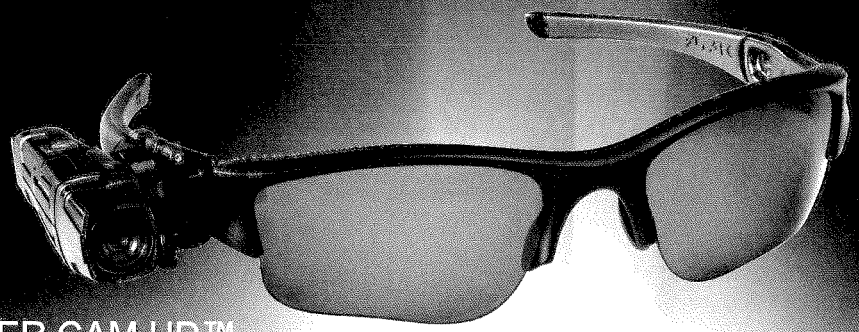
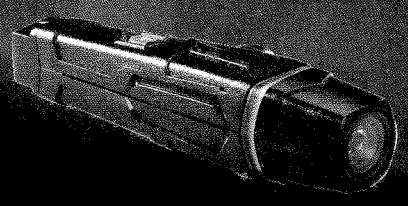
AXON flex™



TASER CAM HD™

STREAM LIFE - ANYTIME, ANYWHERE! - WHEN REQUIRED.



BENEFITS OF AXON FLEX

- Protect yourself from false complaints and avoid frivolous lawsuits
- Protect tax payer money by reducing these complaints and lawsuits
- Protect the truth by accurately capturing video from the officer's perspective
- Enhance community transparency and strengthen public trust
- Improve behavior during public interactions
- Secure download via evidence.sync ™

www.TASER.com

Cyber Akademie

Ausbildungs- und Kompetenzzentrum für IT-Sicherheit

(EP/Ralf Kaschow*) Eine wesentliche Grundvoraussetzung für das Funktionieren unserer modernen Gesellschaft sind Informations- und Kommunikationstechnologien (ITK) und das Internet. Mit der zunehmenden Abhängigkeit der digitalen geschäftlichen wie privaten Kommunikation und Datenübertragung vom Netz hat sich auch die Kriminalität in der digitalen Welt erheblich ausgebreitet.

Dabei steht diese Entwicklung erst am Anfang und wird durch die Popularität von mobilen Endgeräten noch weiter gesteigert. Neben all den Vorteilen, welche das Internet heute mit sich bringt, gibt es auch dunkle Seiten. Eine neuartige Form der Kriminalität, die Internet-genuine "Cybercrime", umfasst bislang unbekannte Arten und Dimensionen der Kriminalität. Sie beinhaltet diverse Betrugsformen und Erpressung mit sensiblen Daten, aber auch gezielte Wirtschaftsspionage. In deutschen Behörden und Verwaltungen stellt der Zugriff auf Adressdaten und vertrauliche Vorgänge ein lohnenswertes Ziel für Hacker dar. Nicht zuletzt sind Verwaltungsnetzwerke selbst im Fokus von Cyber-Kriminellen, um sie z. B. als Bot-Netze zu instrumentalisieren. Hinzu kommt die Bedrohungslage durch globalen Cyber-Terrorismus, der insbesondere Kritische Infrastrukturen (KRITIS) zum Ziel haben kann.

Welche weitreichenden Auswirkungen Cyber-Angriffe auf eine ganze Nation haben können, hat beispielsweise 2007 der großangelegte Bot-Netz-Angriff auf IT-Strukturen in Estland gezeigt.

Hinzu kommen Trends wie Cloud Computing und Soziale Netzwerke, welche neue Fragen hinsichtlich einer wirksamen Absicherung aufwerfen.

Nicht nur die bestehenden Infrastrukturen, sondern auch die Komplexität der IT-Systeme, die Vielfalt der möglichen Bedrohungen und deren rasante und stetig steigende Weiterentwicklung stellen die Behörden und Organisationen mit Sicherheitsaufgaben (BOS) und insbesondere die Polizei vor große Herausforderungen und lassen sie an ihre Grenzen stoßen.

Das Personal der öffentlichen Verwaltung und der Behörden muss daher heute über die notwendigen Qualifikationen verfügen, um Sicherheitsrisiken in Verbindung mit Internet und Datenschutz erkennen, handhaben und letztendlich auch entsprechend aktiv werden zu können.

Das Ausbildungsangebot der Cyber Akademie

Die Cyber Akademie (CAk) bietet praxisorientierte Seminare und Workshops an, welche dem oben beschriebenen Qualifikationsbedarf der öffentlichen Verwaltung gerecht werden.

Anerkannte Experten und Praktiker weisen in rechtliche Grundlagen, technologische Aspekte, Risikoanalyse und -management, Schutzmaßnahmen, organisatorische Herausforderungen, aktuelle Methoden etc. ein.

Adressiert werden Mitarbeiter und Führungskräfte aus Kommunal- und Landesverwaltungen, kommunalen Wirtschaftsbetrieben und Sicherheitsbehörden.

Die Seminarteilnehmer erhalten die Möglichkeit, eine TÜV-Personenzertifizierung nach internationalen Standards, z. B. der ISO 27001, zu erwerben.

CAk Cyber Akademie

Der Programmbeirat der CAk setzt sich aus namhaften Persönlichkeiten aus öffentlicher Verwaltung und Wissenschaft zusammen. Maßgeblich wirken Bernhard Witthaut, Bundesvorsitzender der Gewerkschaft der Polizei (GdP), und Martin Schallbruch, IT-Direktor im Bundesministerium des Inneren, an den Programm- und Ausbildungsleitlinien der CAk mit.

Die Ausbildungsveranstaltungen der CAk finden bundesweit in ausgewählten Konferenzzentren statt. Auf Anfrage werden auch Inhouse-Seminare bei Behörden vor Ort durchgeführt. Dabei können die Seminarinhalte auf den Bedarf der jeweiligen Teilnehmer zugeschnitten werden (z. B. Fokussierung auf spezifische Landesdatenschutzgesetze).

Das Ausbildungsangebot der CAk wird kontinuierlich ausgebaut und weiterentwickelt.

TÜV-Personenzertifizierungen bietet die CAk in Kooperation mit dem TÜV Rheinland für die Seminare zum Datenschutzbeauftragten, Datenschutzkoordinator, IT-Sicherheitsbeauftragten und IT-Sicherheitskoordinator in der öffentlichen Verwaltung an.

In weiterführenden Seminaren geben Praktiker aus Unternehmen und Verwaltung ihre Erfahrungen in der konkreten Umsetzung von Informations- und Kommunikationsstrukturen, IT-Sicherheitsmaßnahmen und BSI-Grundschutz wieder.

Fortbildungsseminare der CAk greifen aktuelle Problemstellungen und Trends auf. Derzeit werden Themen wie Internet Protocol v6 (IPv6), Mobile Device Security, Cloud Computing, Big Data und Social Networks behandelt.

Bestandteile von CAk-Seminaren sind auch praktische Übungen, welche Sicherheitslücken und Angriffsmethoden von Hackern unmittelbar nachvollziehbar machen.

Über den Ausbildungsauftrag hinaus versteht sich die CAk als Kommunikationsplattform und Kompetenzzentrum, welches Experten und Verantwortliche aus Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Unternehmen und Wissenschaft zusammenbringt und an der Entwicklung von Strategien beratend mitwirkt.

**Der Autor ist Geschäftsührer der Cyber Akademie*

Weitere Informationen unter: www.cyber-akademie.de

Transform Police

Die Lösung von Capgemini für das Polizeiwesen der Zukunft

(EP) Gesellschaft, Technologie und Kriminalität sind im Wandel – weltweit stehen Polizeiorganisationen vor der Herausforderung, ihre grundlegende Strategie zu überdenken. Die Budgetsituation engt dabei den Spielraum deutlich ein.

Das rapide Wachstum Sozialer Netzwerke, das die Reaktionszeiten auf Ereignisse drastisch verkürzt, trägt erheblich zu diesem Wandel bei. So entstehen neue Rahmenbedingungen, die sich nicht nur auf soziale, sondern auch auf kriminologische Muster auswirken.

Vor diesem Hintergrund wird die Optimierung der nationalen und internationalen Zusammenarbeit von Polizeiorganisationen immer wichtiger. Hierfür müssen die Akteure aller Ebenen stärker vernetzt, die Kommunikation effizienter und Dienstleistungen gemeinsam genutzt werden – unabhängig von Zuständigkeiten und organisatorischen Grenzen.

Capgemini entwickelt und implementiert Lösungen, die Polizeiorganisationen ermöglichen

1. ihre Mittel auf den Dienst für die Gemeinschaft zu fokussieren,
2. Informationen zur Kriminalitätsbekämpfung bereitzustellen und zu verteilen und
3. wirtschaftliche und zukunftsfähige Polizeidienste zu liefern.

Mit Transform Police (t-police) unterstützt Capgemini die Polizei bei der Transformation ihrer IT-Umgebung hin zu mehr Effizienz und Effektivität. t-police ist eine flexible Technologieplattform, die alle Prozesse moderner Polizeiarbeit in einer integrierten Lösung vereint. Dabei werden wichtige Fragestellungen berücksichtigt:

- Wie kann mit begrenzten Mitteln dauerhaft die Kriminalitätsrate gesenkt, das Recht durchgesetzt und die Öffentlichkeit geschützt werden?
- Wie können die Kosten gesenkt und das übergreifende Potenzial neuer Werkzeuge sowohl für den Polizisten im Außendienst als auch für die Führung in den zentralen Dienststellen demonstriert werden?
- Wie kann, über Abteilungs- und Zuständigkeitsbereiche hinaus, eine sichere Umgebung für die gemeinsame Nutzung kritischer Informationen geschaffen werden?
- Wie können aus sämtlichen zur Verfügung stehenden Informationen Trends und Muster identifiziert werden, die helfen, Ereignisse vorherzusehen und zu verhindern?

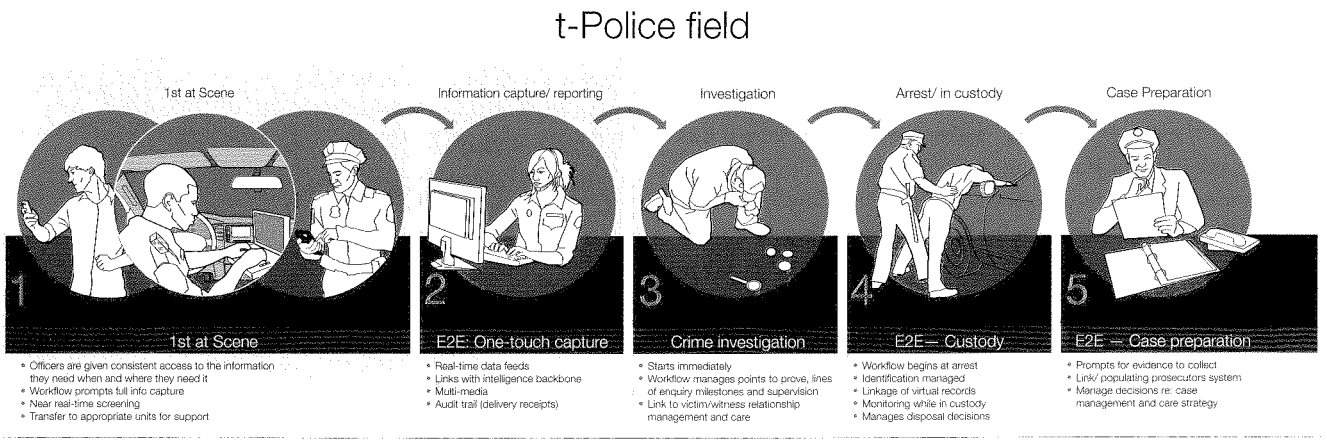
Bessere Resultate in kürzerer Zeit

Weltweit herrscht im Polizeisektor der dringenden Bedarf, operative, verwaltungsorganisatorische und strategische Funktionen in einer Lösung zu vereinen. Mit t-police setzt Capgemini bei genau diesen Herausforderungen an und bildet die Realität der modernen Polizeiarbeit ab. Die Lösung kann in jede bereits bestehende Anwendungslandschaft integriert werden. Sie verringert den administrativen Aufwand, erleichtert und beschleunigt die Kommunikation und reduziert Fehler und Systemausfälle.

t-police basiert auf den folgenden Prinzipien:

- Einfache und kontrollierte Einführung: Eine stufenweise Einführung der priorisierten Einzelkomponenten schafft schnelle Ergebnisse und Planungssicherheit bei der Umsetzung.
- Integriert und flexibel: t-police ist darauf ausgelegt, die Bereitstellung von internen und externen Diensten auszubauen und diese in das polizeiliche Gesamtmodell zu integrieren.
- Return on Investment: Dies ist das treibende Prinzip der Lösung. t-police ist dafür entwickelt, Einsparungen innerhalb von Monaten statt Jahren zu realisieren.
- Fokus auf Nachvollziehbarkeit und Lieferfähigkeit: Die Kombination eines vorgefertigten Lösungsmodells mit einem agilen Vorgehen bei der Einführung erlaubt die Fokussierung auf spezifische Anpassungen innerhalb des Projektes.

Mit t-police bietet Capgemini eine optimal an die Bedürfnisse der Polizei abgestimmte Technologieplattform – für den schnellen und gezielten Kampf gegen das Verbrechen.



Bis zum bitteren Ende?

Kampffront Vorratsdatenspeicherung

(EP/Patricia B. Linnertz) Der "blaue Brief" der Europäischen Kommission war nur eine Frage der Zeit. Die Bundesrepublik Deutschland hatte bis Ende April 2012 Zeit, um für die Umsetzung der bereits 2006 beschlossenen Richtlinie über die Vorratsdatenspeicherung zu sorgen.

Im Sommer letzten Jahres hat die Europäische Kommission die Bundesrepublik Deutschland vor dem Europäischen Gerichtshof (EuGH) verklagt. Doch eine Einigkeit zu diesem Thema schien und scheint in weiter Ferne. Die europäische Richtlinie verpflichtet die Mitgliedsstaaten seit September 2007 dafür zu sorgen, dass Telefon- und Internetanbieter Verbindungs- und Standortdaten für die Strafverfolgung speichern. Doch gerade diese Speicherung wird heftiger diskutiert als jedes andere Thema.

Bundesjustizministerin Sabine Leutheusser-Schnarrenberger will einen anderen Weg und die Vorratsdatenspeicherung auch unter strengen Auflagen nicht mehr zulassen. Ihr Vorschlag ist das so bezeichnete Quick-Freeze-Verfahren. Dabei können Daten unter relativ geringen Voraussetzungen mittels einer Sicherungsanordnung festgehalten, "eingefroren", werden. Nach genauer Prüfung könnten diese dann durch einen Richter "aufgetaut" werden. Dabei ergeben sich allerdings zwei kleinere Probleme. Zum einen müsste eine Speicherung der Daten von den Ermittlungsbehörden sehr früh beantragt werden, zum anderen würde diese Lösung die europäische Richtlinie nicht umsetzen.

An der Front der Vorratsdatenspeicherung kämpfen aber nicht nur die beiden Koalitionspartner. Die SPD spricht sich grundsätzlich nicht gegen die anlasslose Vorratsdatenspeicherung aus, fordert aber eine kürzere Speicherdauer. Drei Monate sollten, so habe es die Ermittlungspraxis gezeigt, in aller Regel ausreichen. Zudem sollten die Ermittlungsbehörden nur unter strengen Auflagen, worunter die Feststellung schwerster Gewalttaten und ein richterlicher Beschluss zählen, auf die Daten zurückgreifen können.

"Wir leben in einer großen demokratischen Familie, in der es auch einige kritische Stimmen gegen die Vorratsdatenspeicherung gibt. Doch obwohl es Einwände gibt, ist die Vorratsdatenspeicherung ein unbedingt erforderliches und wichtiges Mittel. Die viele Diskussionen, die über die Einführung geführt werden, sind jedoch teilweise absurd und ohne jeglichen Inhalt.

Die Ständige Konferenz der Innenminister und -senatoren der Länder ist sich über die Notwendigkeit der Vorratsdatenspeicherung einig. Sie wollen es, und genau das zählt", sagt Michael Hartmann, Innenpolitischer Sprecher der SPD-Bundestagsfraktion gegenüber dem Behörden Spiegel.

Die LINKE lehnt die Vorratsdatenspeicherung dagegen konsequent ab. Eine sechsmonatige Speicherung von Daten leiste keinen sinnvollen Beitrag für kriminalistische Ermittlungen.

Vorratsspeicherung aller Telekommunikationsdaten bedeute praktisch: Alles wird registriert und gespeichert, wer hat wann von wo mit wem telefoniert, wer hat wem eine SMS oder E-Mail geschickt, wer hat wann welche Webseite aufgerufen. Damit werde die Unschuldsvermutung auf den Kopf gestellt und das informationelle Selbstbestimmungsrecht, ein im Grundgesetz verbrieftes Bürgerrecht, ausgesetzt. Verhältnismäßig sei das nicht, zumal das Bundeskriminalamt (BKA) auf eine parlamentarische Anfrage selbst eingeräumt habe: Die Aufklärungsquote könnte mit Vorratsdatenspeicherung lediglich im Promillebereich verbessert werden.

"Also so gut wie gar nicht. Zudem biete ich eine Rechnung an. Gesetzt den Fall, jede zweite Bürgerin oder jeder zweite Bürger würde einmal am Tag telefonieren, eine E-Mail und eine SMS verschicken sowie eine Webseite anklicken. Die dabei anfallenden Daten würden sechs monatelang gespeichert. Heraus kämen ca. 5,5 Milliarden Datensätze. Ein Sack Flöhe hüten ist leichter und die Missbrauchsgefahr ist groß, wie man nach den Datenpannen der letzten Jahre weiß. Datenschutz ist übrigens kein Täterschutz, wie gelegentlich behauptet wird. Das Bundesverfassungsgericht hat sinngemäß mehrfach begründet: Bürgerinnen und Bürger, die nicht mehr

wissen oder wissen können, wer was über sie weiß, sind nicht mehr souverän. Wer nicht mehr souverän ist, kann auch kein Souverän sein. Eine Demokratie ohne Souveräne wiederum ist undenkbar. Die Vorratsdatenspeicherung ist mithin der Demokratie abträglich. Bleibt die EU-Order, der man sich fügen müsse. 2005 sprach sich der Bundestag gegen die Vorratsdatenspeicherung aus. Die Bundesregierung wurde beauftragt, in diesem Sinne auch in der EU zu agieren. Tat sie aber nicht", sagt Petra Pau, Vizepräsidentin des Deutschen Bundestages.

Auch die Grünen wehren sich gegen die Wiedereinführung der anlasslosen verpflichtenden Massenspeicherung der Telekommunikationsverkehrsdaten aller Bürgerinnen und Bürger. Das gegenwärtige Drängen auf Wiedereinführung der Vorratsdatenspeicherung sei unvernünftig.

"Das Bundesverfassungsgericht hat deshalb völlig zu Recht Anfang 2010 die bis dahin bestehende Regelung für nichtig erklärt. Denn die Verkehrsdaten der Telekommunikation, also wer wann mit wem wie lange und auch von welchem Ort telefoniert hat, einschließlich auch der Informationen etwa über den Zeitpunkt des Internetzugangs, fallen unter das grundrechtlich geschützte Telekommunikationsgeheimnis. Grund hierfür ist der Erhalt des in demokratischen Rechtsstaaten besonders wichtigen Vertrauens in die Telekommunikation, bei der im Gegensatz zur unmittelbaren Kommunikation nicht persönlich sichergestellt werden kann, wer alles und in welchem Umfang vom Gespräch Kenntnis nimmt.

Heute bietet die zunehmend allumfassende Digitalisierung unseres Alltages eine breite Vielfalt von neuen Ermittlungsansätzen. Es ist deshalb unredlich, wenn so getan wird, als ob die Strafverfolgung ohne TK-Vorratsdatenspeicherung zukünftig im Dunkeln tappen würde, das Gegenteil ist der Fall. Angesichts der drohenden massenhaften Betroffenheit der Daten völlig unbeteiligter Bürger im Rahmen von Strafverfahren wäre die Vorratsdatenspeicherung ein Dammbruch zulasten der Bürgerrechte. Wir können es uns nicht leisten, das Vertrauen in die unbefangene Nutzbarkeit unsere modernen Kommunikationsinfrastrukturen derartig zu beschädigen", betont Dr. Konstantin von Notz, Mitglied im Innenausschuss des Deutschen Bundestages.

Die CDU/CSU Bundestagsfraktion blickt dennoch positiv gestimmt in die nahe Zukunft.

"Es gibt die Chance, Regelungen zur Vorratsdatenspeicherung noch in dieser Legislaturperiode zu schaffen. Sie muss genutzt werden und besteht darin, dass die grundsätzliche Speicherpflicht der Provider, die uns von der EU zurecht aufgegeben wurde, anerkannt wird. Alles Weitere ist zwischen den Koalitionsfraktionen kompromissfähig: bspw. Speicherdauer, Zugriffsbefugnis auf die Daten, Schutz vor Missbrauch der gespeicherten Daten etc. Deutschland wird sich ein Ausscheren aus der europäischen Vorratsdatenspeicherung auf Dauer nicht leisten können. Keinesfalls darf es dazu kommen, dass Deutschland tausende von Euro Bußgelder der EU auf dem Altar eines falsch verstandenen Datenschutzes opfert", sagt Dr. Hans-Peter Uhl, Innenpolitischer Sprecher der CDU/CSU-Bundestagsfraktion, European Police.

Das gelöschte Internet

Warum das Netz ein Wohnzimmer ist

(EP) Wie verhält sich der Deutsche im Internet? Wie bewegt er sich dort? Welches Lebensgefühl, welche Orientierung, welches Vertrauen zeigt er im Netz? Diesen grundsätzlichen, aber auch weiteren Fragen, widmet sich die DIVSI-Milieu-Studie zu Vertrauen und Sicherheit im Internet, eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI).

Bislang gehen Studien zum Internet von einer einfachen Statistik aus: Deutschland besteht aus 80 Prozent "Onlinern", also Menschen, die einen Zugang zum Internet haben, und 20 Prozent "Offlinern", eben jenen ohne den Netzzugang. "Der Zugang als Kriterium wird aber zukünftig nicht mehr die Relevanz haben", erläuterte Matthias Kammer, DIVSI, vergangenes Jahr in Berlin. Der Deutsche und das Internet müssten heute vielmehr aus der Perspektive des Gesamtalltags der Menschen betrachtet werden. Diese Ethnologie des Alltags ist Basis der neuen Studie.

"Digital Outsiders", "Digital Immigrants" und "Digital Natives"

Im Ergebnis zeigt sich, dass der Deutsche im Internet sich in drei grobe Gruppen unterteilt, die jeweils wiederum Subgruppen umschließen. Grundsätzlich zu unterscheiden, und auch deutlich voneinander zu trennen, sind die "Digital Outsiders" von den "Digital Immigrants" und den "Digital Natives". Innerhalb der Digital Outsiders haben sich derzeit die Gruppen der "Internetfernen Verunsicherten" und die der "Ordnungsfordernden Internet-Laien" herausgebildet. Die "Verunsicherten" kennzeichnen sich als überforderte Offliner bzw. Internet-Gelegenheitsnutzer. Zumindest kennzeichnet dies ihr Verhalten im Netz. Die private Lebenswelt dieser Gruppe zeichnet sich durch Selbstgenügsamkeit, Sittlichkeit und Anstand sowie ein Bedürfnis nach Schutz und Kontrollmechanismen aus. "Die private Lebenswelt eines Menschen zeigt sich in seinem Wohnzimmer. Wie ist dieses gestaltet? Regale eines schwedischen Konzerns oder Antiquitäten? Übertragen auf das Verhalten im Netz stellten wir uns die Frage: Wo steht der Computer?" erläuterte Dr. Silke Borgstedt. Auf diese erste Gruppe bezogen ist die Antwort recht eindeutig: Der Computer steht im Hauswirtschaftsraum, neben dem Bügelbrett. Aber nicht nur die Wohnungseinrichtung spiegelt sich im Netz-Verhalten, sondern genauso die Werteorientierung einer Person. "Ein typischer Satz der Internetfernen Angst, aus Versehen mit der falschen Taste das Internet zu löschen", führte Dr. Borgstedt weiter aus.

In der Gruppe der "Digital Immigrants" werden die "Verantwortungsbedachten Etablierten" von den "Postmateriellen Skeptikern" unterschieden. Die "Etablierten" sind selektive Internet-Nutzer, haben Führungsbewusstsein und eine verantwortungsorientierte Grundhaltung gegenüber digitalem Fortschritt. Die "Skeptiker" wenden das Internet zielorientierter an, haben aber eine kritische Einstellung zu kommerziellen Strukturen und blinder Technik-Faszination. "Hier steht der Computer nicht mehr im Abstellraum, aber noch in der Ecke", so Dr. Borgstedt.

Die "Digital Natives" teilen sich in die Gruppen der "Unbekümmerten Hedonisten", der "Effizienzorientierten Performer" und der "Digital Souveränen". In ihre Lebensphilosophie eingeteilt unterscheiden sich hier Fun-orientierte Internet-User von leistungsorientierten Internet-Profis und von einer digitalen Avantgarde mit ausgeprägter individualistischer Grundhaltung. "Hier haben wir es mit klassischen Fällen zu tun. Schwedische Möbel, Flohmarkt-Möbel, und Obst findet sich als Markenname auf dem Computer."

Die DIVSI-Milieu-Studie kommt letztendlich zu dem Ergebnis, dass Verhalten im Netz die grundlegende Werte-Orientierung eines Menschen widerspiegele. Und in dieser sehr vielfältigen digitalen Gesellschaft gebe es weit mehr Wohnzimmereinrichtungen als 20 Prozent Spanplatten-Möbel und 80 Prozent aus Massivholz.

Der bestmögliche Schutz

Abhör- und manipulationssichere Verbindungen

(EP) Nicht nur Staat und Militär sind in Zeiten von Industriespionage und Internetkriminalität auf abhör- und manipulationssichere Kommunikationsverbindungen angewiesen, sondern auch die Wirtschaft. Hard- und Software für den hochwirksamen Schutz von Informationen entwickelt und produziert die Rohde & Schwarz SIT GmbH, ein weltweit aufgestellter Spezialist für intelligente Verschlüsselungs- und IT-Sicherheitskonzepte.

Die sich durch die zunehmende Verbreitung von Internet, Social Media und Cloud-Anwendungen ergebenden Möglichkeiten stoßen in Behörden und Unternehmen nicht immer auf uneingeschränkte Begeisterung. Sie suchen nach Möglichkeiten, ihre nichtöffentlichen Informationen wirksam vor Missbrauch und Diebstahl zu schützen und unerlaubte Aktivitäten zu monitoren beziehungsweise zu verhindern.

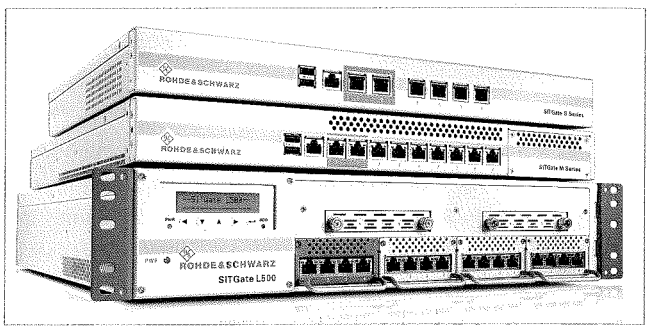
Mit der Next-Generation-Firewall R&S SITGate präsentiert die Rohde & Schwarz SIT GmbH dafür eine überzeugende Lösung. Das Produkt bietet kontinuierliche Anwendungserkennung durch Deep Packet Inspection, Intrusion Prevention sowie einen effektiven Schutz vor Malware. Bedrohungen durch Bot-Netze, Web-2.0-Anwendungen und Zero-Day-Angriffe über den Internetzugang oder Cloud-Provider werden mithilfe der kontextbezogenen Protokollanalyse zuverlässig und in Echtzeit aufgedeckt, ebenso wie Angriffe über verschlüsselte Verbindungen. Der integrierte VPN-Konzentrator gewährleistet zudem die sichere Anbindung externer Standorte und mobiler Anwender.

Ein weiteres Anwendungsfeld ist die Verwendung von Carrier- oder Metro-Ethernet als effiziente Weitverkehrs-Übertragungstechnik, die jedoch keine Manipulationssicherheit bietet. Auf der sicheren Seite sind Nutzer des derzeit einzigen BSI-zugelassenen Ethernet-Verschlüsselers mit erweitertem Temperaturbereich von -20° bis +70°C. Das R&S SITLine ETH50 lässt sich dank des lüfterlosen Designs in unklimatisierten Räumen einsetzen, direkt am Schreibtisch oder mobil in Fahrzeugen und Satcom-Kits. Es ist für den Vertraulichkeitsgrad VS-NfD und NATO Restricted zugelassen.

"Wirtschafts- und Industriespionage sowie Internetkriminalität haben bedenkliche Ausmaße erreicht", gibt Peter Rost, Leiter Produktmanagement und Strategisches Marketing, zu bedenken. "Rohde & Schwarz verfügt über das Know-how und die erforderlichen Produkte, um dem Missbrauch einen Riegel vorzuschieben. Was an Hard- und Software benötigt wird, produzieren wir in Deutschland und decken hierbei auf Wunsch die gesamte Wertschöpfungskette ab. Eine vergleichbar vertrauenswürdige Produktionsumgebung bietet in der Branche sonst kaum jemand an. Daher bedienen wir auch ein breites Branchenspektrum, das von der Industrie bis zu Behörden und dem Militär reicht."

In den vier Geschäftszweigen Messtechnik, Rundfunk, Sichere Kommunikation sowie Überwachungs- und Ortungstechnik betreut die weltweit operierende Firmengruppe vornehmlich Kunden aus der Mobilfunk-, Rundfunk- und Elektronikindustrie sowie aus den Bereichen Luftfahrt, Verteidigung, Homeland Security und Kritische Infrastrukturen.

"Rohde & Schwarz SIT ist innerhalb des Konzerns seit über 20 Jahren zuständig für Verschlüsselung und sichere IT", fügt Peter Rost hinzu. "Anfangs betreuten wir hauptsächlich öffentliche Auftraggeber, zumeist Institutionen der Bundesrepublik Deutschland und ihrer Verbündeten. Ein wichtiges Thema ist nach wie vor die Sprachverschlüsselung auf einem Niveau, das den Anforderungen von Regierungen entspricht und den Einsatz in militärischen Umgebungen erlaubt. Auftraggeber ist jedoch zunehmend auch die Industrie, die intelligente IT-Sicherheitsprodukte mit minimalem administrativem Aufwand benötigt. Unsere daraus resultierenden, kostengünstigen und einfach zu nutzenden COTS-Produkte (Commercial off-the-Shelf) kommen wiederum auch Behörden zugute."



Firewalls mit Anwendungserkennung durch Deep Packet Inspection bieten Schutz vor Zero-Day-Angriffen und Datenverlust. Foto: EP/Rohde&Schwarz

Das Produktprogramm der Rohde & Schwarz SIT basiert auf Verschlüsselungs- und Absicherungslösungen für Netzwerke und die Ende-zu-Ende-Kommunikation sowie speziellen Hardwaremodulen für hochsichere elektronische Identitäten wie den neuen Personalausweis und andere Public-Key-Infrastrukturen. Es umfasst auch die neue, global einsetzbare mobile SVoIP-Lösung für iPhone und Android-Smartphones, auf Basis des verbreiteten TopSec-Mobile-Kryptoheadsets.

Seit 2004 ist Rohde & Schwarz SIT ein IT-Sicherheitspartner der Bundesrepublik Deutschland. Überdies werden verschiedene NATO-Ausrüstungsprogramme vom weltweit aufgestellten Verschlüsselungsspezialisten bedient.

Kontakt

ROHDE & SCHWARZ SIT GmbH
Am Studio 3, D-12489 Berlin
Telefon: (030) 65 88 4 - 223
Telefax: (030) 65 88 4 - 183
info.sit@rohde-schwarz.com
www.sit.rohde-schwarz.com

IT-Sicherheitsstruktur 2020

100 Prozent Sicherheit gibt es nicht

(EP) Eine der meistgebrauchten Aussagen in der IT-Sicherheitsbranche lautet: "100 Prozent Sicherheit gibt es nicht." So richtig diese Aussage im Grunde ist, so wird sie doch oft genug auch als Vorwand benutzt, um zu kostenintensive Präventionsmaßnahmen zu verhindern, oder als Euphemismus, um Probleme zu verharmlosen. Aber ist das wirklich alles, was hinter dieser Aussage steckt?

In der IT wird das zur Verfügung stehende Sicherheitsbudget fast ausschließlich für Maßnahmen zur Verhinderung von Vorfällen ausgegeben. D. h. wir bauen sehr hohe Zäune um unsere IT-Systeme, und mit Blick auf das Motto "Defense in Depth" errichten wir hinter dem Zaun auch noch eine Mauer. Inwieweit ist das alles aber überhaupt sinnvoll?

Abschreckung durch hohe Aufklärungsquoten

Sind Zäune und Mauern der einzige Weg zum Schutz unseres "Werksgeländes"? Allzu gerne wird die Abschreckung durch hohe Aufklärungsquoten, die zielgerichtete Erweiterung der Abwehrmaßnahmen durch gute Angriffsdetektion und die Schadensbegrenzung durch schnelle Reaktion auf Angriffe von den IT-Sicherheitsabteilungen vernachlässigt.

Das nächste Level in der IT-Sicherheit ist die Abkehr von einer rein präventionsgetriebenen Planung. Wir benötigen eine IT-Sicherheitsstruktur, die die Möglichkeit von erfolgreichen Angriffen nicht nur theoretisch anerkennt, sondern ganz konkret und praktisch Vorkehrungen dagegen getroffen hat.

Dipl.-Inf. Florian Oelmaier, Leiter IT-Sicherheit und Computerkriminalität, Corporate Trust – Business Risk & Crisis Management GmbH

Foto: EP/Corporate Trust

Dafür haben wir als IT-Branche noch viele Hausaufgaben zu machen. Und genau hier benötigen wir dringend die Hilfe der Experten für klassische Sicherheit und der Behörden. Diese können ihren ganzen Erfahrungsschatz einsetzen, um die Kollegen aus der IT-Sicherheit bei diesem Wandel zu unterstützen.

Zentrum der Kommunikation

Leitstellentag auf der IPOMEX 2013

(EP) Der Behörden Spiegel, Deutschlands größte unabhängige Zeitung für den Öffentlichen Dienst, veranstaltet im Rahmen der IPOMEX 2013 am Mittwoch, den 17. April den Leitstellenkongress.

Die Einführung des bundeseinheitlichen BOS-Digitalfunks ist aus Sicht der Leitstellen ein hochkomplexes Thema. Darüber erfährt die Leitstellenlandschaft im Rahmen von Strukturreformen vielerorts erhebliche Veränderungen.
Regionale, integrierte, kooperative, vernetzte und virtuelle Leitstellen sind Lösungen, die diskutiert werden und zur Disposition stehen. Planer, Nutzer und Hersteller müssen nicht nur mit einer neuen Technik, sondern auch noch mit grundlegend anderen Strukturen und Organisationen umgehen.
Der Aufbau des BOS-Digitalfunks schreitet voran und verlangt rasche Lösungen von allen Beteiligten. In dieser Situation entsteht nicht zuletzt wegen der heutigen heterogenen Leitstellenlandschaften insbesondere im Bereich der Feuerwehr und der Hilfsorganisationen notwendigerweise eine Vielzahl sehr verschiedener Ansätze mit individuellen Architekturen, Komponenten und Schnittstellen, die mit erheblichen Folgekosten verbunden sein können. Wohlüberlegtes Handeln ist deshalb angesagt.

Die IPOMEX, Fachmesse für Behörden und Organisationen mit Sicherheitsaufgaben, findet vom 16.-18. April zum sechsten Mal in Münster statt. Foto: EP/lin

Die Leitstelle – das Zentrum der Kommunikation

Das Motto des Leitstellentages 2013 heißt "die Leitstelle – das Zentrum der Kommunikation der Behörden und Organisationen mit Sicherheitsaufgaben (BOS)". Ziel der Veranstaltung ist die Information über Leitstellenkonzepte, die technische Ausstattung von Leitstellen, deren Anbindung an den Digitalfunk und den durch neue technische Entwicklungen und die Leistungsmerkmale des Digitalfunks zu generierenden Mehrwert mit Blick auf Gegenwart und Zukunft.
Die Themenschwerpunkte des diesjährigen Leitstellentages sind u. a.

- aktueller Sachstand der Einführung des Digitalfunks,
- Zertifizierung der Leitstellen,
- Status des nutzereigenen Managements (NEM),
- Leitstellenkonzepte,
- Anbindung der Leitstellen an den Digitalfunk,
- Sprach- und Datenkommunikationssysteme,
- Einsatzleit-, Führungs- und Geoinformationssysteme,
- operative Umstellung einer Leitstelle (Migration),
- IT-Sicherheit in Leitstellen,
- Nutzung des Web 2.0 und der Social Media in Leitstellen,
- Status des eCall-Pilotprojektes und die Einbindung in die 112-Leitstellen,
- Alarmierung.
- Stabsarbeit/Lagebilddarstellung.

Der Leitstellentag 2013 richtet sich an Führungskräfte und Entscheidungsträger der Behörden und Organisationen mit Sicherheitsaufgaben (BOS): Polizeien des Bundes und der Länder, Berufs-, Freiwillige und Werkfeuerwehren, Hilfsorganisationen und Katastrophenschutz.

Gemeinsam sind wir stark

Wie die ThreatCloud vor Internetkriminalität schützt

(EP) Internetkriminalität ist eine reale, steigende Bedrohung für Privatpersonen, Behörden und Unternehmen. Das Bundeskriminalamt (BKA) kommt in seinem Cybercrime-Bundeslagebild 2011 zu der Schlussfolgerung, dass, "unabhängig von der Entwicklung der reinen Fall- bzw. Schadenszahlen, die aufgrund des vermuteten Dunkelfeldes ohnehin nur eine sehr begrenzte Aussagekraft besitzen", die Intensität der kriminellen Aktivitäten im Bereich Cybercrime und das für jeden Internetnutzer bestehende Gefährdungspotenzial weiter zugenommen hätten.

Das BKA sieht eine "steigende Professionalität der eingesetzten Schadsoftware" und "eine schnelle, flexible und professionelle Reaktion auf technische Entwicklungen auf Täterseite".

Die Täter zielen häufig auf zahlreiche Webseiten und Organisationen gleichzeitig ab, um so die Wahrscheinlichkeit eines Erfolgs zu erhöhen. Da viele Organisationen bei der Bekämpfung solcher Attacken auf sich alleine gestellt sind, bleibt mehr als die Hälfte dieser Gefahren unentdeckt – und es besteht keine Möglichkeit, die Informationen zu diesen Bedrohungen untereinander auszutauschen. Getreu dem Motto "gemeinsam sind wir stark" sollten die Organisationen aber kollaborieren und die Daten zu auftretenden Gefährdungen gemeinsam nutzen. So können sie die Stärken ihrer Security effizienter einsetzen und aktuelle Gefahren abwenden, noch bevor diese ihr Ziel erreichen und ein eventueller Schaden entsteht.

Eine solche Kollaborationsplattform bietet der Sicherheitsanbieter Check Point.

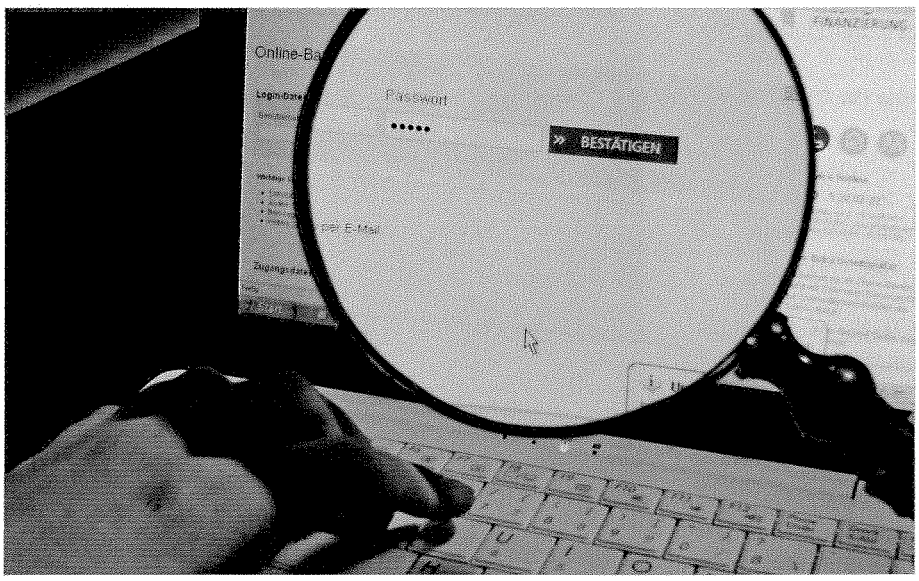
Mit der ThreatCloud betreibt er ein umfangreiches, innovatives Frühwarnsystem. Die Lösung sammelt Gefahreninformationen aus einem weltweiten Netzwerk von Bedrohungssensoren. ThreatCloud speist die Gefahren-Updates direkt in die Gateways der Kundenbasis ein und ermöglicht so die Durchführung präventiver Schutzmaßnahmen gegen neue, hoch entwickelte Gefährdungen wie Bots, APTs (Advanced Persistent Threats) und andere Formen raffinierter Schadsoftware.

Zusätzlich können die Kunden ihre eigenen Gefahrenmeldungen in die ThreatCloud einspeisen. Im Gegenzug erhalten sie über ihre mit "Threat-Intelligenz" angereicherten Security Gateways alle erforderlichen und aktuellen Schutz-Updates. Werden im Netzwerk einer Organisation neue Bots oder neue Malware-Bedrohungen identifiziert, wird der Malware-Identifikator – etwa die IP-Adresse, URL oder DNS – an die ThreatCloud gesendet, die wiederum im Sekundentempo ein Update an sämtliche Peers und Kunden weltweit verschickt. Darüber hinaus bezieht die ThreatCloud auch Daten aus anderen Quellen mit ein, wie zum Beispiel Check-Point-Research, die installierte Basis an Check Point-Security Gateways und branchenspezifische Malware-Feeds.

In Anbetracht all der neuen Formen von Malware, die täglich generiert werden, funktioniert ThreatCloud für die Kunden quasi wie eine Erweiterung seines Security-Radius. Die Organisation erhält deutlich mehr Informationen und Analysen zu Attacken, als sie – auf sich alleine gestellt – jemals bekommen könnte. ThreatCloud basiert auf einer globalen Kollaboration, die das Volumen, die Qualität und die Schnelligkeit von Threat-Informationen signifikant erhöht.

Ein hohes Gefährdungspotenzial bescheinigt das BKA in seinem Cybercrime Lagebild der wachsenden Nutzung mobiler Endgeräte. Diese rücken zunehmend in den Fokus der Kriminellen und müssen besonders geschützt werden. Auch hier bietet Check Point mit Mobile Information Protection ein Datensicherheitskonzept zum Schutz von Daten außerhalb des klassischen Perimeters auf mobilen Geräten, das auf unterschiedlichen Bausteinen – Sicherer Zugriff auf Unternehmensressourcen, Verschlüsselung, Data Loss Prevention – basiert. Im Fachforum IV – Mobile Kommunikation für Sicherheitsbehörden – wird Bernd Ullritz dieses Konzept vorstellen.

Check Point tritt auf dem Kongress gemeinsam mit seinem Platinum Partner Computacenter auf. Im Lösungsbereich "Secure Information" fasst Computacenter alle Lieferungen, Beratungsleistungen und Lösungen zusammen, die dazu beitragen, die Anwendungen und IT-Infrastrukturen von Unternehmen und Behörden zu schützen, sicher zu implementieren und zu betreiben.



Laut dem Bundeskriminalamt (BKA) haben die kriminellen Aktivitäten im Internet weiter zugenommen. Foto: EP/Cristine Lietz/Pixelio.de

Den zukünftigen Herausforderungen stellen

Lösungen und Services für Leitstellen

(EP) Der Bereich Building Technologies der Siemens AG bietet Lösungen und Services rund um das Leitstellengeschäft, speziell für Leitstellen der Feuerwehren, Polizei und Rettungsdienste (BOS-Leitstellen). Siemens stellt sich den aktuellen und zukünftigen Herausforderungen, die die steigenden Anforderungen an die Strukturen und Anforderungen von Leitstellen mit sich bringen. Dies macht es erforderlich, Vertrieb und Service mit der notwendigen Fachkompetenz, Engineeringkapazität und neuen Supportstrukturen zu ergänzen.

Siemensstadt Berlin, Nonnendammallee *Foto:EP/Siemens*

Zum 1. August 2012 wurde deshalb die Gesamtsteuerung aller BOS-Projekte für Siemens in Deutschland in dem "Center of Competence" in Berlin gebündelt. Zu den Aufgaben gehören unter anderem die Abstimmung und Steuerung der erforderlichen Engineeringkompetenzen für projektspezifische Entwicklungen und Systemschnittstellen sowie die Implementierung effizienter Supportfunktionen. Die weiteren Aufgaben des Center of Competence umfassen die Betreuung von Ingenieurbüros, die Unterstützung von Mitarbeitern der Leitstellen und Behörden, Messeauftritte, strategische Workshops und Fachpräsentationen.

Die Leitung des Center of Competence wurde Jörg Marks übertragen. Er ist seit sieben Jahren Leiter der Siemens-Division Building Technologies in der Vertriebsregion Ost und seit mehr als 20 Jahren innerhalb von Siemens tätig.

Aktuelle Leitstellen-Projekte sind unter anderem die "Landeslösung Niedersachsen", die "Landeslösung Thüringen", die Anschaltung an den Digitalfunkan der Polizeilichen Dienste in Berlin und weitere Projekte in allen Bundesländern.

Videoüberwachung auf Plätzen

Ein wesentlicher Beitrag zum Schutz der Bürger

(EP) "2011 sind die registrierten Straftaten an den durch die hessische Polizei videoüberwachten Örtlichkeiten um 19,5 Prozent zurückgegangen", sagt der hessische Innenminister Boris Rhein. Die Videoüberwachung auf öffentlichen Plätzen habe sich damit als ein wirkungsvolles Instrument zur Abschreckung von potenziellen Tätern und zur Aufklärung von Straftaten gezeigt.

Seit 2009 sei es gelungen, die Zahl der Aufzeichnungsanlagen von elf auf 18 zu erhöhen. Damit sind inzwischen 102 statt 48 Kameras in den Anlagen im Betrieb. Die Speicherdauer beträgt in der Regel sieben Tage und für die Bild- bzw. Aufzeichnungsqualität gibt das Hessische Landeskriminalamt (LKA) strenge Maßstäbe vor, die bereits bei der Planung der Anlagen Berücksichtigung finden.
Auf diesem Wege sei – auch mit Blick auf die aktuelle Diskussion um den glücklicherweise gescheiterten Anschlagsversuch in Bonn – sichergestellt, dass eine Täteridentifizierung ermöglicht werde.
Wie wirkungsvoll der Betrieb der Videoüberwachungsanlagen auf Plätzen ist, belegen die Zahlen aus Hessen. Im Jahr 2011 wurden auf videoüberwachten Plätzen insgesamt 1.871 Straftaten registriert, 2006 lag die Zahl mit 3.976 registrierten Straftaten noch deutlich höher. Die hessische Polizei verzeichnete dabei die stärksten Rückgänge im Bereich der Konstablerwache in Frankfurt.

Erfolgreicher Einsatz der Videoüberwachung

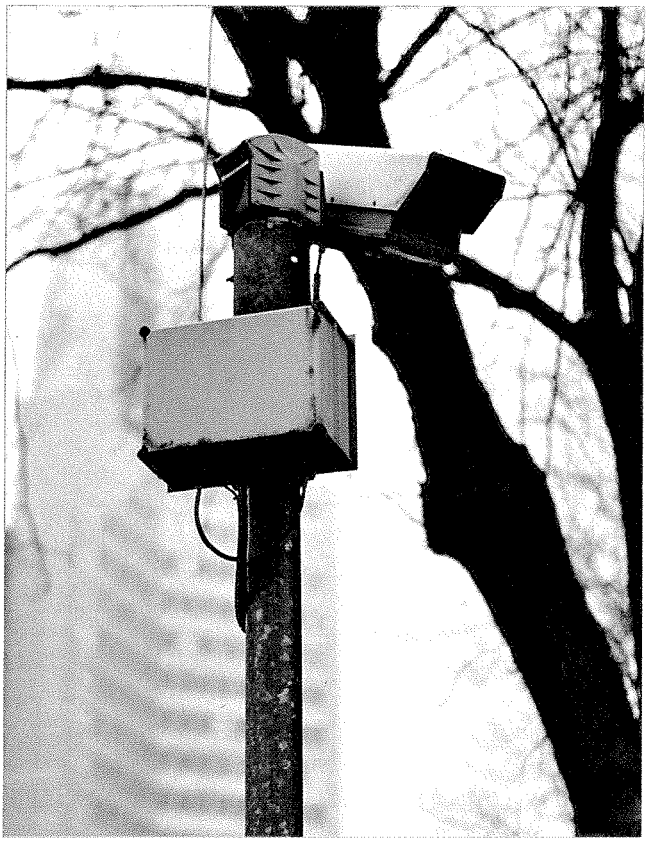
"Insbesondere in den Bereichen der klassischen Beschaffungskriminalität und der Rauschgiftkriminalität konnte die Polizei mithilfe der Videoüberwachung sehr erfolgreich arbeiten. Gerade die Videoüberwachungsanlage an der Konstablerwache ist ein Musterbeispiel für die gelungene Auflösung einer Drogenszene mit der Folge, dass die Bürgerinnen und Bürger den zuvor als Angstraum geltenden Platz wi der bedenkenlos nutzen können und mögen", so Innenminister Rhein.
Zum Zeitpunkt der Inbetriebnahme der Videoüberwachungsanlage im Jahr 2002 wurden an der Konstablerwache 475 Straftaten registriert. Im Jahr 2011 nur noch 196, ein Minus von 58,7 Prozent.
Aufgrund der Bildaufzeichnungen durch die Polizeibehörden fanden landesweit insgesamt 174 gefahrenabwehrende Maßnahmen statt, darunter 59 Platzverweise, 28 Durchsuchungen, fünf Sicherstellungen, 58 Ingewahrsamnahmen und 24 Durchsuchungen von Sachen. In 100 Fällen wurden bei der Auswertung der Bildaufzeichnungen strafrechtlich relevante Sachverhalte festgestellt. Darunter vier Sachbeschädigungen, acht Raubdelikte, 12 Körperverletzungen, 42 Verstöße gegen das Betäubungsmittelgesetz sowie vier Fälle von Hehlerei.
Die Erfahrungen zeigten nach wie vor, dass mithilfe der Videoüberwachung:

- potenzielle Täter abgeschreckt werden,
- bei Gefahren und Straftaten umgehend polizeiliche Maßnahmen eingeleitet werden können,
- begangene Straftaten mit Beweissicherungs- und Identifizierungsmaßnahmen besser aufgeklärt werden.

"Wir wissen natürlich, dass teilweise Verdrängungsmechanismen einsetzen. Durch begleitenden starken Kontrolldruck in den angrenzenden Gebieten ist aber eine Austrocknung bzw. eine Ausdünnung der Szenen an den Brennpunkten zu erreichen. Sobald die Behörden neue Sammelpunkte erkennen, wird das polizeiliche Handeln entsprechend angepasst", erläutert Innenminister Rhein.

Unterstützung der Kommunen

Die Landesregierung unterstützt Kommunen, die Videoüberwachung im öffentlichen Raum planen. Eine Arbeitsgruppe der Polizei hat dazu eine "Handlungsempfehlung für die Errichtung und den Betrieb von Videoüberwachungsanlagen im öffentlichen Raum" erarbeitet sowie die wichtigsten Informationen "auf einen Blick" zusammengefasst.
"Der Einsatz moderner Videotechnik kann nur auf Dauer Erfolg haben, wenn er in ein polizeiliches Gesamt- und Begleit-



In Hessen hat sich die Videoüberwachung auf öffentlichen Plätzen als wesentlicher Erfolg zur Erhöhung der Sicherheit gezeigt. Foto: EP/Alipictures/Pixelio.de

konzept insbesondere für die nähere Umgebung der videoüberwachten Plätze eingepasst ist. Dieses Konzept wiederum muss auf die jeweiligen örtlichen Gegebenheiten abgestimmt sein. Deshalb ist eine enge Zusammenarbeit zwischen der Vollzugspolizei und der Kommune sehr wichtig", erläuterte Rhein. So konnten im Rahmen der Videoüberwachung durch die hessischen Kommunen auch 40 gefahrenabwehrende Maßnahmen durchgeführt werden und zudem 56 strafrechtlich relevante Sachverhalte festgestellt werden.
Besonders erfreulich sei in diesem Zusammenhang, dass es in Hessen gelungen sei, gerade Deliktsformen der Straßenkriminalität, die das Sicherheitsgefühl der Bevölkerung negativ beeinflussen können, zu reduzieren. So hätten sich beispielsweise die Raubstraftaten im videoüberwachten Bereich der Konstablerwache seit Einführung der Videoüberwachung nahezu halbiert. Ebenso seien die registrierten Rauschgiftdelikte von 295 Fällen im Jahr 2000 auf 90 Fälle in 2011 zurückgegangen. Auch in den umliegenden Referenzbereichen (nicht videoüberwachte B-Ebene und Passage der Konstablerwache) sei eine direkte Verdrängung der Szene durch die begleitenden Konzepte des Polizeipräsidiums Frankfurt und der Stadtpolizei verhindert worden.

Als erstes Bundesland eingeführt

"Hessen war bereits im Jahr 2000 das erste Bundesland, das mit der Einführung von Videoüberwachung öffentlicher Straßen und Plätze begonnen hat. Dass dies der richtige Weg war, zeigen die guten Ergebnisse. Die Videoüberwachung hilft dabei, den Bürgerinnen und Bürgern ein Stück Lebensqualität zu geben und ist eine sinnvolle Ergänzung der Polizeiarbeit, die dadurch flexibler erfolgen kann. Daher erscheint mir auch die weitere Einrichtung punktueller Videoüberwachung zielführend", so der hessische Innenminister Rhein abschließend.

Förderung von Videoüberwachungsanalgen

Die hessische Landesregierung stellt jährlich 300.000 Euro für die Förderung der Errichtung von Videoüberwachungsanlagen durch die Kommunen bereit. Die Handlungsempfehlung, die mit dem Hessischen Datenschutzbeauftragten abgestimmt ist, richtet sich sowohl an die Polizei als auch an die Bedarfsträger in den Städten und Kommunen.
In Zusammenarbeit mit der örtlich zuständigen Polizeidirektion bzw. dem Polizeipräsidium und dem Hessischen Landeskriminalamt wird eine Kriminalitätsanalyse für die zu überwachende(n) Örtlichkeit(en) erstellt sowie im Rahmen einer Begehung vor Ort die Art der Videoüberwachungsanlage und Anzahl der anzubringenden Kameras ermittelt. Über die Beratung vor Ort wird ein Beratungsbericht erstellt und auf Basis einer Kostenschätzung ggf. ein Landeszuschuss von bis zu einem Drittel der Errichtungskosten gewährt.

Info

Digitales Bild des öffentlichen Raumes – Videoüberwachung
Ende letzten Jahres ist die Bundesstadt Bonn nur knapp einer Katastrophe entgangen. Eine herrenlos aufgefundene Tasche enthielt tatsächlich eine Bombe mit zündfähigem Material. Es soll jedoch nicht gezündet worden sein. Augenzeugen konnten die Person, von welcher die Tasche abgestellt worden war, gegenüber der Polizei beschreiben.
Obwohl der Hauptbahnhof Bonn videoüberwacht wird, gibt es jedoch keine bewegten Bilder der Sicherheitskameras, die zur eindeutigen Aufklärung beitragen können. Denn mit den bestehenden Anlagen der Deutschen Bahn wurden keine Bilder aufgezeichnet.
Die geringe Qualität von Videoüberwachungsbildern wurde im Rheinland schon einmal bemängelt. Der Kofferbomber von Köln, der im Sommer 2006 Sprengsätze in Regionalzügen deponiert hatte, war auf den Bildern der örtlichen Überwachungskameras kaum zu erkennen.
Nach dem versuchten Anschlag am Bonner Hauptbahnhof steht die Videoüberwachung des öffentlichen Raumes erneut in der Diskussion.
Der Vorstandsvorsitzende der Deutschen Bahn, Rüdiger Grube, hat jetzt intern erklärt, dass die Bahn in Absprache mit der Bundespolizei ihre Anlagen nun verstärkt überwachen wird. Es stehen also Beschaffungen an.
⇢ Mittwoch, den 20. Februar 2013, von 15:30 Uhr bis 17:00 Uhr

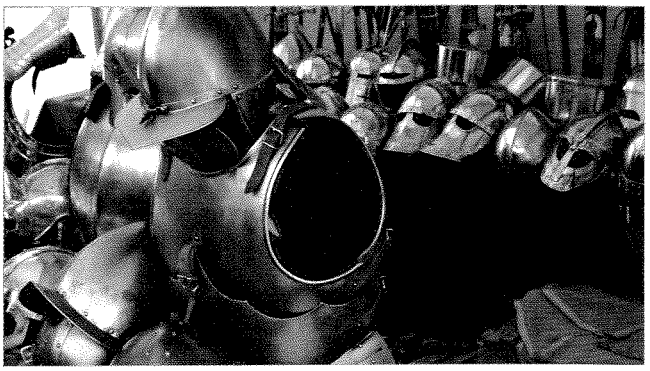
"Schutzlücken sind intolerabel!"

Das Schlachtfeld des 21. Jahrhunderts

(EP) Die Innere Sicherheit Deutschlands steht vor großen Herausforderungen, wie Hans-Joachim Schaprian, Friederich-Ebert-Stiftung, im Rahmen des Sicherheitspolitischen Forums NRW 2012 in Bonn erläuterte: Terrorismus, Extremismus und Organisierte Kriminalität (OK) seien reale Bedrohungen, das Internet aber werde sich zum "Schlachtfeld des 21. Jahrhunderts" entwickeln.

Durch Cyber-Kriminalität entstehe jährlich ein weltweiter Schaden von rund 745 Milliarden Euro. Alleine in Deutschland liege der jährliche Schaden bei rund 50 Milliarden Euro. "Wir sehen uns einem Wettrüsten in der Cyber-Sicherheit gegenüber. Hier müssen die Behörden und Organisationen mit Sicherheitsaufgaben zusammenarbeiten und an einem Strang ziehen", so Schaprian.

"Cyber Crime ist ein Problem, das wir national nicht mehr lösen können", betonte auch Ralf Jäger, Minister für Inneres und Kommunales des Landes Nordrhein-Westfalen in Bonn. Es sei eine internationale Zusammenarbeit von Sicherheitsbehörden und Justiz notwendig. "Die Sicherheitsbehörden müssen sich globalisieren", so Jäger weiter. Das besondere Problem der Cyber-Kriminalität liege in der Thematik der Datenspeicherung. "Die Datenspeicherung ist keine neue Erfindung. Die gibt es seit der Erfindung des Telefons. Mit den derzeitigen gesetzlichen Vorgaben haben wir allerdings eine Schutzlücke in Deutschland erreicht, die nicht mehr tolerabel ist. Das können wir uns nicht mehr leisten", betonte der nordrhein-westfälische Innenminister. Es sei eine Abwägung der individuellen Freiheit zugunsten der Sicherheit zu diskutieren. Zudem müsse man sich Gedanken über die Ausgestaltung der Datenspeicherung machen, etwa diese auf schwerste Fälle von Kriminalität zu beschränken. Die Problematik verdeutlichte Jäger an einer einfachen Zahl: "In 85 Prozent der Fälle sind keine Daten mehr zu erhalten. Das bedeutet, dass 85 Prozent der Straftaten nicht aufgeklärt werden können." Durch fehlende Daten sei vor allem auch die Kinderpornografie in Deutschland, anders als in anderen Ländern, kaum aufklärbar.



Diese Zeiten sind lange vorbei: Das Internet ist das Schlachtfeld des 21. Jahrhunderts. Foto: EP/Janina Scholz/Pixelio.de

Diese Herausforderung, gerade für die Polizei, unterstrich auch Erich Rettinghaus, NRW-Landesvorsitzender der Deutschen Polizeigewerkschaft (DPolG). "Das nächste 9/11 könnte uns per E-Mail erreichen. Die Cyber-Abwehr braucht nicht nur Mauern, sondern auf diesen Mauern auch Kanonen zum Schießen. Eine präventive Abwehr reicht nicht aus. Wir müssen auch proaktiv handeln können", sagte Rettinghaus in Bonn.

Mit dem Cyber-Abwehrzentrum (CAZ) habe der Staat eine effiziente Koordinierung an zentraler Stelle geschaffen, wie Horst Flätgen, Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), erklärte. Bildlich gesprochen spiele man in der Bekämpfung der Cyber-Kriminalität in der "Champions-League". Dennoch gebe es Verbesserungspotenziale des CAZ. "Wir brauchen eine stärkere Einbindung der Polizeibehörden in die Cyber-Abwehr", so Flätgen. Gleichzeitig betonte er, in Bezug auf die Aussagen des DPolG-Landesvorsitzenden, aber auch die eigentliche Problematik der Cyber-Abwehr. "Kanonen sind schön und gut. Aber auf wen sollen wir denn schießen? Das Entdeckungsrisiko der Cyber-Kriminellen im Internet ist gleich null", so Flätgen.

Cyber-Abwehr

Bedrohungen und moderne Lösungen

(EP/Ramon Mörl, itWatch GmbH) Öffentliche Auftraggeber besitzen Daten bester Qualität und sind somit besonders intensiv den Angriffen der Daten-Piraten ausgesetzt. Leider kann auch der loyale Mitarbeiter Opfer dieser versteckten Angriffe werden, ohne dass jemand etwas bemerkt. Organisatorische Maßnahmen greifen hier nicht – die Haftung z. B. nach BDSG bleibt aber trotzdem bestehen und ist z. B. bei Outsourcing nicht delegierbar. Angriffe wie Stuxnet, Duqu, Flame und Roter Oktober zeigen die Brisanz dieser Themen. Die Kombination verschiedenster Angriffstechniken erhöht hier die Gefahr. Nur ein variantenreiches Abwehrsystem, welches die Abwehrmethoden aus Geräte-Kontrolle (Device Control), Anwendungskontrolle (Application Control), Inhaltskontrolle (Content Control), Protokollierung, Verschlüsselung, sicherheitsbewusstseinsbildender Maßnahmen (Security Awareness) und Virtualisierung geschickt kombiniert, bietet den geeigneten Schutz und gleichzeitig die einfache Nutzbarkeit der IT-Systeme.

Neue Inhalte oder sogar neue Anwendungen können für den Arbeitsablauf wesentliche Inhalte enthalten. Damit ein Anwender seine Aufgaben direkt von seinem Arbeitsplatz ausführen und schnell reagieren kann, muss er die kritischen Aktionen sofort durchführen, kann aber deren Kritikalität nicht einschätzen. Die neuen Inhalte könnten natürlich auch Schadcode enthalten. Zuerst gilt es, alle bekannten Anwendungen in Echtzeit von den unbekannten zu unterscheiden. Executables in dem Format *.exe sind dabei nur die Spitze des Eisberges – Makros in Excel-Dateien, JavaSkript in PDF-Dateien oder einfach in Word-Dokumente eingebettete, ausführbare Programme können genauso gefährlich sein.

Ein Remote Controlled Application System löst dieses Problem einfach und effizient durch das automatische Erkennen von ausführbaren oder aktiven Elementen – auch als eingebettete Objekte z.B. in Word-Dokumenten oder in verschlüsselten Zip-Archiven und das Überführen der ausführbaren Elemente mit dem Kontext (z. B. ganze CD zur Installation) in die dafür geeignete virtualisierte Umgebung in Echtzeit ohne Benutzerinteraktion.

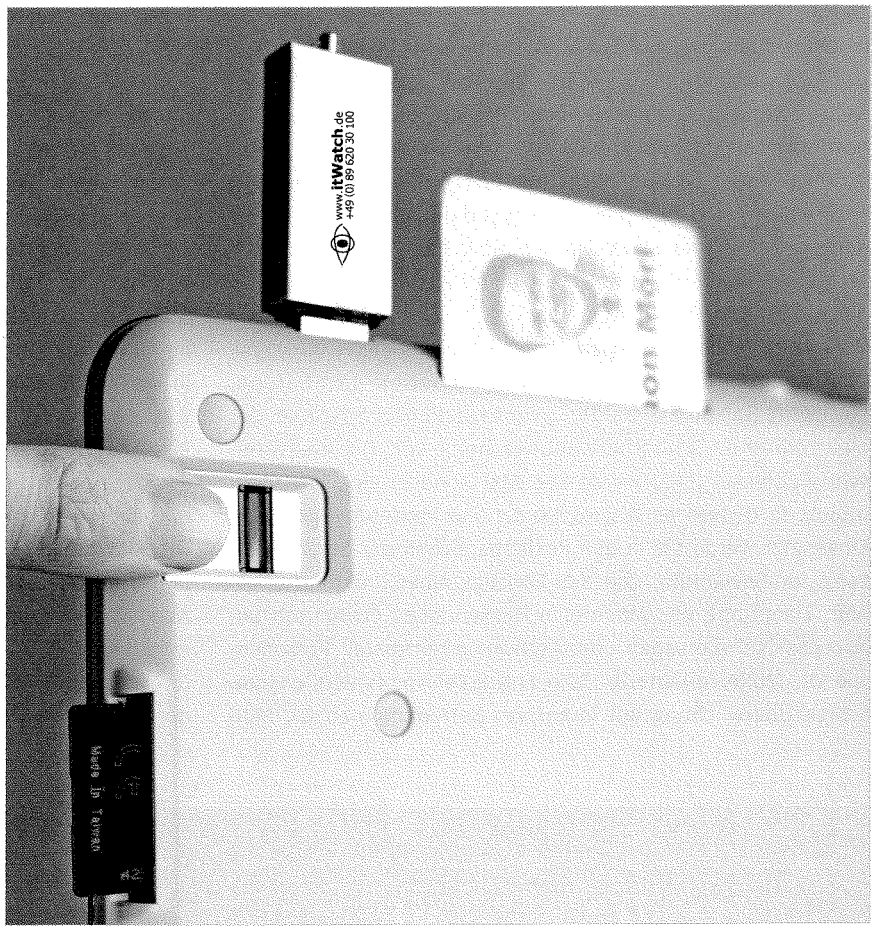


Foto: EP/itWatch

Nach diesen Vorsichtsmaßnahmen ist das innere Netz bei dem Import von Inhalten gut abgesichert. Die exportierten Daten beim Transport sind durch eine Verschlüsselungslösung kontextabhängig zu schützen, welche Firmenschlüssel und selbst definierte Schlüssel unterstützt. Firmenschlüssel reduzieren das Data Loss Risiko auf null Prozent – persönliche Schlüssel erlauben den sicheren und kontrollierten Datentransport zu Dritten.

Die itWatch Security Suite setzt diese Funktionen einfach um und erlaubt auch die Produktion von sicheren Tablet-Lösungen, die bis VS-NfD zugelassen sind. Natürlich sind alle Funktionen auch schon für Windows 8 verfügbar.

Bundeswehr, Nachrichtendienste, Polizei, und kommunale Einrichtungen vertrauen seit Jahren auf die Produkte der itWatch. Neben VS-NfD-klassifizierten Installationen gibt es mehrere tausend Lizenzen in GEHEIM klassifizierten Umgebungen. Bei der Ausschreibung des Bundes, welche inhaltlich durch das BSI begleitet wurde, hat die itWatch Enterprise Security Suite den Zuschlag erhalten – viele weitere Rahmenverträge und günstige Bezugsquellen bestehen für öffentliche Auftraggeber. Eine jahrelange Zusammenarbeit von itWatch und BWI mündet nun in der flächigen Ausstattung des Zielbetriebes Hercukules mit der itWatch Security Suite in der Premium Edition auf 140.000 Clients.

Alles ist besser als Haft

Möglichkeiten elektronischer Aufenthaltsüberwachung

(EP/Patricia B. Linnertz) Sowohl über die Sicherheitsverwahrung als auch die so bezeichnete elektronische Fußfessel wird seit geraumer Zeit diskutiert. Der Einsatz elektronischer Aufenthaltsüberwachung ist in Deutschland derzeit noch nicht politisch geregelt.

"Dabei gibt es große Einsatzbereiche für die Aufenthaltsüberwachung. Diese sollten auch genutzt werden", betonte Siegfried Kauder, MdB, Vorsitzender des Rechtsausschusses des Deutschen Bundestages, auf dem Parlamentarischen Abend des Behörden Spiegel. Denn: "Jede Alternative ist besser als Haft. Die elektronische Fußfessel ist besser als gar nichts", so Kauder weiter.

In Deutschland sei die Fußfessel nur eingeschränkt nutzbar. Das Einsatzspektrum des Systems könne jedoch durchaus erweitert werden, als Beispiel um auffällige Personen über die Aufenthaltsfeststellung von Fußball-Spielen fernzuhalten. "Die Fußfessel ist aber nicht nur besser als Haft, sie spart auch Kosten und Ressourcen", sagte Kauder weiter und forderte anschließend dazu auf, es nicht bei Modellen zu lassen, sondern die elektronische Aufenthaltsüberwachung und deren Möglichkeiten nun zu nutzen.

Dr. Jochen Müller, stellvertretender Abteilungsleiter im Hessischen Ministerium der Justiz, für Integration und Europa, stellte in Berlin die beiden grundsätzlichen Systeme der elektronischen Aufenthaltsüberwachung vor. Die elektronische Fußfessel (EFF) werde seit Mai 2000 in einem Modellprojekt in Hessen an bislang über 1.000 Probanden getestet. Eingesetzt werde sie in den Rechtsbereichen der Strafaussetzung zur Bewährung und des Vollzugs einer Untersuchungshaft. Zielgruppe des Modells in Hessen seien "chronisch unzuverlässige" Personen oder "schwer erreichbare" Personen, wie Dr. Müller erläuterte. "Die Fußfessel kombiniert engmaschige Überwachung mit intensiver Betreuung", so Dr. Müller. Und sie spare Kosten: "Pro Person und Tag liegt die Fußfessel bei einem Betrag von etwa 30 Euro. Ein Tag Haft kostet pro Person rund 100 Euro." Die Erfolgsquote des hessischen Modellprojektes liege bei 90 Prozent. Die Fußfessel habe sich als Hilfe sowohl für die Betroffenen als auch für die Justiz erwiesen.

Das zweite System, die elektronische Aufenthaltsüberwachung (EAU), erfasse Daten der zu überwachenden Person über das GPS-Signal. Diese Form der permanenten Echtzeitüberwachung dürfe nicht anlassunabhängig durchgeführt werden. Die zukünftigen Einsatzmöglichleiten dieses Systems seien laut Dr. Müller enorm. Das System könnte etwa gegen häusliche Gewalt oder Hooligans eingesetzt werden. Dr. Müller stellte aber auch die Frage in den Raum, ob der elektronisch überwachte Hausarrest nicht auch eine neue Form des Strafvollzugs werden könnte oder auch der Entlassungsvorbereitung dienen könnte.

In jedem Fall seien beide Methoden der elektronischen Überwachung nur als komplementäre Weisung und als Einbettung in andere Maßnahmen zu nutzen. "Der Einsatz dieser Systeme ist ein schwieriges Thema. Aber es lohnt sich, darüber nachzudenken", so Dr. Müller abschließend.

Ursula Werner, Hessische Zentrale für Datenverarbeitung, erläuterte den rund 100 Teilnehmern des Parlamentarischen Abends ihre Erfahrungen aus der Praxis der Aufenthaltsüberwachung. Die EAU werde in Hessen seit fast zwei Jahren mit rund 27 Probanden getestet. Der Vorteil liege vor allem in der technisch sehr individuell einzustellen Kontrolle von Verbots- oder Gebotszonen. So könne als Beispiel festgelegt werden, ob eine Person sich etwa einem Kindergarten nicht im Umkreis von 500 Metern nähern darf oder ob eine Person den heimatlichen Landkreis nicht verlassen dürfe. Zudem sei über das GSP-Signal ein Trailing des Aufenthaltes möglich. Somit lasse sich genau nachvollziehen, welche Wege die Person, auch in welcher Geschwindigkeit, zurückgelegt hat oder ob sie sich etwa stetig nur wenige Meter um die festgelegte "Verbotszone" herum aufhält.

Service an erster Stelle

Innovative Konzepte an die Bedürfnisse angepasst

(EP) Die mh SERVICE GmbH bietet als einziger europäischer Hersteller von IT-forensischer Hardware ein Gesamtkonzept über Hardware, Software und Dienstleistungen an. Seit 1993 werden immer neue, innovative Lösungen entwickelt, die genau an Ihre Bedürfnisse angepasst sind. Eine riesige Auswahl von Software aller weltweit führenden Hersteller, exzellenter Support und Servicepartner als Dienstleister rundet unser Angebot ab.

Service steht bei uns an erster Stelle. Wir bieten standardmäßig erweiterte Garantie auf unsere Geräte, Support für Hard- und Software sowie schnelle Lösungen mit mobilen Service-Teams, um jederzeit, wenn nötig auch vor Ort, an Ihrer Seite zu stehen.

Mobile Lösungen:

TreCorder – mobiles forensisches Labor

Der TreCorder ist das weltweit leistungsstärkste Gerät für die mobile EDV-Beweissicherung in der Computerforensik und ermöglicht die Erstellung von drei forensischen Images simultan.

Forensic Cube – Forensic Barebone

Kompakter Barebone PC – leistungsstark wie eine Workstation. Eine Intel i7 CPU der neusten Generation, bis zu 64 GB RAM und zwei integrierte Schreibschutzblocker von Tableau lassen keine Wünsche offen! Ein Wechselrahmen für 4x-Hot-Swap-fähige Festplatten bietet zudem genügend Speicherkapazität für die gesicherten Beweise. Touchscreen!

BeeCube

Preiswertes mobiles Beweissicherungssystem mit Touchscreen. Ideal zur Erstellung schreibgeschützter Images direkt vor Ort. Der im Lieferumfang enthaltene Hartschalenkoffer ermöglicht den einfachen Transport mit sämtlichem Zubehör. Das komplette System wiegt dabei nur knapp zehn kg.

Laborgeräte:

AntAnalyzer

Der momentan leistungsstärkste AntAnalyzer hat enorme 32 CPU-Cores (Hyper-Threading) und kann mit bis zu 512 GB-RAM ausgestattet werden. Erhältlich sind fünf verschiedene Editionen oder genau die, welche optimal auf Sie zugeschnitten ist. AntAnalyzer S-Type: Weltweit erste Forensic Workstation mit integrierten, verschlüsselbaren Ziellaufwerken, diese werden per Hardware-Key auf AES 256 Bit verschlüsselt.

OktaGraph – High-End Password Recovery

Diese Server-Lösung mit acht NVIDIA Tesla Grafikkarten setzt neue Maßstäbe bei der Passwort-Wiederherstellung. Das System ist getestet und zertifiziert für den Einsatz mit Passware Kit Forensic oder ElcomSoft Password Recovery. Mit maximal 4.096 CudaCores werden bis zu 10.648 Gigaflops erreicht

GeCo – General Electronic Copy

High-End-Beweissicherung für enorme Datenmengen. Forensisches Imagen auf höchstem Niveau! Das Sichern von bis zu acht Festplatten gleichzeitig gepaart mit höchsten Transferraten machen den GeCo einzigartig.
Die Gesamtgeschwindigkeit beträgt ca. 43 GB/min = 2.6 TB/h

Forensic Server

Unser Forensic Server wird genau nach Ihren Wünschen gefertigt. Sowohl Storage-Lösungen mit enormer Speicherkapazität als auch High-End-Serverlösungen für forensische Labore sind konfigurierbar. Jede realisierbare und technisch mögliche Ausstattung ist bei uns erhältlich!

PALADIN – Komplettes IT-Forensik-Labor auf Räsern:

PALADIN ist ein unabhängiges, vollständig eingerichtetes Labor für IT-forensische Untersuchungen auf Lkw-Basis. Bis zu acht voll ausgestattete forensische Arbeitsplätze, Konferenzbereich mit großem LED-Display, Server Rack zur Indizierung, Analyse, Passwort-Wiederherstellung, Storage und vieles mehr. Der Paladin kann auch kostengünstig gemietet werden.

Für alle unsere Geräte bieten wir mindestens 36 Monate Garantie auf alle Komponenten.

Software:

Im Angebot stehen alle großen Hersteller von IT-forensischer Software wie AccessData, FireEye, Guidance Software, Katana Forensics, Magnet Forensics, NUIX, Paraben, Passware, Vidientifier, Vound und viele mehr.

→ Bitte besuchen Sie uns an unserem Stand B08. Der PALADIN steht vor dem Gebäude zur Besichtigung bereit. Das mh SERVICE Team wünscht Ihnen einen informativen und erfolgreichen Kongress.

Kontakt

mh SERVICE GmbH
An der Rainmühle 9
D-76185 Karlsruhe
Tel.: +49 (0) 721 831 7330
Fax: +49 (0) 721 831 7349
info@mh-service.de
www.mh-service.de

Kompetenzen bündeln

LKA NRW konzentriert die Cybercrime-Kräfte

(EP/rup) Die rasant zunehmende Zahl krimineller Aktivitäten im Cyberraum hat das Landeskriminalamt Nordrhein-Westfalen (LKA NRW) zum Umdenken veranlasst. Allein im Jahr 2010 wurden über 48.000 Straftaten registriert, die über das Internet begangen wurden. Bei den besonders schweren Fällen ergab sich im Vergleich zu 2009 eine Steigerung von 27 Prozent.

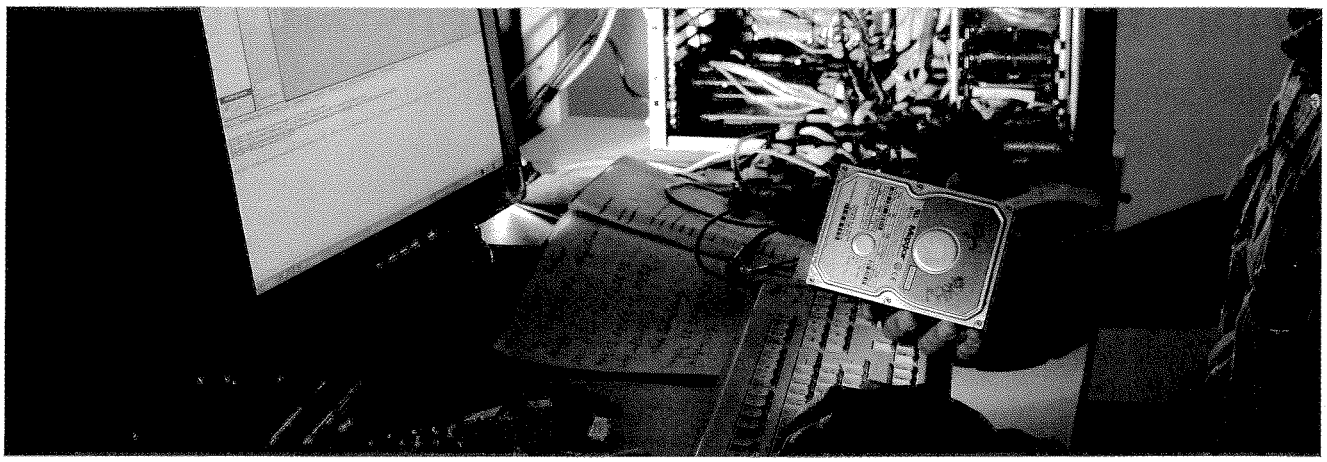
In 2011 wurden daher die vorhandenen Ressourcen im Bereich der Informations- und Kommunikationstechnik gebündelt und ein Kompetenzzentrum Cybercrime im LKA geschaffen. Die Wege sollten kürzer, die Reaktionszeiten schneller und das Personal aufgestockt werden. Die ersten Erfahrungen seien positiv, freut sich der Leiter des Kompetenzzentrums, Markus Röhrl. Doch man müsse mit der dynamischen Entwicklung im Cyber-Raum Schritt halten.

Wenn ein polizeiliches Verfahren zu komplex wird, um es dezentral in den nordrhein-westfälischen Kreispolizeibehörden zu bewältigen, übergibt die Staatsanwaltschaft die Ermittlungen an das LKA NRW. Internationale Phishing-Banden, großangelegte Hacker-Attacken oder Kinderpornografie-Ringe werden dann im rund zwei Jahre alten Neubau in Düsseldorf untersucht. Dort arbeiten die Spezialisten für die Bekämpfung von Computerkriminalität und Kinderpornografie mit Fachleuten für die Internetrecherche, die Telekommunikationsüberwachung, die IuK-Lageunterstützung und die IT-Forensik im neu formierten Kompetenzzentrum Cybercrime in einer Abteilung. Kriminalbeamte und IT-Ingenieure ergänzen ihr Fachwissen so auch räumlich in enger Zusammenarbeit. Neben den Beamten vor Ort, werden je nach Bedarf weitere Spezialisten angefordert. "Hoch spezialisiertes Personal, das nur begrenzt verfügbar ist, soll die komplexen Verfahren lösen", erläutert Röhrl. Allerdings beschränke sich dieses Vorgehen nicht nur auf die Stammbelegschaft des Kompetenzzentrums, sondern fördere den Kompetenzaustausch mit den Polizeibehörden im Land. Neben umfangreichen Fortbildungen von bis zu neun Monaten für das eigene Personal wird der Wissenszuwachs auch durch gegenseitige Hospitationen mit Wirtschaftsunternehmen ergänzt. "Nicht die Menge des Personals ist entscheidend, sondern die handverlesene Qualität", betont Röhrl die Bedeutung der steten und gezielten Weiterbildung.

Die ersten Erfolge der neuen Strategie und der neuen Möglichkeiten konnten die Beamten schon nachweisen: Der Hackergruppierung No-Name-Crew, die sensible Daten des Zolls und der Bundespolizei gestohlen und veröffentlicht hatte, konnte mittels massivem Personaleinsatz in einer großen Kommission binnen weniger Wochen das Handwerk gelegt werden. "Die eigene Flexibilität und die Einbindung von Spezialisten aller Polizeibehörden in NRW waren die Erfolgsfaktoren", schildert Dezernatsleiter Helmut Picko seine Erfahrungen. 25 namentlich ausgewählte Experten hatte man zunächst angefordert, im Verlaufe des Verfahrens wurden rund 200 Kräfte eingesetzt, vom Beamten aus dem Mobilen Einsatzkommando (MEK) bis zum Ingenieur. Die ersten Mitglieder der No-Name-Crew konnten nach fünf Tagen festgenommen werden, von Schülern bis zu IT-Projektmanagern reichte die Bandbreite der Delinquenten. "Das waren keine Scriptkiddies", schildert Picko, "sondern Profis, die auch einige kommerzielle Straftaten über das Internet begangen hatten." Dank der guten und koordinierten Zusammenarbeit unterschiedlicher Experten der Zentrale Internetrecherche (ZIR), der IuK-Ermittlungskommission und der IuK-Forensiker konnte das "sehr komplexe und aufwändige" Verfahren, bei

Info

Der **"Organisierten Kriminalität im Internet"** widmet sich ein Fachforum des 16. Europäischen Polizeikongresses in Kooperation mit dem Bund Deutscher Kriminalbeamter (BDK) am **19. Februar 2013, 11:00 bis 12:30 Uhr.** Hieran nimmt u. a. Dr. Ole Schröder, Parlamentarischer Staatssekretär beim Bundesminister des Innern, teil.



Dank moderner Technik sind die Spezialisten vom LKA NRW schneller und flexibler geworden.

Foto: EP/Ministerium für Inneres und Kommunales NRW

dem die Schwierigkeit darin bestand, den Tätern mit ihren verschlüsselten, virtuellen Identitäten Gesicht und Namen in der realen Welt zu geben, erfolgreich abgeschlossen werden. Auch zur Aufklärung der Operation Payback trug das LKA NRW seinen Teil bei. Der Angriff von Anonymous auf den Zahlungsverkehr von Finanzdienstleistern, die WikiLeaks-Konten gesperrt hatten, wurde auch über Server koordiniert, die in Köln standen. Über eine sogenannte Low-Orbit-Ion-Cannon", einem Tool, das man sich über einen Download beschaffen konnte, wurden die Angriffe gebündelt und gezielt eingesetzt. "Die große Macht der Internetcommunity" zwang die Finanzdienstleister dann in die Knie. "Die Folgen waren wesentlich dramatischer, als es in der Presse dargestellt worden ist", erläutert Picko. Dennoch führte innerhalb weniger Stunden eine gemeinsame Aktion von LKA NRW, Bundeskriminalamt (BKA) und US-Bundespolizei (FBI) zur Festnahme mehrerer Drahtzieher in Frankreich und den USA.
"Auf die Dynamik und Internationalität der Internetcommunity müssen wir entsprechend reagieren können", mahnt Röhrl und verweist auf die neue Infrastruktur, die im Kompetenzzentrum Cybercrime geschaffen wurde. Über Videokonferenzen und Sharepoint-Technologie kommunizieren die Kriminalisten mit Kollegen in ganz Deutschland. Drei physikalisch voneinander getrennte Netze gewährleisten die nötige Sicherheit. "Wir müssen aber dorthin kommen, dass diese Herangehensweise und die Vernetzung aller Experten zur Normalität wird", fordert Picko. Noch gehörten lange Dienstfahrten und das Kopieren von Akten in Papierform allzu oft zum Tagesgeschäft der Ermittler. "Durch unsere Kommunikationsplattform sind wir wesentlich flexibler und schneller geworden", so Röhrl. Auch mit diesen Mitteln konnte zusammen mit dem LKA Baden-Württemberg eine internationale Phishing-Bande dingfest gemacht werden. "Nur mit modernen Arbeitsplätzen, top-ausgebildeten Fachleuten und einer fortschrittlichen Arbeitsorganisation können wir mit der Entwicklung im Cyberspace mithalten – und manches Mal auch einen Schritt voraus sein", prophezeien Röhrl und Picko.

Info

Neue Technologien für die Polizei
Unter der Leitung von Dietrich Läpke, Deutsche Hochschule der Polizei (DHPol), diskutieren u. a. Uwe Lührig, Präsident Zentrale Polizeidirektion Niedersachsen, und Dieter Schürmann, Landeskriminaldirektor im Ministerium für Inneres und Kommunales Nordrhein-Westfalen, am **Mittwoch, 20. Februar 2013, 15:30 Uhr bis 17:00 Uhr** über "Neue Technologien für die Polizei"

Robuste Hardware im rauen Dienstalltag

Mobile-Computing-Lösungen für Polizei und Sicherheitskräfte

(EP) Der Polizeialltag stellt besonders hohe Anforderungen an mobile elektronische Geräte. Sensible Computertechnik erreicht bei rauen Bedingungen unterwegs im Außeneinsatz schnell ihre Grenzen. Widrige Witterungsbedingungen wie Regen, Schnee oder blendendes Sonnenlicht, Stöße und Stürze in hektischen Situationen sowie Vibrationen in den Einsatzfahrzeugen lassen sich allerdings nicht vermeiden und fordern der eingesetzten Hardware einiges ab.

Nicht selten kommt es zu kostspieligen Totalausfällen, die durch unvorhersehbare Zusatzkosten – etwa für Reparaturen – sowie die Nichtverfügbarkeit der Geräte die Arbeitsleistung und Motivation der Einsatz-Teams und der gesamten Administration beeinträchtigen.

Der Elektronikkonzern Panasonic hat sich auf Lösungen für solche schwierigen Einsatzbedingungen spezialisiert. Bekannt für hochwertige Consumer-Electronics-Produkte, bietet Panasonic für Firmenkunden besonders energieeffiziente, widerstandsfähige und zuverlässige Mobile-Computing-Lösungen an. Das Produktspektrum unter den Marken "Toughbook" und "Toughpad" reicht von robusten Outdoor-Notebooks über Business-Laptops bis hin zu Tablet PCs. Bereits im Jahr 1994 brachte Panasonic den ersten robusten Mobil-PC auf den Markt.

Inzwischen hat das Unternehmen einen Marktanteil von rund 65 Prozent auf dem europäischen Markt für robuste, langlebige Notebooks (nach verkauften Einheiten 2011, VDC Research, März 2012) und verfügt über einen großen Erfahrungsschatz, der sich auf zahlreiche Branchen erstreckt. In enger Zusammenarbeit mit Kunden und Partnern werden Lösungen entwickelt, die exakt auf kunden- und branchenspezifische Herausforderungen angepasst sind – von der Wartung von Maschinen und Anlagen über Transport und Logistik bis hin zum Einsatz in medizinischen Einrichtungen sowie bei Sicherheits- und Polizeikräften. Höchsten Ansprüchen an Mobilität, Leistungsfähigkeit und Widerstandsfähigkeit werden die Geräte durch geringes Gewicht, äußerst lange Akkulaufzeiten und besondere Schutzmaßnahmen gerecht. Weder Wasser, Staub, Stürze noch Erschütterungen können den gemäß Ingress Protection (IP65) und Militärstandards (MIL-STD-810G) zertifizierten Modellen der "Full Ruggedized" Schutzklasse etwas anhaben. Selbst bei extremen Temperaturen von -20° bis +60° Celsius bleiben sie zuverlässig im Einsatz und bieten dank eigens entwickelter Displaytechnologien selbst unter direkter Sonneneinstrahlung hervorragende Lesbarkeit.

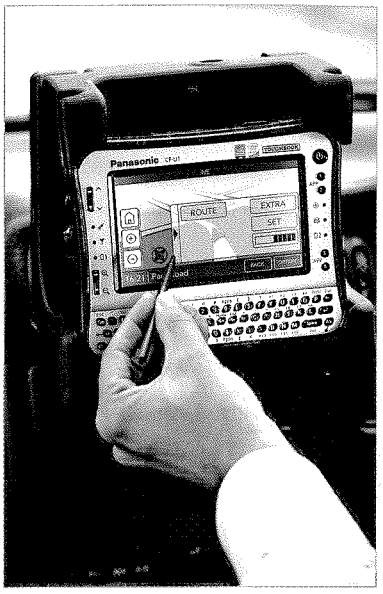
CF-U1 PIMD – ideal für Personenkontrollen unterwegs

Speziell für die Arbeit von Grenzkontrolleuren, Sicherheitskräften und Polizeistreifen hat Panasonic in Zusammenarbeit mit DESKO eine 4-in1-Lösung entwickelt. Der handliche Ultra-Mobile PC (UMPC) CF-U1 umfasst in Kombination mit dem sogenannten "Person Identification Mini Dock" (PIMD) vier Funktionen in einem Gerät: einen Kontakt-Smart-Card-Leser zur Anwender-Authentifizierung, einen OCR- und einen RFID-Leser sowie einen optionalen Fingerabdruck-Scanner.

Pässe und Ausweise können über das PIMD eingelesen und Dokumente mit einer integrierten Kamera gescannt werden.

Dank des vollfunktionalen Betriebssystems können die erfassten Daten auf einer Office-ähnlichen Plattform bearbeitet und per Wireless LAN oder ein optional integrierbares 3G-Breitband-Modul mit einem zentralen Server synchronisiert werden.

Die Daten können sowohl über die Tastatur als auch per Stift- oder Fingereingabe über einen sonnenlicht-tauglichen 5,6 Zoll Touchscreen bearbeitet werden. Die technische Ausstattung bietet ein optimales Verhältnis zwischen Mobilität und Leistung: WSVGA-Auflösung (1024x600), zwei GB RAM, ein 64 GB Solid-State-Laufwerk, ein Doppel-Akku-System sowie ein energieeffizienter 1,6 GHz Intel Atom Prozessor sind im CF-U1 untergebracht.



CF-U1 mit Kfz-Einbaulösung

Foto: EP/Panasonic

Die robuste Gerätekombination lässt sich optimal zur mobilen Personenüberprüfung oder für die Kontrolle von Sicherheitszugängen bei Großveranstaltungen wie Konzerten oder Fußballspielen verwenden.

Derzeit wird das CF-U1 etwa in einem groß angelegten Pilotprojekt zur allgemeinen Besucheridentifizierung bei Fußballspielen in der Schweiz eingesetzt. Robuste Hardware im rauen Dienstalltag.

Besondere Produkteigenschaften

Speziell für Polizei und Sicherheitskräfte:

- verlässliche Wireless-Konnektivität auch in entlegenen Gebieten,
- ausdauernde Akkus sowie Doppel-Akku-Lösungen für lange Nutzungszeiten ohne Stromzufuhr,
- sonnenlicht-taugliche Displays für Einsätze in hellem Umgebungslicht,
- Fahrzeug-Einbaulösungen für die Nutzung während der Fahrt sowie
- Halte-, Trage- und Body-Mounting-Systeme.

Der Spur auf der Spur

Asservaten- und Spurenverwaltung mit Workflow-Management

(EP) Asservate und Spuren sind essenzielle Bestandteile der kriminalpolizeilichen Fallbearbeitung. Aber: je komplexer und umfangreicher der Fall, umso komplizierter und zeitaufwändiger die Verwaltung und Auswertung von Asservaten.

Nicht nur Gegenstände, auch Spuren müssen gesichert, erfasst, einem Vorgang zugeordnet werden, sie müssen verschickt und kriminaltechnisch untersucht werden, Ergebnisse zurückgemeldet und recherchierbar gespeichert werden, schließlich müssen Beweismittel katalogisiert und auffindbar gelagert werden.
Das alles erfordert einen hohen Verwaltungsaufwand. Zugleich sollen alle Schritte zeitnah erfolgen und möglichst ohne komplizierte Bearbeitungsschritte.
Die rola Security Solutions GmbH Oberhausen hat mit rs*Evid* eine IT-Lösung für Asservate und Spuren entwickelt, das als eigenständiges Tool mit Systemen zur polizeilichen Vorgangsbearbeitung oder auch mit IT-Lösungen für kriminalpolizeiliche Fallbearbeitung und Analyse wie rs*CASE* von rola eng zusammenarbeitet.

Die kriminalpolizeiliche Fallbearbeitung, auch von Schusswaffen, erfordert einen hohen Verwaltungsaufwand. Foto: EP/Rola Security

Erfassung

Asservate und Spuren werden nach BKA-Systematik strukturiert erfasst. Klar gegliederte Eingabemasken vereinfachen und beschleunigen die Erfassung erheblich. Jeder Eintrag erhält eine Asservaten-Nummer, die fortlaufend und ebenenbezogen vergeben wird. Eine Aufteilung in Unterasservate ist ebenso möglich wie die Zusammenfassung zu Paketen. Die Visualisierung in Baumstruktur sorgt für schnelle Orientierung. Auch Datenmatrix-Scanner können eingesetzt werden.

Bearbeitung

Das Asservatentool kann aus einem Vorgangsbearbeitungssystem gestartet werden, dabei erfolgt die Übergabe aller relevanten Vorgangsinformationen automatisch. Der gesamte Prozess für die Verwaltung und Bearbeitung von Asservaten und Spuren oder auch Asservatenpaketen wird elektronisch abgewickelt: Erstellung von KTU-Anträgen über eine Schnellerfassungsmaske (inkl. Checklisten für alle notwendigen Informationen), Aufnahme des Untersuchungsergebnisses, Ergebnisfreigabe, Antrag auf Erstellung von Gutachten, Nutzung des FTS-1.09-Schnittstellenstandards und Übergabe der Asservate/Spuren sowie der Vorgangsgrunddaten an ein Laborinformationssystem oder an ein Fallbearbeitungssystem wie rs*CASE*. Kategorien, Situationsspuren und Asservate werden mit sonstigen Ermittlungsspuren und anderen Entitäten verknüpft und können so auch in Charts und anderen Auswertungsfunktionen verwendet werden. Ebenso ist die Anbindung von Geo-Informationssystemen möglich.

Recherche

Zahlreiche äußerst mächtige Recherchefunktionen wie Wildcardsuche, fragmentarische Suche, phonetische Suche, Ähnlichkeitssuche oder Komplexrecherche erleichtern den schnellen Zugriff auf Spuren und Asservate.

Dokumentation und Ausgabe

Die Vita von Spuren und Asservaten wird lückenlos dokumentiert, der Verbleib aufgezeichnet (Asservatenbuchfunktion). Der komplette Bearbeitungsprozess kann grafisch in einem Chart dargestellt werden. Alle für die Untersuchung von Asservaten notwendigen Formblätter und Anträge werden automatisiert erzeugt, auch Datenmatrix-Codes können ausgedruckt werden. Die Generierung von Statistiken erlaubt es, Übersichten zu erhalten und weitere Auswertungen vorzunehmen.
rsEvid bietet ein komplettes Workflow-Management für Asservate und Spuren und stellt einen entscheidenden Baustein im Rahmen der rola Gesamtlösung rs*Frame* dar, speziell in Zusammenarbeit mit der rs*Frame*-Variante rs*CASE*, dem System für kriminalpolizeiliche Fallbearbeitung und Analyse.
Mit den rola IT-Lösungen für Informationsmanagement im Sicherheitsbereich arbeiten über 50.000 Anwender in deutschen und ausländischen Polizei-, Militär- und anderen Sicherheitsbehörden.

⇢ *Weitere Informationen unter www.rola.com.*

"Allein" völlig abwegig

Optimale Möglichkeiten im Internet

(EP) "Das Internet bildet die optimale Tarnung für Cyber-Kriminelle", bekräftigte Dr. Harald Niggemann, BSI, im Rahmen des 5. Symposiums des Niedersächsischen Verfassungsschutzes, das 2012 in Hannover unter dem Titel "Spionage, Cyber-Angriffe, Know-how-Verluste – Was tun gegen Bedrohungen von Wirtschaft, Wissenschaft und Staat?" stattfand. Es biete aber darüber hinaus auch optimale Möglichkeiten: "Alles in Verbindung mit dem Internet ist attackierbar, und vor allem sind die Angriffsmittel permanent beschaffbar und verfügbar."

Als besonders gefährlich bezeichnete Niggemann auch die professionelle Arbeitsteilung innerhalb der Underground Economy. "Der Umfang und die Komplexität moderner Software verhindert die Fehlerfreiheit. Über die entsprechenden Schwachstellen tauscht man sich in den Schattenforen der Underground Economy rege aus", erläuterte Niggemann. Diese Sicherheitslücken führten zu einem kritischen Zeitfenster der Schutzlosigkeit, da die Installation entsprechender Patches oft Wochen oder sogar Monate dauern könnte. In dieser Zeit sei man dann nahezu schutzlos den möglichen Cyber-Angriffen ausgeliefert. Als besondere Herausforderung für die Cyber-Sicherheit bezeichnete Niggemann weiterhin die mehrstufigen Angriffe auf die Sicherheitsinfrastrukturen des Internets, die oftmals Folgeangriffe nach sich zögen. Beispielhaft sei etwa der Diebstahl von Sicherheitszertifikaten.

Die Polizeiliche Kriminalstatistik (PKS) des Jahres 2010 verzeichnete 59.839 Fälle von Cybercrime im engeren Sinne, wie Fred-Mario Silberbach, Bundeskriminalamt (BKA), in Hannover erläuterte. Obwohl die Statistiken für das vergangene Jahr 2011 noch nicht vorlägen, gehe der Trend dieser Zahlen nach oben ungebrochen weiter. "Opfer von Cybercrime zu werden ist heutzutage kein Problem mehr", so Silberbach, und verdeutlichte dies am Beispiel der sogenannten "Man-in-the-Middle"-Attacken. Dabei würden, etwa beim Vorgang des Onlinebankings, Daten in Echtzeit während der Transaktion gestohlen. Besorgniserregend sei auch die Zunahme von Angriffen mit Scareware. "Auf Ihrem Computer wird plötzlich die Infizierung durch ein Schadprogramm angezeigt. Die ist natürlich falsch, aber das wissen Sie ja noch nicht. Gleichzeitig wird Ihnen eine Anti-Viren-Software, mit der Sie das Schadprogramm auf jeden Fall loswerden und sich auch permanent dagegen schützen können, zum Kauf angeboten. Kaufen Sie dann diese besagte Software, erhält der Täter Ihre Kreditkartendaten, schickt Ihnen mit der neu erworbenen Software einen richtigen Trojaner und nimmt Ihren Computer gleichzeitig noch in ein Botnetz auf. Das nennt man dann einen ganzheitlichen Ansatz der Täter", erklärt Silberbach.

Daneben seien aktuell auch digitale Erpressung und der Handel mit Daten aus den Sozialen Netzwerken deutlich zunehmend: "Die Daten von Sozialen Netzwerken sind für Cyber-Kriminelle hoch lukrativ. Man erreicht einen großen Verteilerkreis, aber vor allem auch einen hohen Wirkungsgrad. Weil, E-Mails mit Anhängen seiner "Freunde" vertraut man ja schließlich eher als solchen von fremden Personen."

Als Maßnahme gegen die Internetkriminalität könne neben einer verbesserten Aus- und Fortbildung sowie der verstärkten Sensibilisierung auch eine institutionalisierte Öffentlich Private Partnerschaft (ÖPP) wirksam sein. Hierbei sollten Mitarbeiter öffentlicher Einrichtungen unter einem Dach gemeinsam mit Unternehmen gegen Cyber-Kriminalität vorgehen können.

"Wir sind nicht auf alles vorbereitet. Wir haben auch noch nicht alle Probleme gelöst. Wir brauchen ein Umsteuern unserer Denk- und Arbeitsweise. Die Sicherheitsbehörden müssen im Internet Streife surfen und permanent präsent sein", bekräftigte auch Uwe Schünemann, niedersächsischer Minister für Inneres und Sport, und hob dabei auch den erforderlichen breiten Austausch mit der Wirtschaft in den Vordergrund: "Allein gegen Cybercrime ist völlig abwegig", so der Minister.