArcGIS sowie allen Dienstleistungen dieser Thematik.

Eine neue technologische Entwicklung ist Cloud Computing. Im privaten Umfeld haben sich Cloud-Lösungen bereits in den letzten Jahren etabliert, in der Wirtschaft finden sie immer mehr Anwendung. Für Behörden und Organisation mit Sicherheitsaufgaben (BOS) bietet Esri ein Lösungskonzept für die private Cloud an. Eine private Cloud wird innerhalb einer eigenen Infrastruktur betrieben und ist damit nur aus dem eigenen Netzwerk zu erreichen. Die Informationen, die in dieser geschlossenen Cloud innerhalb einer Organisation zur Verfügung gestellt werden, können von den zugangsberechtigten Personen genutzt werden. Dies vereinfacht wesentlich die interne Kommunikation und den Informationsaustausch zwischen einzelnen Fachbereichen – unter anderem dadurch, dass die zur Verfügung gestellten Informationen auch von Personengruppen genutzt und verstanden werden, die keinerlei GIS-Kenntnisse haben.

Durch die aktive Mitarbeit in allen führenden GIS-Standardisierungsgremien garantiert Esri die Zukunftssicherheit und Interoperabilität der eigenen Software- und Datenformate. Neben der permanenten Weiterentwicklung bestehender Anwendungen wird die ArcGIS-Produktpalette kontinuierlich erweitert. Dabei setzt Esri auf modernste Technologien sowie offene und skalierbare Systeme und setzt so Trends in der GIS-Branche.



GIS verwandelt Ihre Daten in interpretierbare Informationen.

Foto: EP/Esri

Zahlreiche Partner bauen auf die Technologie von Esri und entwickeln für den Sicherheitsmarkt spezialisierte Lösungen, die auch heute schon in vielen Behörden und Organisationen mit Sicherheitsaufgaben in Deutschland und weltweit zum Einsatz kommen. Esri stellt mit ArcGIS eine komplette Produktfamilie zum Aufbau und zur Nutzung komplexer Geodateninfrastrukturen zur Verfügung und unterstützt seine Partner bei der Durchführung von Projekten.

Die Esri Deutschland GmbH vertreibt als Distributor und Systemhaus die Produkte von Esri Inc., Redlands/Kalifornien (USA), exklusiv über elf Standorte in Deutschland und der Schweiz. Esri unterstützt die Anwender mit einem breit gefächerten Schulungs-, Support- und Consultingangebot und dem gesamten Erfahrungsreichtum von mehr als 450 Mitarbeitern der Esri Unternehmensgruppe.

Für das Marktsegment BOS hat die Esri Deutschland GmbH eine eigene Niederlassung in Bonn aufgebaut, die diesen Bereich in Deutschland und der Schweiz verantwortet. Die Geosecure Informatik GmbH, ein hundertprozentiges Tochterunternehmen der Esri Deutschland Unternehmensgruppe, bietet tief gehendes Know-how für Projektmanagement, Consulting, Entwicklung und Support im sicherheitsaffinen Umfeld.

Kontakt

Esri Deutschland GmbH
Niederlassung Bonn
Rheinallee 24
D-53173 Bonn
Telefon +49 89 207 005 1720
info@bonn.esri.de

Exzellenz fördern

Zukunftspreis Polizeiarbeit "Soziale Netzwerke"

(EP/lin) Polizei und Behörden und Organisationen der Inneren Sicherheit Deutschlands stehen vor großen Herausforderungen. Eng bemessene Haushalte, der demographische Wandel und die neuen Bedrohungen durch den Cyber-Raum sind hier zu nennen. Qualifikation und Exzellenz sind daher notwendig.

Wie kann die Polizei diesen neuen Bedrohungen und Aufgabenfeldern begegnen?
Dieser Frage widmet sich der 16. Europäische Polizeikongress mit dem Titel "Schutz und Sicherheit im digitalen Raum" und den Schwerpunktthemen "Polizei in Sozialen Netzwerken", "ePolice" und "Ausrüstung und Ausstattung".

Zukunftspreis Polizeiarbeit
Soziale Netzwerke

Exzellenz fördern

Zum 16. Europäischen Polizeikongress hat der Behörden Spiegel mit der Cyber Akademie (CAk) erstmalig den Zukunftspreis Polizeiarbeit ausgelobt, der in diesem Jahr mit dem Titel "Soziale Netzwerke" verliehen wird.
Herausragende Master-, Bachelor- und andere Arbeiten von Studenten in den Fachhochschulbereichen Polizei, Justizvollzug und Sicherheitsmanagement sowie kriminologischer Institute der Universitäten werden mit diesem Preis ausgezeichnet.
Honoriert werden Arbeiten, die neue Lösungsansätze und Innovationen für die polizeiliche Facharbeit vorschlagen.
Die eingereichten Arbeiten wurden von einer Fachjury, bestehend aus namhaften Experten der Inneren Sicherheit Deutschlands, bewertet.

Info

Der **Zukunftspreis Polizeiarbeit "Soziale Netzwerke"** wird im Plenum des 16. Europäischen Polizeikongresses verliehen.
⇢ Mittwoch, den 20. Februar 2013, 12:15 Uhr