Bundeskriminalamt

COD-Literatur-Reihe

Band 25

Cybercrime - Bedrohung, Intervention, Abwehr

Eine Literaturauswahl

HERBST-TAGUNG BKA 2013 AUTUMN CONFERENCE

COD - LITERATUR - REIHE
BAND 25

Cybercrime - Bedrohung, Intervention, Abwehr

Eine Literaturauswahl anlässlich der Herbsttagung 2013

Inhalt

Begleitwort

Band 25 der COD-Literatur-Reihe führt mit einer Literaturauswahl zur Herbsttagung 2013 die Reihe der Literaturdokumentation des Bundeskriminalamtes fort. Die ausgewählten Beiträge wurden im Datenbestand des **Co**mputergestützten **D**okumentationssystems für Literatur (COD-Literatur) recherchiert, für das derzeit mehr als 150 Fachzeitschriften und Buchreihen inhaltlich erschlossen werden.

Die Auswahl der Literatur zum Thema der diesjährigen Tagung „Cybercrime - Bedrohung, Intervention, Abwehr“ orientierte sich an den Vorträgen der Tagung. Viele der Beiträge weisen eigene Literaturquellen nach, die dem Leser zusätzlich die Möglichkeit eröffnen, die Themen der Tagung weiter zu vertiefen.

Der Band beinhaltet aus der Fülle der Veröffentlichungen eine Auswahl aus den Jahren 2010 bis 2013. Er beginnt mit den zeitlich aktuellsten Literaturquellen.

Alle Einzelbeiträge liegen auch in digitalisierter Form vor und können von Polizeibediensteten unter der u.a. E-Mail-Adresse bei der Literaturdokumentationsstelle angefordert werden.

Franziska Wallraff-Unzicker — Wiesbaden, November 2013

Bundeskriminalamt
KI 35-Literaturdokumentation
Tel: 0611-55-14050
Fax: 0611-55-45070

e-Mail: ki35Literaturdokumentation@bka.bund.de
http://www.cod.extrapol.de

ID-nummer: 20131173

Burandt, Klaus; Tölle, Ralph

Cybercrime - nicht nur in der Großstadt! Erfahrungen am Beispiel einer Ermittlungskommission

Kriminalistik, 2013, 8-9, S. 523-525
mit 1 QU

Im Frühjahr 2012 kam es im Kreis Steinfurt in Nordrhein-Westfalen zu einer Häufung von Kontoeröffnungsbetrugsdelikten, bei denen bis dahin unbekannte Täter bei unterschiedlichen Direktbanken im gesamten Bundesgebiet unter Nutzung diverser Aliaspersonalien Girokonten eingerichtet hatten. Auf Grund einer dezentralen Bearbeitung dieser Delikte in verschiedenen regionalen Kriminalkommissariaten waren Tatzusammenhänge zu Beginn der Ermittlungen nicht erkennbar und konnten dann erst mittels einer zentralen Ermittlungsführung hergestellt werden. Die Komplexität der unterschiedlichen Handlungen führte schließlich zur Einrichtung der Ermittlungskommission "Rock".
In dem Beitrag stellen die Autoren die kriminalistischen Aspekte dieses Ermittlungsverfahrens dar und geben Anregungen für die zukünftige Bearbeitung ähnlicher Straftatenkomplexe.
Sie plädieren beispielsweise für einen Aufbau eigener Cybercrime-Dienststellen mit sachkundigem Personal oder Arbeitsteams auch in ländlichen Regionen, wie aktuell im Land Nordrhein-Westfalen per Erlass vorgesehen. Darüber hinaus ist ein frühzeitiger und intensiver bundesweiter Informationsaustausch auf polizeilicher Ebene, der über den normalen Meldedienst hinausgehen muss notwendig sowie das Vorantreiben einer noch immer fehlenden Rechtsgrundlage zur Vorratsdatenspeicherung.

Computerbetrug; Internetkriminalität; Internetforum; Kreditinstitut; Bankkonto; Warenbetrug; Schattenwirtschaft; Ermittlungskommission; Ermittlungsansatz; Spurenauswertung; Täterstruktur; Täterstrategie

ID-nummer: 20131089

Riedel, Rene; Urban, Tobias; Pohlmann, Norbert; Robles, Antonio González

Anforderungen an IT-Systeme in kritischen Infrastrukturen; Gefahrenpotenzial intelligenter Stromnetze aus Sicht der IT-Sicherheit

IT-Sicherheit - Management und Praxis, 2013, 4, S. 50-53
mit 1 BILD, 2 TAF, 6 QU

Das Energienetz der Zukunft läuft zusammen mit IT-Komponenten, die eine intelligente Steuerung erlauben. Dadurch entstehen neue Angriffsflächen, die nun erstmals nicht auf ein bestimmtes IT-System wirken, sondern auf eine komplette Bevölkerung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat daher ein Schutzprofil für ein Smart-Metering-Gateway entwickelt, welches diese Problematik in intelligenten Stromnetzen adressieren soll.

Kritische Infrastruktur; Stromausfall; Energienetz; IT-Sicherheit; Angriffsziel; Elektrizität; Gefahrenanalyse

ID-nummer: 20130993

Mischkowitz, Robert

Fragen an die Kriminologie ... aus der Sicht der Polizei

MschrKrim - Monatsschrift für Kriminologie und Strafrechtsreform, 2013, 2-3, S. 212-221
Zur Lage der Kriminologie in Deutschland, Freiburg i.Br.; BR Deutschland, 2012 [28.06.-30.06.] mit 18 QU

Die Fragen an die Kriminologie aus Sicht der Polizei werden vor dem Hintergrund einer historischen Betrachtung aufgegriffen. Ausgehend von Fragestellungen, die der ehemalige Präsident des Bundeskriminalamtes, Horst Herold, in einem im Jahre 1973 stattfindenden Kriminologentreffen aufgeworfen hatte, werden wesentliche Aspekte der Zusammenarbeit von Polizei und Kriminologen während der letzten Jahrzehnte, wie der Praxisbezug und die Anwenderorientierung, verschiedene Kooperationsformen der Zusammenarbeit und die Umsetzungsproblematik kriminologischer Erkenntnisse in polizeiliches Handeln thematisiert. Daran schließt eine Betrachtung der gegenwärtig im Blickpunkt stehenden und auch zukünftig dringlicher werdenden kriminologischen Themen- und Forschungsfelder an. Zu nennen sind hier neben dem Terrorismus und Extremismus besonders die Entwicklungen im Bereich Cyberkriminalität, aber auch Bemühungen in den deliktsformübergreifenden Bereichen Dunkelfeldforschung und Prävention.

Kriminologische Forschung; Kriminalistisch-kriminologische Forschung; Kriminalistisch-kriminologische Forschungsgruppe; Bundeskriminalamt; Forschungsaufgabe; Forschungsprojekt; Polizeiforschung; Polizeiliche Praxis; Praxisbezug; Angewandte Forschung; Dunkelfeldforschung; Cybercrime

ID-nummer: 20130937

Kirchhoff, Martin

IuK-Kriminalität (Cyberkriminalität); Grundkompetenzen im Bachelorstudium der Polizei

Kriminalistik, 2013, 7, S. 491-495
mit 13 QU

Die IuK-Kriminalität im engeren Sinne umfasst Straftaten bei denen Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind. IuK-Kriminalität im weiteren Sinne bezeichnet alle Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung eingesetzt wird. Diese erstrecken sich mittlerweile auf nahezu alle Deliktsbereiche. Eine deutlich negative Entwicklung, die aufgrund der Sachlage zwingend gegensteuernde Maßnahmen postuliert. Die Polizei muss handeln; ohne Spezialisierung ist das nicht möglich. Kriminalistisches Fachwissen muss daher möglichst bei allen Polizeibeamten vorhanden sein.
Denn Täter hinterlassen auch Spuren auf digitalen Systemen. Es ist für Polizeibeamte von essentieller Bedeutung, folgenden Fragen mit fachlicher Kompetenz zu begegnen:
- Welche digitalen Spuren gibt es?
- Wo kann ich die digitalen Spuren finden?
- Wie kann ich diese Spuren sichern?
In dem Aufsatz werden Grundkenntnisse der Computerkriminalität dargestellt. Der Autor definiert und erklärt die digitale Spur und beschreibt insbesondere die forensischen Maßnahmen beim 1. Angriff.

Kriminalitätsphänomen; Cybercrime; Cyberspace; Computerkriminalität; Phishing; Skimming; Schadsoftware; Soziales Netzwerk; Mobbing; Ermittlungsführung; Erster Angriff; Sicherungsangriff; Auswertungsangriff; Spurenträger; Spurensicherung; Spurenauswertung

ID-nummer: 20130613

Ritter-Dausend, Dirk

Die Kunst des Hackens; Social Engineering und Wirtschaftsspionage

IT-Sicherheit - Management und Praxis, 2013, 2, S. 40-42
mit 1 BILD, 3 QU

Social Engineering bedeutet vereinfacht übersetzt "soziale Manipulation. Im Kontext der Unternehmenssicherheit wird der Begriff für die soziale Manipulation des Menschen verwendet. Ziel ist die Herrschaft über die Sicherheitsarchitektur eines Unternehmens, um sensible Kundendaten beziehungsweise das Know-how des Unternehmens auszuspähen. Eine Hauptrolle spielen dabei Internet-basierte Angriffe, die hohen Nutzen bei kalkulierbaren Risiken versprechen. Dabei ist zu berücksichtigen, dass nicht mehr lediglich Hochtechnologieunternehmen besonders gefährdet sind, sondern eine branchen- und größenübergreifende Gefährdung durch Studien nachgewiesen werden konnte.
Der Verfasser schildert diverse Angriffsvarianten und unterstreicht, dass der Datenschutz eines Unternehmens heute nur in einem ganzheitlichen Sicherheitskonzept (Corporate Security) bestehen kann. Dieses sollte sich aus organisatorischen, technischen und Awareness-Maßnahmen zusammensetzen. Das personell und materiell erstellte Sicherheitskonzept sollte in der Corporate Identity verankert werden. Denn Sicherheit im Unternehmen ist mehr als reine IT-Sicherheit und muss in der heutigen Zeit durch organisatorische Maßnahmen und entsprechende Awareness-Konzepte ergänzt werden.

Wirtschaftsspionage; Konkurrenzspionage; Hacking; Computerkriminalität; Wirtschaftsunternehmen; Schadsoftware; Computervirus; Spam-E-mail; Soziales Netzwerk; Unternehmenssicherheit; Sicherheitsmangel; Sicherheitsrisiko; BSI; Schutzkonzept

ID-nummer: 20130873

Seidl, Alexander

Online-Abzocke und Datenklau - Die digitale Alltagskriminalität

Deutsche Polizei, 2013, 7, S. 4-9
mit 4 BILD

Das Gabler Wirtschaftslexikon definiert den Begriff folgendermaßen: "Cybercrime (lat. crimen: "Beschuldigung, Anklage, Schuld, Verbrechen"; engl. cyber: auf das Internet bezogen) bezeichnet Vergehen beziehungsweise Verbrechen in Zusammenhang mit dem Internet, synonym für Internetkriminalität." Nach der etwas weiteren Ansicht des Bundeskriminalamtes (BKA) hingegen umfasst Cybercrime alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden. Allgemein gesprochen meint Cybercrime alle Aktivitäten, bei denen ein Computer oder Netzwerk entweder Werkzeug, Ziel oder Handlungsort einer Straftat ist. Cybercrime stellt eine Querschnittsmaterie dar und kann in einer Vielzahl von Bereichen und Varianten in Erscheinung treten. Sie umfasst sowohl althergebrachte Delikte, die nunmehr mittels des Internets begangen werden wie den Warenbetrug bei eBay als auch ganz neue Phänomene wie das Verbreiten von Schadsoftware, Phishing, DDoS-Attacken (Distributed Denial of Service) und Account Takeovers (Identitätsdiebstahl). Der Autor bewertet die statistische Aussagekraft und beschreibt einzelne Deliktfelder.

Cybercrime; Definition; Deliktart; Kriminalitätsverlagerung; Statistische Angaben

ID-nummer: 20130615

Cybercrime - das Internet als Werkzeug für kriminelle Machenschaften; Interview André Dornbusch - Stefan Mutschler

IT-Sicherheit - Management und Praxis, 2013, 2, S. 48-50
mit 3 BILD

Die Gefahren, die eine Nutzung des Internets mit sich bringt, werden täglich größer. Verbrecherringe haben sich globalisiert und perfekt organisiert, um sowohl Unternehmen wie Privatpersonen zu bestehlen oder zu betrügen.
Laut Polizeilicher Kriminalstatistik wurden im Jahr 2007 rund 34.000 Fälle von Cybercrime erfasst, 2011 waren es fast 60.000. Der polizeilich registrierte, durch Cybercrime verursachte Schaden hat sich in diesem Zeitraum auf über 71 Millionen Euro mehr als verdoppelt. Rund 5O Millionen Euro entfielen dabei allein auf den Computerbetrug.
Andre Dornbusch erläutert im Gespräch mit IT-SICHERHEIT die aktuellen Cybercrime-Trends und verrät, wie sich das Bundeskriminalamt für die Bekämpfung von Angriffen mit und über das Internet einsetzt.

Cybercrime; Internetkriminalität; Kriminalitätsphänomen; Computersabotage; Computermanipulation; Computerbetrug; Schadenshöhe; Dunkelfeld; Täterstrategie; Modus operandi; Polizeiliche Kriminalstatistik

ID-nummer: 20130784

Henrichs, Axel

Polizeiliche Befugnisse zu Ermittlungsmaßnahmen mit TK- und Internetbezug; Neuregelung zur Bestandsdatenauskunft ab 1. Juli 2013

Kriminalistik, 2013, 6, S. 388-392
mit 27 QU

Mit der zunehmenden Verbreitung und Nutzung des Internets veränderten sich in den letzten Jahren auch die polizeilichen Herausforderungen. So sind z. B. Betrug, Daten- und Identitätsdiebstahl sowie Verbreitung von kinderpornografischem Material mit wenigen Mausklicks möglich. Die Täter agieren im Verborgenen und schützen sich mit falschen Angaben, Nicknames und Fakeaccounts oder speichern polizeirelevante Daten passwortgeschützt im Netz. Die neuen Modelle der Mobiltelefone (Smartphones, Tablet-PCs) ermöglichen eine mobile Nutzung der klassischen TK und auch des Internets. Diese Geräte sind Universalgeräte und vereinen in sich die Funktionen von u.a. Telefon, Kamera, PC, Mailingsystem, Notizbuch, Applikationsboard, Fernsehgerät, Radio, Kalender, Navigationsgerät oder Ortungsmittel. Auch der Begriff der TK hat sich in den Gesetzen mit Polizeirelevanz verändert, technische Maßnahmen gewinnen mehr und mehr an Aktualität. Die Bandbreite polizeilicher Maßnahmen mit Bezug zu diesen Geräten reicht von einfachen Maßnahmen zur Identifizierung bzw. Lokalisierung von Tatverdächtigen oder Störern bis hin zu hochkomplexen Ermittlungen zur Aufklärung von informationstechnischen Systemen. In diesem Beitrag sind primär von Interesse die TK-Bestandsdatenauskünfte. Mit der Neuregelung ist ein wichtiger Schritt getan worden, um die Ermittlungen mit TK- und Internetbezug auf dem laufenden Stand zu halten

Polizeiliche Ermittlung; Ermittlungsmaßnahme; Befugnisnorm; Befugniszuweisung; Internet; Internetkriminalität; Telekommunikation; TKG P 113; TKG P 113 a; TKG P 113 b; Neuregelung; Rechtsgrundlage; Gefahrenabwehrrecht

ID-nummer: 20130387

Mayer, Arno; Bönisch, Markus; Schellenbeck, Siegfried; Kegel, Volker; Frantzen, Andreas

Ins Netz gegangen - Wenn die Polizei im Internet fischt; Neue Abteilung 'Iuk-Einsatz und Cybercrime' stellt sich vor

HPR - Hessische Polizeirundschau, 2013, 1, S. 8-13
mit 7 BILD, 3 TAF

Die hessische Polizei begegnet der rasanten Entwicklung im Bereich der Internetkriminalität mit der neuen Abteilung ‚IuK-Einsatz und Cybercrime'. Ermittlungen, Auswertungen, Internetrecherchen und IT-Beweissicherung sind in der Abteilung zentral gebündelt. Innerhalb der Abteilung gibt es die Sachgebiete (SG) 331 (IuK-Ermittlungen, Cybercrime, Auswertung), 332 (Task Force Internet, Ansprechstelle Kinderpornografie), 333 (Forensische IuK, Ermittlungsunterstützung) und 334 (Netzwerkforensik). Es bearbeiten speziell ausgebildete Ermittler gemeinsam mit IT-Spezialisten herausragende Fälle der Cybercrime in schwierigen, umfangreichen oder bedeutsamen Verfahren.

Polizeiarbeit; Polizeiliche Ermittlung; Internet; Internetkriminalität; Cybercrime; Ermittlungsgruppe; Ermittlungsarbeit; Hessen; Landeskriminalamt

ID-nummer: 20130612

Even, Burkhard

Prävention durch Information; Wirtschaftsspionage - vielfältige Risiken erfordern gemeinsames Handeln

IT-Sicherheit - Management und Praxis, 2013, 2, S. 36-39
mit 4 BILD, 2 QU

Made in Germany ist begehrt. Ein Synonym für technologischen Fortschritt, höchste Qualität und Präzision. Gerade deshalb stehen die deutsche Wirtschaft und besonders der deutsche Mittelstand im Fokus von Wirtschaftsspionen. Fremde Nachrichtendienste und Wettbewerber interessieren sich vor allem für zukunftsträchtige Technologien, die für die Wettbewerbsfähigkeit moderner Volkswirtschaften und bei der Eroberung von Märkten von Relevanz sind. Den Erkenntnissen des Bundesamtes für Verfassungsschutz zufolge sind die Nachrichtendienste der Russischen Föderation und der Volksrepublik China die Hauptträger von Spionageaktivitäten in Deutschland. Dies gilt für die Ausforschungsbereiche Politik, Militär sowie Wirtschaft, Forschung und Technik. Nach wie vor werden menschliche Quellen genutzt, um Zugang zu geschütztem Know-how zu erhalten. Zunehmende Bedeutung erhält jedoch auch die weltweite Datenvernetzung für neuartige Angriffs- und Ausspähungstechniken. Die Sicherheitsbehörden nehmen sich dieser neuen Herausforderungen an. Hierfür steht u.a. die im Jahr 2011 erfolgte Einrichtung des Cyber-Abwehrzentrums unter Federführung des Bundesamtes für Sicherheit der Informationstechnik (BSI) sowie unter Beteiligung des Bundesamtes für Verfassungsschutz (BfV). Ergänzend dazu schloss das BSI 2012 eine Allianz für Cybersicherheit mit dem Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), um auch in Kooperation mit der Wirtschaft die Sicherheit der IT-Infrastruktur und der deutschen Unternehmen zu fördern. Das BfV nimmt in diesem Aufgabenfeld eine wichtige Funktion ein. Mit seiner jahrzehntelangen Erfahrung im Bereich der Aufklärung von Spionageaktivitäten fremder Nachrichtendienste sieht es sich als Dienstleister für Spionageabwehr und als Partner der Unternehmen sowie von Forschungs- und Wissenschaftseinrichtungen.

Wirtschaftsspionage; Konkurrenzspionage; Sabotage; Cybercrime; Technologietransfer; Nachrichtendienstliche Tätigkeit; Wirtschaftsunternehmen; Kritische Infrastruktur; BSI; Bundesamt für Verfassungsschutz; Spionageabwehr; IT-Sicherheitskonzept; Unternehmensschutz; Sicherheitspartnerschaft

ID-nummer: 20130398

George, Michael

Cyberwar und Wirtschaftsspionage - Ein Strategiewechsel bei der Abwehr ist erforderlich; Gefahren der Wirtschaftsspionage von Unternehmen weitgehend unterschätzt

Der Kriminalist, 2013, 4, S. 23-25
mit 2 BILD, 1 QU

Angriffe aus dem Netz werden in absehbarer Zeit zu einem größeren Sicherheitsrisiko als Terrorismus. Beinahe täglich gibt es neue Berichte über Datendiebstahl, Wirtschafts- und Industriespionage oder den Verlust geheimer Dokumente. Die üblichen Verdächtigen sind oft schnell gefunden: schlecht administrierte Server, nachlässige Mitarbeiter, technische Defekte. Betroffen sein kann jeder - vom Privatmann über Wirtschaftsbetriebe bis zur Sicherheitsbehörde. In der Studie "Industriespionage 2012" gaben über 20 Prozent aller befragten Unternehmen an, in den letzten drei Jahren durch einen konkreten Spionagefall und/ oder Know-how-Abfluss geschädigt worden zu sein. Addiert mit der Anzahl der Verdachtsfälle (über 33 Prozent) ist also davon auszugehen, dass jedes 2. Unternehmen in Deutschland schon Ziel eines Spionageangriffs war. Am stärksten betroffen ist laut Studie nach wie vor der Mittelstand, zu dem in Bayern der überwiegende Teil der Unternehmen gerechnet wird. Wollen Firmen und Behörden vor dem Hintergrund der immer komplexeren Angriffe ihre schutzbedürftigen Informationen sichern, ist ein Strategiewechsel erforderlich. Das Bayerische Landesamt für Verfassungsschutz berät Unternehmen, wie sie sich besser vor dem Verlust wertvoller Informationen schützen können und liefert damit einen wichtigen Beitrag im Kampf gegen Wirtschaftsspionage.

Wirtschaftsspionage; Industriespionage; Betriebsgeheimnis; Datendiebstahl; Nachrichtendienst; Unternehmenssicherheit; Spionageabwehr; Sicherheitsrisiko; Sicherheitsmangel; Schutzkonzept; IT-Sicherheitskonzept; Bayern; Landesamt für Verfassungsschutz; Verfassungsschutz

ID-nummer: 20130406

Bönisch, Markus; Bretschneider, Harald

Der verdeckte polizeiliche Einsatz im Internet

Die Polizei, 2013, 4, S. 99-105
mit 46 QU

Verdeckte Ermittlungen im Cyberspace werden zukünftig immer größere Bedeutung erlangen. Nicht nur die Tatsache, dass alternative Wege, um an verborgene Informationen zu gelangen, nicht erfolgversprechend sind, spielt dabei eine Rolle. Der im Vergleich zur realen Welt deutlich geminderte Vertrauensschutz in Bezug zur Identität und zur Motivation des Gegenübers sollte Anlass sein, dieses Ermittlungsinstrument vermehrt einzusetzen.
Die Autoren befassen sich mit den mannigfaltigen juristischen Fragestellungen rund um den verdeckten polizeilichen Einsatz im Internet. Dabei wird zunächst die Notwendigkeit des legendierten Vorgehens bei Internetermittlungen verdeutlicht und im Anschluss daran aufgezeigt, dass die hergebrachten Rechtsgrundlagen und entwickelten Grundsätze für Ermittlungen in der realen Welt nicht ohne Weiteres auf die virtuelle übertragen werden können. Anhand der Rechtsprechung wird schließlich herausgearbeitet, was Polizeibeamte bei ihrem Einsatz im Internet zu beachten haben.

Verdeckte Informationsgewinnung; Verdeckte Datenerhebung; Polizeiliche Ermittlung; Nicht öffentlich ermittelnder Polizeibeamter; Verdeckter Ermittler; Cyberspace; Internetkriminalität; Internetplattform; Internetforum; Identitätstäuschung; Rechtsgrundlage; Online-Durchsuchung; HSOG; StPO P 110 a; StPO P 161; StPO P 163; Zugangskontrolle; Legende; Geheimhaltung

ID-nummer: 20130120

Artkämper, Heiko; Clages, Horst

Kriminalistik, 2013, 1, S. 41-43
Internetkriminalität - Das Internet und seine Wirkungen in sozialer, psychologischer und kriminalistischer Sicht; Bericht zur 9. Jahrestagung der Deutschen Gesellschaft für Kriminalistik e. V., Villingen-Schwenningen; BR Deutschland, 2012 [25.09.-26.09.]
mit 2 BILD, 3 QU

Das Leitthema der 9. Jahrestagung der DGfK befasste sich mit dem Phänomen Internetkriminalität und den vielfältigen Facetten der digitalen Nutzung und deren gesellschaftlichen Auswirkungen in sozialer und psychologischer Hinsicht.
Eröffnet wurde die Fachtagung durch den Präsidenten der DGfK Dr. Heiko Artkämper, der auf die aktuelle Relevanz des Phänomens Internetkriminalität sowohl für unser Gemeinwesen als auch für die Sicherheitsorgane hinwies. Wegen der vielfältigen Facetten der digitalen Realität wurde das Tagungsthema auf folgende Aspekte beschränkt:
- Auswirkungen der digitalen Nutzung auf das Individuum und die soziale Kompetenz
- mediales Informationsaufkommen und dessen Auswirkungen
- Sicherheit im Netz und deren Nutzer
- Datenschutz und Internet
- digitale Phänomene aus kriminologischer und kriminalistischer Sicht

Internetkriminalität; Phänomenologie; Computerkriminalität; Multimediale Technik; Soziales Netzwerk; Medienkompetenz; Cyberspace; Datensicherheit

ID-nummer: 20130304

Fuchs, Bernd

Schutz und Sicherheit im digitalen Raum; Ein Bericht vom 16. Europäischen Polizeikongress in Berlin

Kriminalistik, 2013, 3, S. 185-190
16. Europäischer Polizeikongress, Berlin; BR Deutschland, 2013 [19.02.-20.02]
mit 6 BILD, 4 QU

Allgemeine Betrugsdelikte, Diebstahl, Mobbing bis hin zur politischen Agitation und Rekrutierung von Extremisten verlagern sich zunehmend von der realen in die virtuelle Welt. Neue Wortschöpfungen wie Phishing, Malware oder Botnetze sind Synonyme für genuine kriminelle Phänomene. Vor allem junge Menschen kommunizieren mit Smartphones fast ausschließlich in Sozialen Netzwerken und unterschätzen häufig die damit verbundenen Gefahren. Aktueller denn je stellt sich die Frage, ob und in welcher Form der Staat und seine Sicherheitsbehörden in der Lage sein werden, im Spagat zwischen Freiheit und Sicherheit, jeden Einzelnen, aber auch das Gemeinwesen in Form der bestehenden Infrastrukturen, zu schützen. Der Autor gibt einen komprimierten Einblick in der Tagung.

Internetkriminalität; Cybercrime; Cyberspace; Internet; Sicherheitsanalyse; Sicherheitsaufgabe; Kriminalitätslage; Deliktart; Kriminalitätsverlagerung; Polizeiliches Handeln; Politisches Handeln; Freiheit; Datenschutz; Datenmissbrauch

ID-nummer: 20130544

Jaeger, Rolf Rainer

"Organisierte Kriminalität im Internet" - Die Strukturmerkmale und Besonderheiten der Internetkriminalität

Der Kriminalist, 2013, 5, S. 21-25
16. Europäische Polizeikongress 2013; "Schutz und Sicherheit im digitalen Raum", Berlin; BR Deutschland, 2013 [19.02.-20.02.]
mit 5 BILD

Der Referent führte sehr pointiert - aber auch sehr kritisch - in die Tagungsthematik ein. Dabei analysierte er die Strukturmerkmale und Besonderheiten der Internetkriminalität im Vergleich zur sonstigen Alltags-, Massen- und Organisierten Kriminalität. Er machte deutlich, dass die derzeitige OK-Definition völlig ungeeignet ist die kriminellen Aktivitäten im Bereich der Internetkriminalität einzuordnen - Cyberkriminalität eröffnet völlig neue Dimensionen der Kriminalität und erfordert entsprechende Bekämpfungsmethoden - wie etwa die Vorratsdatenhaltung. Darüber hinaus fordert er schlagkräftige Spezialdienststellen mit Internetkriminalisten, die sich ausschließlich mit diesen Phänomenen beschäftigen und nicht nur bei den Zentralstellen wie Landeskriminalämtern und dem Bundeskriminalamt angesiedelt sind, sowie eine möglichst kurzfristige Wiedereinführung einer speziell auf die Aufgaben der Kriminalpolizei in einem zusammenwachsenden Europa ausgerichteten einheitlichen Kriminalistenausbildung.

Internetkriminalität; Cybercrime; Computerkriminalität; Kriminalitätsphänomen; Organisierte Kriminalität; Internationale Kriminalität; Ermittlungsansatz; Bekämpfungsansatz; Bekämpfungskonzept; Vorratsdatenspeicherung

ID-nummer: 20130207

Starke Allianz; Instrumente zur IT-Sicherheit; Interview Hans Peter Friedrich - Annabelle Schott-Lung

W&S - Das Sicherheitsmagazin, 2013, 1, S. 14-15
mit 1 BILD

Beinahe jeden Tag kommt es zu Hackingattacken bei Behörden oder in der Wirtschaft. Das Szenario der letzten LÜKEX-Übung - Angriffe auf die IT von kritischen Infrastrukuren ist fast schon Realität geworden. Die Schäden, die dadurch entstehen, werden von Fachleuten auf zehn Milliarden Euro weltweit pro Jahr geschätzt.

IT-Sicherheit; Kritische Infrastruktur; Cybercrime; Wirtschaftsunternehmen; Industriebetrieb; Hacking; Abwehrmaßnahme; Sicherheitsstrategie

ID-nummer: 20121546

Ritter, Stefan

CERTs als zentrales Element nationaler Cyber-Sicherheit; Computernotfallteams

KES - Die Zeitschrift für Informations-Sicherheit, 2012, 6, S. 33-36
mit 1 BILD

CERTs (Computer-Emergency-Response-Teams) bieten mit ihrem auf Computernotfälle spezialisierten Wissen und Verfahren wertvolle Hilfen für die nationale Cybersicherheit. Ein wesentlicher Vorteil ist dabei die gute Vernetzung und Kooperation untereinander.
Neben der Bewertung und der Weitergabe von Schwachstelleninformationen der verschiedenen Software-Hersteller an die Kunden ist eine wichtige Aufgabe der Informationsaustausch zwischen den CERTs. Das Zusammenführen des verteilten Wissens durch den Austausch von Informationen führt in der vernetzten Welt zu konkreten und verbesserten Erkenntnissen sowie zu einer differenzierteren Lageeinschätzung.
Ein besonderer Typ sind nationale CERTs; davon gibt es in jedem Land lediglich eines. In Deutschland hat CERT-Bund diese Aufgabe übernommen. Als nationales CERT kommt dem Team neben der Vertretung der Interessen des Landes in internationalen Gremien und Treffen vor allem die Aufgabe des "CERT of last resort" - des "letzten Auswegs" - zu. Mit ihrer zentralen und vernetzten Rolle als Informationsdrehscheibe und "Helfer in der Not" spielen CERTs bei der Bewältigung von IT-Sicherheitsvorfällen und zur Wahrung der Cyber-Sicherheit in Deutschland eine wesentliche Rolle.

IT-Sicherheit; Sicherheitseinrichtung; Sicherheitsstrategie; Sicherheitsverbund; Sicherheitslage; Cybercrime; Informationssicherheit; Internationale Zusammenarbeit

ID-nummer: 20121555

Gauss, Daniel; Meyer, Stefan

Virtuelle Welten. Reale Gefahren. Herausforderungen der Kriminalität 2.0; Symposium zum 60-jährigen Jubiläum des Landeskriminalamtes Baden-Württemberg

Kriminalistik, 2012, 12, S. 707-714
Kriminalität 2.0, Stuttgart; BR Deutschland, 2012 [23.10.]
mit 2 BILD, 2 TAF

Die Lebenswirklichkeit der Menschen in der realen Welt ist mittlerweile so stark mit der virtuellen Welt verwoben, dass keine klare Trennlinie mehr gezogen werden kann. Mit der Verlagerung von Aktivitäten aller Lebensbereiche in den Cyberspace haben sich auch die Phänomene der klassischen Kriminalität dorthin verlagert. Aus diesem Grund hatte das Landeskriminalamt Baden-Württemberg sein 60-jähriges Bestehen zum Anlass genommen ein Symposium zu veranstalten, das sich interdisziplinär und über nationale Grenzen hinweg intensiv mit den Herausforderungen dieser "Kriminalität 2.0" auseinandersetzte. Aus unterschiedlichen Blickwinkeln wurden Probleme verdeutlicht, die die Digitalisierung des Alltags mit sich bringen, bereits eingeleitete Gegenmaßnahmen aufgezeigt, weitergehender Handlungsbedarf artikuliert und Lösungsansätze skizziert. Das Symposium für das Fachpublikum bot zudem den idealen Rahmen um einen "Internetsicherheits-Parcours" für die Bürgerinnen und Bürger einzuweihen.

Cybercrime; IT-Sicherheit; Sicherheitsanalyse; Sicherheitsstrategie; Kriminalitätsanalyse; Polizeiaufgabe; Polizeiausbildung

ID-nummer: 20121561

Meyer, Alexander

Das Web 2.0 - Möglichkeiten und Grenzen der strafprozessualen Ermittlung in sozialen Netzwerken

Kriminalistik, 2012, 12, S. 759-764
mit 1 TAF, 91 QU

Für die Sicherheitsbehörden können soziale Netzwerke von großem Interesse sein, da sie eine umfangreiche außerpolizeiliche Informationsdatenbank darstellen. Die öffentlich im Internet preisgegebenen Daten können bei der polizeilichen Fahndungs- und Ermittlungstätigkeit in vielfältiger Weise genutzt werden.
Daher verwundert es nicht, dass die deutschen Sicherheitsbehörden seit einigen Jahren bereits vielfältige Ermittlungsmaßnahmen in sozialen Netzwerken durchführen. Neben einer passiven Informationsbeschaffung durch das Beobachten eines offenen Chats oder das Identifizieren von bestimmten Zielpersonen kommt es auch zur aktiven Teilnahme der Ermittlungsbehörden, so zum Beispiel durch "legendiertes Chatten" in einer geschlossenen Gruppe.
Aus der staatlichen Tätigkeit in sozialen Netzwerken ergeben sich zwangsläufig rechtliche Fragestellungen. Da es sich um ein sehr neues Phänomen handelt, gibt es über die Entscheidung des Bundesverfassungsgerichts zur Onlinedurchsuchung hinaus wenig Rechtsprechung zu relevanten Problemfeldern und damit einen Rest Rechtsunsicherheit auf Ermittlerseite.
Der Verfasser geht in seiner Arbeit daher folgender Fragestellung nach: "Welche taktischen Möglichkeiten der Ermittlungen in sozialen Netzwerken stehen der Polizei zur Verfügung und welche rechtlichen Grenzen sind zu beachten?"
Dabei werden zunächst das Phänomen der sozialen Netzwerke beschrieben und polizeiliche Nutzungsoptionen aufgezeigt; im zweiten Schritt offene und verdeckte Maßnahmen der Ermittlungsbehörden mittels Analyse der einschlägigen Literatur und Auswertung der vorhandenen Rechtsprechung untersucht. Aus der abschließenden Beantwortung der Untersuchungsfrage im Fazit sollen Möglichkeiten der Optimierung abgeleitet werden.

Internetkriminalität; Internetforum; Soziales Netzwerk; Tatmittel; Polizeiliche Ermittlung; Ermittlungsführung; Informationserhebung; Datennutzung; Datenzugriff; Verdeckte Maßnahme; Fahndungshilfsmittel; Anlassunabhängige Recherche; Online-Durchsuchung; Recht auf informationelle Selbstbestimmung

ID-nummer: 20121547

Niggemann, Harald

Allianz für Cyber-Sicherheit

KES - Die Zeitschrift für Informations-Sicherheit, 2012, 6, S. 36-38
mit 1 BILD

Cyberangriffe werden von unterschiedlichen Tätergruppen mit diversen Zielsetzungen durchgeführt. Das Spektrum reicht von Denial-of-Service-Angriffen durch Aktivisten über die Manipulation von Internetbanking-Vorgängen durch Kriminelle bis hin zu Spionage und Sabotage in Behörden und Unternehmen durch fremde staatliche Stellen. Aufgrund der vielfältigen Szenarien und Formen von Angriffen im Cyberraum ist eine Schätzung der Schäden, die dadurch in Deutschland entstehen, schwierig. Unbestritten ist jedoch, dass nicht nur die Überlebensfähigkeit einzelner Institutionen bedroht ist. Auch IT-Systeme der kritischen Infrastruktur, die für unsere Gesellschaft von besonderer Bedeutung sind und zu denen beispielsweise die Energie- und Lebensmittelversorgung gehören, sind Teil des Cyberraums und stehen dadurch unter ständiger Bedrohung.
Der Herausforderung "Cybersicherheit" kann nur durch gemeinsame Anstrengungen von Wirtschaft, Wissenschaft und Verwaltung begegnet werden. Als Plattform für den Informations- und Erfahrungsaustausch auf diesem Gebiet haben das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) die Allianz für Cyber-Sicherheit gegründet.

Cybercrime; IT-Sicherheitskonzept; Sicherheitsmaßnahme

ID-nummer: 20121508

Schneider, Dieter; Gauss, Daniel

Cyberkriminalität und die Folgen der Digitalisierung des Alltags - die zentrale Herausforderung für Staat und Gesellschaft; Cyberkriminalität verändert die Kriminalitätslandschaft

Der Kriminalist, 2012; 2013, 12-1, S. 11-17 Villingen-Schwenningen; BR Deutschland, 2012 [September]
mit 4 BILD, 2 TAF, 6 QU

Neue Medien und Kommunikationsarten haben die Kriminalität wie kaum eine Entwicklung zuvor verändert. Ein erheblicher Teil der klassischen Straftaten findet sich zunehmend im Internet wieder. Das Internet ist sowohl Angriffsobjekt, Tatmittel als auch Beweismittel. Die Spurensuche ist im Netz aber denkbar schwieriger, denn der "Täter 2.0" ist weder behördlich gemeldet, noch hinterlässt er im weltweiten Netz eine eindeutige Visitenkarte. Seine digitalen Spuren sind flüchtig, austauschbar und leicht zu verschleiern.
Die beim LKA Baden-Württemberg geführten Ermittlungsverfahren bestätigen die in den vergangenen Jahren bereits festgestellte Entwicklung einer qualitativen und quantitativen Veränderung des Organisationsgrades der Täter und der von ihnen eingesetzten innovativen Techniken im Bereich der Cyberkriminalität. Die festgestellten Gruppierungen agieren international, arbeitsteilig, bandenmäßig und teilweise mit Strukturen der Organisierten Kriminalität.
In dem Beitrag werden die Auswirkungen dieses atemberaubenden technologischen Fortschritts und die damit verbundenen Konsequenzen für die Arbeit der Polizei aus dem Blickwinkel des Landeskriminalamts Baden-Württemberg dargestellt.

Cybercrime; Cyberspace; Kriminalitätsphänomen; Technologische Entwicklung; Internetkriminalität; Hacking; Computerstrafrecht; Ermittlungsverfahren; IT-Sicherheit; Baden-Württemberg

ID-nummer: 20121428

Bacigál, Ivan; Masárová, Mária

Soziale Netzwerke als Quelle polizeirelevanter Informationen; Verbreitung von Informationen in sozialen Netzwerken

MEPA - Mitteleuropäische Polizeiakademie, 2012, 2, S. 41-46
mit 1 TAB, 3 TAF

Mit der Entwicklung von Sozialnetzwerken und mit den ersten Versuchen künstliche Intelligenz hervorzubringen und zu nützen, wurden als Konkurrenzformen der realen Welt neue, virtuelle Welten hervorgebracht, und zwar mit dem Risiko, einen Teil des Privatlebens zu verlieren. Es ist ein Paradox, dass viele User der sozialen Netzwerke - also natürliche Personen, Bürger - deren Rechte auf Schutz des Privatlebens durch langjährig gestaltete Gesetzesnormen gesichert wurden, durch einen Klick auf ihre Rechte verzichten bzw. diese Rechte während der Nutzung sozialer Netzwerke schrittweise verlieren. Zudem fördert das Gefühl einer teilweisen bzw. absoluten Anonymität und Unidentifizierbarkeit den Missbrauch der sozialen Netzwerke.
Allerdings gab es in der Geschichte der Menschheit für operative Einheiten der Strafverfolgungsorgane kaum eine günstigere Zeitspanne für das Erfassen von Beziehungsstrukturen von Mitgliedern organisierter Verbrechensgruppierungen als in der Zeit nach der Entstehung sozialer Netzwerke. Dank der Zusammenarbeit der Betreiber und der Polizei bieten die sozialen Netzwerke der Polizei nach der Erfüllung bestimmter Kriterien Informationen an, die eine Menge polizeirelevanter Erkenntnisse beinhalten.

Soziales Netzwerk; Kommunikationsmittel; Informationsaustausch; Privatsphäre; Missbrauchsgefahr; Vertraulichkeit; Verdeckte Informationsgewinnung; Polizeiliche Ermittlung; Identitätsfeststellung

ID-nummer: 20121554

Oerting, Troels

Das Europäische Cybercrime Centre (EC3) bei Europol

Kriminalistik, 2012, 12, S. 705-706
mit 1 TAF

Die Europäische Kommission entschied Ende März 2012, Europol damit zu beauftragen, das EUROPÄISCHE CYBERCRIME ZENTRUM (European Cybercrime Center, EC3) aufzubauen. Es soll den Mitgliedstaaten zum 1. Januar 2013 zur Verfügung stehen und ab 2014 vollständig arbeitsfähig sein.
EC3 wird die Ermittlungen der Mitgliedsstaaten im Cyberspace unterstützen und zum Fokus der Europäischen Union werden. Eine Experten-Datenbank dient dem Austausch von Informationen (best practice) und der fachlichen Qualifikation. Die Zusammenarbeit mit einer Vielzahl von anderen Behörden, aber auch namhafter Unternehmen und Einrichtungen, wird weiterentwickelt, um letztendlich ein gemeinsames Ziel zu erreichen: Ein freies, offenes und sicheres Cyberspace. Der Leiter von EC3 und stellvertretende Direktor von Europol stellt in dem Beitrag seine neue Abteilung vor.

Cybercrime; Cyberspace; Technologische Entwicklung; Europol; Sicherheitsverbund; Sicherheitsstrategie; Bekämpfungskonzept

ID-nummer: 20121426

Jedrzejczak, Lukasz

Zusammenarbeit der Polizei mit den Sicherheitsabteilungen der sozialen Netzwerke

MEPA - Mitteleuropäische Polizeiakademie, 2012, 2, S. 32-35
mit 6 BILD

Am 11.11.2006 haben Studenten der Fachrichtung Informatik an der Breslauer Universität das Portal "nasza-klasa.pl" gegründet. Im Juni 2012 wurde das Portal von nasza-klasa.pl auf nk.pl umbenannt und ist unter den populärsten Seiten im polnischen Internet auf Platz elf.
Nl.pl (ursprünglich nasza-klasa.pl) kann auch eine sehr gute Informationsquelle für die Polizei sein, die Personen sucht, die sich vor den Verfolgungsorganen verbergen oder mit Hilfe eines Steckbriefs gesucht werden und sich oft in solche Portale einloggen, aktuelle Fotos anhängen und Kontakte verteilen. Die Zusammenarbeit mit der Sicherheitsabteilung des Portals beeinflusst die schnelle Feststellung des Einloggens eines Users und dem zufolge die Bestimmung seines Aufenthaltsorts. In dem Aufsatz werden zwei Fälle beschrieben, wie Straftäter, die das überall im Land bekannte Portal genutzt haben, von der Polizei ermittelt wurden.

Polen; Internetkriminalität; Soziales Netzwerk; Polizeiliche Ermittlung; Ermittlungsarbeit

ID-nummer: 20121424

Kedzierzawska, Anna

Sexting in sozialen Netzwerken - gegenwärtige Herausforderung für die Polizei

MEPA - Mitteleuropäische Polizeiakademie, 2012, 2, S. 21-27
mit 5 QU

Aus vor einigen Jahren in den Vereinigten Staaten durchgeführten Untersuchungen geht hervor, dass jeder fünfte junge Mensch seine eigenen oder fremde Nacktfotos schon per Telefon, iPhone oder Mail verschickt oder in einem sozialen Netzwerk veröffentlicht hat. Am Anfang sieht alles ganz sicher aus. Leider verändert sich diese Situation mit der Zeit dramatisch: Es gibt Erpressung, Demütigung und sogar Selbstmordversuche. Weltweit wurden schon Fälle bekannt, in denen sich Mädchen selbst umgebracht haben, gleich nachdem ihre Nacktfotos im Internet gefunden wurden. Das sogenannte Sexting entwickelt sich damit zu einer Herausforderung für Eltern, Schule, Polizei, Staatsanwaltschaft, Gericht und viele andere Institutionen. Auch in Polen wird angenommen, dass dieses Problem immer mehr Jugendliche betrifft, besonders im Gymnasiums- und Obergymnasiumsalter.
Das polnische Recht reguliert die Problematik des Abbildungsschutzes in zwei Verordnungen: im Gesetz über Urheberrecht und Schutzrechte und im Strafgesetzbuch. Wenn man z.B. im Internet Nacktfotos oder Fotos während einer Sexualtätigkeit ohne die Einwilligung der teilnehmenden Personen veröffentlicht, wird dieser Sachverhalt von der Polizei und Staatsanwaltschaft überprüft. Wenn wir mit dem Verstoß gegen Persönlichkeitsgüter zu tun haben, kann man das Problem auf dem Zivilrechtsweg lösen.

Polen; Internetplattform; Soziales Netzwerk; Fotografie; Bildnisveröffentlichung; Pornographie; Minderjähriger; Persönlichkeitsrecht

ID-nummer: 20121423

Simonin, Mathieu

Tatort Soziale Netzwerke

MEPA - Mitteleuropäische Polizeiakademie, 2012, 2, S. 15-20
mit 1 TAF

Die Schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) erhält jährlich über 6.000 Meldungen zu verdächtigen, das heißt möglicherweise illegalen Internetinhalten. Die Angaben werden einer ersten Prüfung unterzogen, die Daten gesichert und die Meldung an die zuständige Strafverfolgungsbehörde im In- oder Ausland weitergeleitet. KOBIK beantwortet auch Fragen zu verdächtigen Internetseiten und durchsucht das Internet nach Websites mit strafrechtlich relevantem Inhalt.
Der Autor gibt einen Überblick über die Formen, in denen das Internet und vor allem soziale Netzwerke für kriminelle Zwecke missbraucht werden und zeigt Möglichkeiten auf, die sich den Strafverfolgungsbehörden bieten, diese Netzwerke als Ermittlungsinstrument in ihre Arbeit einzubeziehen.

Schweiz; Internetkriminalität; Soziales Netzwerk; Missbrauchsgefahr; Strafverfolgungsbehörde; Ermittlungsansatz

ID-nummer: 20121422

Zeiler, Uwe; Kleile, Martin

Internet und Web 2.0 - Mehrwert für polizeiliche Ermittlungen in Deutschland

MEPA - Mitteleuropäische Polizeiakademie, 2012, 2, S. 7-14
mit 1 TAF, 6 BILD

Das Internet ist weltweit aus dem Alltag nicht mehr wegzudenken. Virtuelle Soziale Netzwerke sind für viele Menschen heutzutage Bestandteil ihres täglichen Lebens. In den Netzwerken werden durch die Nutzer massenhaft persönliche Daten eingestellt wie beispielsweise Bilder, Videos sowie Informationen über Hobbies und zum Berufsleben. Darüber hinaus geben die Vernetzung mit "Freunden" sowie Diskussionsbeiträge weitere Informationen über den Verfasser preis, die auch für die polizeilichen Ermittlungen von großer Bedeutung sein können.
In dem Beitrag zeigen die Verfasser die Möglichkeiten auf, welche insbesondere das Web 2.0 der Polizei bei der täglichen Ermittlungsarbeit bietet und geben Hinweise, wie Daten gerichtsverwertbar gesichert werden können.

Soziales Netzwerk; Internetplattform; Neue Medien; Chatprogramm; Polizeiliche Ermittlung; Datenerhebung; Informationserhebung; Verdeckte Datenerhebung; Personenfahndung; Täteridentifizierung

ID-nummer: 20130035

Barchnicki, Sebastian; Pohlmann, Norbert

"Bezahlen" mit dem guten Namen; Facebook als Angriffstool für Cybercrime

IT-Sicherheit - Management und Praxis, 2012, 6, S. 53-57
mit 8 TAF

Die Webseite von Facebook ist einladend: Unter der Registrierung steht "Facebook ist und bleibt kostenlos". Das weltgrößte soziale Netzwerk suggeriert eine kostenlose Erfahrung, die ein umfangreiches Angebot an Informationen und Kontakten mit einschließt. Auch wenn kein Geld fließt - bezahlt wird dennoch: mit persönlichen Daten der Nutzer, für die sich Facebook weitreichende Rechte in den AGBs als Gegenleistung einräumen lässt. Über individualisierte Werbung kommt schließlich doch Bares in die Kasse. Die persönlichen Daten aber bilden auch ein attraktives Ziel für Kriminelle, die sich damit entweder direkt bereichern oder die bei weiteren Usern Missbrauch treiben wollen.
Die Autoren schildern unterschiedliche Angriffsmethoden:
- Angreifer erstellen eine scheinbar echte Fan-Seite
- Gefälschte Facebook-E-Mail-Benachrichtigungen versenden
- Manipulierte Anwendungen (Apps) anbieten
- Horror-, Sex- oder Promi-Video anbieten
- Hoaxes und falsche Warnungen verbreiten
- Identitätsdiebstahl und Gutgläubigkeit oder "Bitte sende mir schnell Geld".
Darüber hinaus geben die Autoren Tipps für den adäquaten Umgang mit dem sozialen Netzwerk.

Soziales Netzwerk; Hacking; Internetkriminalität; Internetplattform; Cybercrime; Datenmanipulation; Datendiebstahl; Datenmissbrauch; Personendaten

ID-nummer: 20121421

"Unternehmen müssen ihre Mitarbeiter stärker für die Cybercrime-Risiken sensibilisieren"; Interview mit Hans Helmut Janiesch

DSD - Der Sicherheitsdienst, 2012, 1, S. 20-22
mit 1 BILD

Hans-Helmut Janiesch verfügt als ehemals leitender Polizeidirektor/Kriminaldirektor und Mitglied des "Kötter-Sicherheitsbeirates" über wichtige Erfahrungen in Hinblick auf die Kooperation von Polizei und Sicherheitsunternehmen. In einem Interview beantwortet er Fragen zu Cybercrime - unter der alle Straftaten zu verstehen sind, die unter Ausnutzung moderner Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden - und geht dabei sowohl auf die Bedrohungslage als auch auf Sicherheitsmaßnahmen ein.

Unternehmenssicherheit; IT-Sicherheit; Cybercrime; Hacking; Gefahrenanalyse; Sicherheitsrisiko

ID-nummer: 20130033

Recino, Angela

Umstellen auf Abwehrkette; Neue Taktik gegen gezielte Angriffe

IT-Sicherheit - Management und Praxis, 2012, 6, S. 40-41
mit 1 BILD

Sie nehmen drastisch zu, werden immer komplexer und bleiben oft unbemerkt - gezielte Angriffe auf Großunternehmen, innovative Mittelständler und öffentliche Institutionen. Bei den Advanced Persistent Threats, kurz APTs, geht es Cyberkriminellen meist darum, aus dem geistigen Eigentum Dritter Profit zu schlagen. Fachleute gehen davon aus, dass Konzerne und große Mittelständler sowie Institutionen mit hoheitlichen Aufgaben innerhalb der nächsten sechs Monate von einem "ernsthaften Vorfall" bedroht sind. Es ist anzunehmen, dass auch alle 30 DAX-Unternehmen von APTs betroffen sind. Die Schäden sind enorm. Verhindern lassen sich solche Angriffe noch nicht, immerhin aber deutlich begrenzen. Der Schlüssel ist ein ganzheitliches Threat-Management, das effektive Technologie und qualifizierten Service sinnvoll miteinander verbindet.

Cybercrime; Datendiebstahl; Computerspionage; Schadsoftware; Computervirus; IT-Sicherheit

ID-nummer: 20121386

Bendiek, Annegret; Wagner, Ben

Die Verfassung des Internets; Die EU muss eine gemeinsame Strategie für Cybersicherheit erarbeiten

Internationale Politik, 2012, 6, S. 85-92
mit 1 BILD, 3 QU

Die globale Cyberpolitik befindet sich in einer entscheidenden Phase. Im Dezember 2012 verhandeln Vertreter von über 190 Staaten in Dubai über die International Telecommunications Regulations (ITRs), wobei nicht nur die Regulierung, sondern auch die normativen Grundlagen des Internets der Zukunft beraten werden. Dabei stellen sich folgende Fragen: Wie viel Freiheit soll das Internet gewährleisten, welche Sicherheitsvorkehrungen muss es gegen Kriminalität und Terrorismus geben und wo sollen die Grenzen zwischen nationaler Selbstbestimmung und globalem Raum verlaufen? Wird es zukünftig überhaupt noch ein globales Internet geben oder verstärkt sich der bereits zu beobachtende Trend einer Fragmentierung des Netzes und vermehrter nationaler Kontrolle über Zugang und Inhalte?

Internet; Cybercrime; Cyberterrorismus; Spionage; Spionageabwehr; IT-Sicherheit; Politik; Strategieentwicklung; Politisches Handeln; Europäische Union

ID-nummer: 20121385

Glenny, Misha

Das Ende der Nettigkeiten; Cyberkrieg und Sicherheit im Internet

Internationale Politik, 2012, 6, S. 80-84
mit 1 TAF

In den vergangenen Jahren hat die technologische Entwicklung auf einem Sektor rasante Fortschritte zu verzeichnen - dem Cyberkrieg.
Zum Thema Cyberkrieg existieren zwei diametral entgegengesetzte Auffassungen. Auf der einen Seite herrscht der Glaube vor, dass wir bereits von einem potenziellen Großangriff bedroht sind, der unsere vernetzten Computersysteme weitgehend lahm legen könnte. Anhänger dieser These meinen, dass unsere sozialen und wirtschaftlichen Infrastrukturen bereits so stark von Computernetzwerken abhängig sind, dass eine Serie von Angriffen mit Schadsoftware eine Katastrophe auslösen könnte. Die andere Denkschule geht davon aus, dass die Gefahr des Cyberkriegs systematisch übertrieben wird und dass die Albtraumvisionen nur in Gedankenwelten existieren. Politisch motivierte "Hacktivisten" wie die Gruppe "Anonymous" argumentieren, dass das Säen von Angst und Zweifel dazu beitragen solle, die Gewinne der wachsenden Cybersicherheitsindustrie zu mehren und zugleich die hohen Investitionen des Militärs in Hochtechnologiewaffen zu rechtfertigen.
In dem Beitrag untersucht der Verfasser folgende Fragen. Was ist Cyberkrieg? Gibt es ihn? Und wie gefährlich ist er?

Cybercrime; Cyberspace; Internetkriminalität; Hacking; Schadsoftware; Computervirus; Spionage; Datenspionage; Technologische Entwicklung

ID-nummer: 20121084

Nur die Drogenmafia ist schlimmer; Die Dimension der Wirtschaftskriminalität; Interview Jörg Ziercke - Klaus Henning Glitza

W&S - Das Sicherheitsmagazin, 2012, 4, S. 12-13
mit 1 BILD

Strukturen der Organisierten Kriminalität haben längst das "Geschäftsfeld" Wirtschaftskriminalität entdeckt. Delikte zum Nachteil von Unternehmen rangieren in der Kriminalstatistik gleich hinter dem illegalen Rauschgifthandel. Die Studie einer Wirtschaftsprüfungsgesellschaft kommt zu dem Ergebnis, dass 73 Prozent der befragten Unternehmen von Wirtschaftskriminalität betroffen sind. Dennoch werden den Strafverfolgungsbehörden aus Furcht vor Image- und Reputationsschäden viele dieser Straftaten nicht gemeldet. Insofern ist von einem hohen Dunkelfeld auszugehen. Laut Bundeslagebild Wirtschaftskriminalität 2010 wird inzwischen bei mehr als jedem vierten Fall das Tatmittel Internet eingesetzt, insbesondere im Betrugsbereich.

Wirtschaftskriminalität; Wirtschaftsunternehmen; Korruption; Betrug; Internetkriminalität; Dunkelfeld; Zusammenarbeit; Bundeskriminalamt

ID-nummer: 20121075

Kudlich, Hans

Straftaten und Strafverfolgung im Internet; Zum strafrechtlichen Gutachten für den 69. Deutschen Juristentag 2012

StV - Strafverteidiger, 2012, 9, S. 560-566
mit 69 QU

Die strafrechtliche Abteilung des 69. Deutschen Juristentages in München befasste sich im Jahr 2012 mit dem Problemkreis Strafrecht und Internet. Der Deutsche Juristentag hat mit dem Direktor des Freiburger Max-Planck-Instituts, Ulrich Sieber, einen der unbestrittenen Spezialisten auf diesem Gebiet und vor allem auch der Pioniere des Informationsrechts als Gutachter gewinnen können. Entsprechend ist auch sein Gutachten ein beeindruckendes Werk geworden, das eine ganz außergewöhnliche Tour d' Horizon zu dem Thema Strafrecht und Internet bietet. Im Gutachten gelingt es Sieber anschaulich, einen roten Faden erkennen zu lassen und dennoch gemessen am beschränkten Umfang eine erstaunliche Informationsfülle und eine Vielzahl von Details zu behandeln. Es enthält neben strafrechtsdogmatischen Darlegungen auch mehr oder weniger ausführliche empirisch-kriminologische, rechtsvergleichende und rechtspolitische Teile.
In dem Beitrag werden einige besonders interessante bzw. aktuelle Aspekte kurz angerissen. Der Autor zeigt auf, wie vielfältig die unter dem Stichwort Strafverfolgung und Internet diskutierten Probleme sind und dass sich diese durch geänderte technische und gesellschaftliche Rahmenbedingungen auch gegenwärtig noch ständig wandeln.

Internet; Internetkriminalität; Strafverfahren; Strafrecht; Strafverfolgungsmaßnahme; Strafverfolgungsbehörde; Informationsrecht; Ermittlungsverfahren; Tatbestandsmerkmal; Online-Durchsuchung; Telekommunikationsüberwachung; Cloud Computing; Soziales Netzwerk; StPO P 110 a; StPO P 100 a; StPO P 100 b

ID-nummer: 20121346

Stockhausen, Lucas von

Top-Risiken im Cyberspace; Schweregrad von Sicherheitslücken im Web nimmt zu

IT-Sicherheit - Management und Praxis, 2012, 5, S. 23-25
mit 4 TAF

Mit dem "Top Cyber Security Risks Report" gibt HP im Halbjahres-Rhythmus einen Überblick über Sicherheitslücken und Angriffs-Trends. Der Zweck dieses Reports ist es, die größten Risiken aufzuzeigen, sodass Unternehmen und Verwaltungen entsprechende Prioritäten in ihren Schutzstrategien setzen können.
In dem Beitrag werden ein paar zentrale Ergebnisse des Gesamtjahres-Reports für das Jahr 2011 zusammengefasst, wobei ein Schwerpunkt auf die Sicherheitslücken und dabei insbesondere auf die der Web-Anwendungen gelegt wird. Die dokumentierten Ergebnisse beruhen auf der statischen Analyse von 359 unterschiedlichen Anwendungen. Die Ergebnisse zeigen, dass Web-Anwendungen auf mehreren Ebenen verwundbar sind.

Cyberspace; Sicherheitslage; Sicherheitsdefizit

ID-nummer: 20121349

Propach, Thomas; Pohlmann, Norbert

Die Kunst des weißen Hackens; Ziele, Methoden und Praxis des Penetrationstests

IT-Sicherheit - Management und Praxis, 2012, 5, S. 62-64
mit 1 TAF, 3 QU

Beinahe täglich hört man von erfolgreichen Hackerangriffen und gestohlenen Unternehmensdaten. Jede Woche werden große Unternehmen Opfer von Cyberangriffen. Die Hacker finden immer wieder Schwachstellen in den IT-Systemen der Unternehmen, die sie für erfolgreiche Angriffe nutzen können. Doch warum sind Hacker so erfolgreich, und wie kann sich ein Unternehmen besser vor ihnen schützen - Penetrationstests liefern darauf eine Antworten. In dem Beitrag werden diese Testszenarien erläutert.

IT-Sicherheit; Unternehmenssicherheit; Hacker; Hacking; Testverfahren; Schwachstellenanalyse

ID-nummer: 20130922

Kögel, Helko; Rosmus, Konrad

Cyber Security und Kritische Infrastrukturen im Kontext neuer Bedrohungslagen

Jahrbuch Öffentliche Sicherheit, 2012, Sonderbd 6.3 [2. Aufl.], S. 115-129
mit 23 QU

Bei Kritische Infrastrukturen - und alle anderen Bereichen mit IT-Abhängigkeiten - können Schwachstellen auf allen Ebenen, von der menschlich-sozialen Ebene bis zum Mikrobefehl im Prozessor vorliegen. Dies nichts Neues ist. Neu hingegen ist, dass diese Schwachstellen auch konsequent ausgenutzt werden. Im Sekundentakt werden zahlreiche Computer über das Internet angegriffen. Bundes- und EU-Behörden, Unternehmen, Militärische Einrichtungen, Betreiber kritischer Infrastrukturen und somit wesentliche Säulen von Wirtschaft und Gesellschaft sehen sich massiven Bedrohungen ausgesetzt.
Daher kommt der sog. Cyber Security eine stetig steigende Bedeutung zu. Cyber Security umfasst alle Maßnahmen zur Erreichung und Aufrechterhaltung der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit) im sog. "Cyber Space". Sie beinhaltet vorbeugende Elemente wie die Etablierung von Regeln und den Aufbau von Sicherheitsinfrastrukturen und operative Aufgaben wie die Beseitigung von Software-Schwachstellen und die Aktualisierung von Schutzmechanismen bis hin zu aktiven Maßnahmen gegen Bedrohungen wie dem Ausheben von Botnetzen. In diesem Sinne ist Cyber Security sowohl auf Individuen als auch Objekte oder Systeme bezogen und muss im Zusammenhang zukünftig als durchgängige Aufgabe für die Entwicklung von Prozessen, Anwendungen und Produkten wahrgenommen werden.
In dem Beitrag werden einige neue bzw. zu neuer Bedeutung gelangte Bedrohungsarten kurz beschrieben, Attribute und Kriterien zu ihrer Beschreibung und Bewertung angeführt und exemplarisch die Bedeutung für wichtige Infrastrukturen angesprochen. Die Ausführungen stellen keine systematische oder gar vollständige Behandlung des Themas dar, sondern greifen einige interessante Fragestellungen heraus, welche aus Sicht der Autoren nicht aus den Augen verloren gehen dürfen, sondern vielmehr einer systematischen Untersuchung und Bewertung unterzogen werden sollten.

Cybercrime; Cyberspace; Kritische Infrastruktur; Angriffsziel; Gefahrenanalyse; Bedrohungspotential; Computermanipulation; Computervirus; Schadsoftware; Schwachstellenanalyse; IT-Sicherheit

ID-nummer: 20121102

Redler, Ursula

Die strafprozessuale Online-Durchsuchung; Ein Gesetzesentwurf

Strafrecht in Forschung und Praxis, 2012, Bd 233, 210 S.
mit 1 TAB, ANL, LITVZ S. 25-38

Die Arbeit beleuchtet zunächst die Problematik der zunehmenden Internetkriminalität, insbesondere am Beispiel der Nutzung des Internets durch terroristische Vereinigungen respektive (potentielle) Terroristen. Vor diesem Hintergrund wird die technische Umsetzbarkeit und (mögliche) Umsetzung einer strafprozessualen Online-Durchsuchung sowie die aktuelle Rechtslage in der Strafprozessordnung sowie im polizeilich-präventiven Bereich thematisiert. Sodann beschäftigt sich die Autorin mit der Frage der Vereinbarkeit einer Rechtsgrundlage für eine strafprozessuale Online-Durchsuchung mit dem Grundgesetz. Auf der Basis der so gewonnenen Erkenntnisse wird abschließend ein konkreter Gesetzentwurf mit Erläuterungen für einen § 100k StPO als Rechtsgrundlage für eine strafprozessuale Online-Durchsuchung aufgezeigt.

Internetkriminalität; Terrororganisation; Ermittlungsmethode; Online-Durchsuchung; Datenerhebung; Rechtslage; Rechtsgrundlage; GG; Gesetzentwurf; StPO P 100 a; StPO P 100 c; StPO P 100 i; StPO P 102; Schutzbereich; Ermächtigungsgrundlage

ID-nummer: 20121229

Dirro, Toralv

Spezialisiert auf Unternehmenskonten; Neue Angriffe durch Banking-Trojaner

WIK - Zeitschrift für die Sicherheit der Wirtschaft, 2012, 5, S. 36-37

Inzwischen werden nicht mehr nur große Finanzinstitute und mehr oder weniger zufällig ausgewählte Kunden Opfer von Cyber-Kriminellen. Wie eine aktuelle Untersuchung zeigt, haben Cyberkriminelle mit Blick auf die höheren Kontenstände bei Unternehmen, Verfahren entwickelt, um auch höhere Sicherheitsvorkehrungen auszuhebeln.
Im Rahmen der Untersuchung wurden erfolgreiche Angriffe bei weltweit 60 Banken festgestellt. In Deutschland wurden 176 betroffene Konten identifiziert, von denen insgesamt knapp 1 Mio. € entwendet wurden. Die Täter sind weiterhin aktiv und haben ihre Trojaner bisher jeweils so angepasst, dass sie die Erkennung durch Antiviren-Programme unterlaufen können. Der Betrugsring, der aufgrund der Höhe der Beträge auf den Überweisungen "High Roller" genannt wird, besteht aus mindestens einem Dutzend Gruppen. Verwendet werden bei den Kontoabschöpfungen neuartige Techniken, die auch automatisierte Überweisungen, völlig ohne menschliches Zutun, erlauben.
Unternehmen sollten sowohl ihre Sicherheitskontrollen verstärken als auch die Schulung der Mitarbeiter mit Überweisungsberechtigungen intensivieren, um sie gegen die auch bei "High Roller" nach wie vor nötigen Social-Engineering und Phishing-Angriffe zu wappnen. Zudem dürfte die neue Angriffsform auch dann erfolglos bleiben, wenn Unternehmen ihre Kontrollen und Erkennungssoftware in mehreren Schichten eingerichtet haben.

Cybercrime; Kreditinstitut; Bankkonto; Online-Banking; Phishing; Schadsoftware

ID-nummer: 20121545

Oelmaier, Florian

Mehr als Abwehr; Umfassende Sicherheitsstrategien brauchen auch eine gute Vorfallsbearbeitung und Vorsorge zur Forensik

KES - Die Zeitschrift für Informations-Sicherheit, 2012, 6, S. 24-27
mit 1 TAF, 9 QU

Investitionen in Sicherheit dürfen sich nicht auf eine reine Vorfallsprävention beschränken. Denn noch so gute Abwehrmaßnahmen werden nicht jeden Security-Incident verhindern - und dann sind passende Mechanismen und Ressourcen zur Erkennung, Behandlung und Verfolgung der Vorfälle gefragt. Im Zeitalter des Cyberwars - der systematischen und von langer Hand geplanten Attacken, verübt von gut ausgerüsteten Angriffseinheiten - geht es bei der Verteidigung der IT-lnfrastruktur nicht mehr um das "Ob", sondern um das "Wann". Jede IT-Sicherheitsabteilung sollte die deutsche Cybersicherheitsstrategie und die Aufgabenteilung zwischen Landeskriminalämtern, Bundeskriminalamt, Landes- und Bundesämtern für Verfassungsschutz sowie BSI kennen und wissen, wer bei welchem Vorfall zu informieren ist.

IT-Sicherheit; Sicherheitsstrategie; Strategieentwicklung; Cybercrime; Sicherheitsmaßnahme

ID-nummer: 20121109

Anonym

Lagebericht zur Informations-Sicherheit

KES - Die Zeitschrift für Informations-Sicherheit, 2012, 4, S. 26-30, 32-34; 5, S. 47-52, 54-55; 6, S. 52-60
mit 2 BILD, 25 TAF, 28 TAB

Verlässliche und neutrale Zahlen zur Informations-Sicherheit im deutschsprachigen Raum sind selten - noch seltener sind konkrete Angaben zu aufgetretenen Schäden und Budgets. Die Grundlage für die im Beitrag vorliegenden Daten haben die Teilnehmer an der diesjährigen kes/Microsoft-Sicherheitsstudie im Rahmen einer selbstkritischen Bestandsaufnahme durch die Arbeit mit dem Studien-Fragebogen gelegt. Es gingen 133 verwertbare Fragebögen ein - ein beträchtlicher Teil davon kam erneut aus kleinen und mittleren Unternehmen (KMU) mit unter 500 Mitarbeitern (55 %), doch auch größere Organisationen waren wieder stark vertreten (42 %- 3 % k. A.).
Der erste Teil der Auswertung befasst sich vor allem mit der aktuellen Risikosituation, im zweiten Teil der Auswertung geht es überwiegend um Strategie und Management der Informationssicherheit sowie Kenntnisstand und Weiterbildung. Teil 3 befasst sich mit Maßnahmen, Vertraulichkeit und Netznutzung, Netzwerksicherheit, Endgerätesicherheit, Content- und E-Mail-Security, Open-Source-Software, Notfallvorsorge, Datenverluste und Forensik sowie Dienstleistungen.

IT-Sicherheit; Informationssicherheit; Unternehmenssicherheit; Datensicherheit; Sicherheitsanalyse; Sicherheitslage; Sicherheitsmanagement; Risikoanalyse; Risikoabwägung; Vertraulichkeit; Netzwerk; Sicherheitssystem; Spam-E-mail; E-mail

ID-nummer: 20121055

Robles, Antonio González; Pohlmann, Norbert

Smart Objects und Objekt-Identitäten im globalen Internet; Risiken der Standard-IT-Vernetzung in kritischen Infrastrukturen und in der Industrie

IT-Sicherheit - Management und Praxis, 2012, 4, S. 54, 56-58
mit 1 BILD, 1 QU

Ein nach wie vor großer Teil der deutschen Industrie ist mit alter, industrieller, meist sehr proprietärer IT-Technologie versehen. Das mag nicht ganz zeitgemäß sein, hat jedoch den klaren Vorteil, dass hier so gut wie keine Angriffsflächen für externe Manipulationen existieren. Inzwischen gibt es jedoch den Trend, industrielle Umgebungen mit Standard-IT-Netzwerken zu verbinden und weitere Austauschmöglichkeiten wie beispielsweise DVD-Laufwerke und USB-Anschlüsse einzurichten. Damit werden Angreifern sämtliche Einfallstore geöffnet, die auch in klassischen Büroumgebungen üblich sind. Hinzu kommt noch, dass mehr und mehr auch das "Internet der Dinge" und die damit einhergehende Integration von intelligenten Objekten (Smart Objects) Fahrt aufnimmt. Und was für die Industrie gilt, gilt ebenso für Organisationen und Einrichtungen, ohne die eine moderne Gesellschaft nicht funktionieren könnte, die sogenannten "Kritischen Infrastrukturen" (KRITIS). Um ein hohes Sicherheitsniveau auch unter den neuen Gegebenheiten aufrechtzuerhalten, müssen sowohl in der Industrie als auch in KRITIS zunächst strukturell bedingte IT-Sicherheitsschwächen behoben werden. Des Weiteren gilt es, die durch die Smart Objects eingebrachten Fähigkeiten und Objekt-Identitäten besonders zu berücksichtigen. Um auch die Fähigkeiten der Identifikation und des Ausführens systematisch handhaben zu können, muss ein Identity-Management-Konzept erarbeitet werden, das neben den personen- auch die objektbezogenen Identitäten mit ihren Fähigkeiten einbezieht.

Industriegesellschaft; Industriebetrieb; Kritische Infrastruktur; Vernetzung; Informationstechnologie; Informations- und Kommunikationstechnologie; Cybercrime; Gefahrenpotential; IT-Sicherheit; Sicherheitsrisiko; Schwachstellenanalyse

ID-nummer: 20121054

Die populären Betriebssysteme sind nicht sicher zu kriegen! Interview Sandro Gaycken - Stefan Mutschler

IT-Sicherheit - Management und Praxis, 2012, 4, S. 32-35

Fundamentale Cybersicherheitsprobleme für Wirtschaftsunternehmen und Behörden sind beispielsweise, dass populäre Betriebssysteme nicht für Sicherheit entwickelt wurden und dass die IT-Sicherheitsindustrie auf Angriffs-Paradigmen basiert, die es so längst nicht mehr gibt. So sieht es zumindest Dr. Sandro Gaycken, Technik- und Sicherheitsforscher an der Freien Universität Berlin. Im Gespräch mit IT-SICHERHEIT erklärt Dr. Gaycken, warum perfekte Sicherheit auch langfristig eine Illusion bleibt, mit welchen Maßnahmen dennoch ein gewisses Maß an Sicherheit herstellbar ist und wie sich aktuelle Trends wie geheimdienstlich unterstützte Spionage, Cloud Computing und Mobility auf die Sicherheit von IT-Systemen auswirken.

IT-Sicherheit; Spionage; Hacking; Cybercrime

ID-nummer: 20121110

Jaschob, Angelika; Kleinert, Till

Cyber-Sicherheit ist nur in Kooperation erreichbar

KES - Die Zeitschrift für Informations-Sicherheit, 2012, 4, S. 41-44
mit 1 TAB, 2 TAF, 7 QU

Komplexen und professionellen Gefährdungen im Cyber-Raum wirksam entgegenzutreten, ist für einzelne Akteure in vielen Fällen unmöglich - nur gemeinsam, durch den Zusammenschluss vieler wichtiger Akteure, kann man dieser Bedrohung begegnen. Die Ende Mai als Pilot gestartete Allianz für Cyber-Sicherheit in Deutschland will sich dieser Aufgabe stellen. Es genügt nicht mehr, dass sich der Einzelne abschottet und seine "Grenzen" zum Internet absichert: Anzahl, Komplexität und Professionalität der Cyber-Angriffe nehmen stetig zu. Dabei können Cyber-Angriffe sowohl die Verfügbarkeit von Diensten oder Geschäftsprozessen beeinträchtigen als auch das Ausspionieren von vertraulichen Informationen, Entwicklungsdaten oder die Destabilisierung von Kommunikationsnetzen oder Produktionsprozessen zum Ziel haben. Ein zusätzliches Problem stellt die Ortsunabhängigkeit der Täter da: Cyber-Angriffe können von jedem Ort der Welt aus durchgeführt werden.

Cybercrime; IT-Sicherheit; Schwachstellenanalyse; Gefahrenlage; Zusammenarbeit

ID-nummer: 20121052

Oelmaier, Florian

Die Angst sitzt tief; Die Grenzen technischer Sicherheitsmaßnahmen

IT-Sicherheit - Management und Praxis, 2012, 4, S. 18-20
mit 3 TAF, 1 QU

Die von Corporate Trust in Zusammenarbeit mit Brainloop und dem TÜV SÜD durchgeführte Studie "Industriespionage 2012 - Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar" offenbarte Stärken und Schwächen im Informationskrieg. So sollten die befragten Unternehmen sowohl ihre aktuellen Schutzmaßnahmen als auch das bestehende Restrisiko einschätzen und bewerten. Der Autor hat beide Aussagen in Beziehung gesetzt. Das Ergebnis gibt Aufschluss darüber, welche Schutzmaßnahmen in den Unternehmen nach subjektiver Wahrnehmung effizient umgesetzt werden. Gleichzeitig lassen sich auch Defizite ausmachen und Handlungsempfehlungen ableiten.

IT-Sicherheit; IT-Sicherheitskonzept; Industriespionage; Cybercrime; Risikoanalyse; Schadensrisiko; Wirtschaftsunternehmen; Sicherheitsmaßnahme

ID-nummer: 20121019

Meier, Bernd Dieter

Sicherheit im Internet; Neue Herausforderungen für Kriminologie und Kriminalpolitik

MschrKrim - Monatsschrift für Kriminologie und Strafrechtsreform, 2012, 3, S. 184-204
mit LITVZ S.202-204

Ungeachtet der erheblichen Relevanz, die dem Internet für Wirtschaft, Verwaltung und die Gestaltung des Alltags zukommt, ist das kriminologische Interesse an der Internetkriminalität bislang nur gering. Der Autor greift den Befund auf und liefert einen Überblick über den gegenwärtigen Erkenntnisstand und die sich stellenden Fragen. In Anlehnung an die Cybercrime Convention des Europarats wird zwischen vier Erscheinungsformen der Internetkriminalität unterschieden: Angriffen auf die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen, Angriffen auf netzunabhängige Rechtsgüter, bei denen die IuK-Technologie als Tatmittel eingesetzt wird, über das Internet verbreiteten inhaltsbezogenen Straftaten und strafbewehrten Schutzrechtsverletzungen. Es wird versucht, eine Einschätzung zur Häufigkeit der jeweiligen Kriminalitätsformen, den dabei bewirkten Schäden und den jeweils maßgeblichen Risiko- und Schutzfaktoren zu liefern. Im Anschluss werden die Herausforderungen skizziert, die sich aus der Internetkriminalität für die Kriminologie, aber auch für die Kriminalpolitik ergeben.

Internet; Internetkriminalität; Erscheinungsform; Cybercrime; Hacking; Tatmittel; Angriffsobjekt; Sicherheitslage; Datensicherheit; IT-Sicherheit; Computerbetrug; Phishing; Urheberrechtsverletzung; Kriminologe; Kriminalpolitik

ID-nummer: 20120976

Wenner, Georg

Cyber-Sicherheit - Aufgabe des Staates; Cyberabwehr - Bekämpfung von digitalen Angriffen

Homeland Security, 2012, S. 25-27

Die Abwehr von Cyberattacken ist ein wesentlicher Teil der Cyber-Sicherheit (CS). Die kontinuierliche Entwicklung der Cyber-Sicherheitslage trägt zu einer regelmäßigen neuen Beurteilung bei. CS ist daher zentrale und gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft sowohl national als auch im internationalen Kontext. Ein wirksamer Schutz vor Angriffen ist realisierbar, wenn Gefährdungen im Internet sowie die eigene Gefährdungslage z. B. mittels Risikoanalyse bekannt sind. Adäquate präventive und reaktive Maßnahmen, die kontinuierlich zu aktualisieren. sind, unterstützen dabei.

Cybercrime; Abwehrmaßnahme; Sicherheitskonzept; Infrastruktur; IT-Sicherheit

ID-nummer: 20120975

Berberich, Ruthard; Kolb, Hans Joachim; Schmidt, Klaus Ehrenfried; Schönbohm, Arne

Information Fusion; Unabdingbar für Effizienz und Effektivität im proaktiven Kampf gegen Bedrohungen

Homeland Security, 2012, S. 20-24
mit 1 TAF

Ein breites Spektrum an Bedrohungen unterschiedlichster Art wirkt heute auf den Staat und die Gesellschaft, das zu beobachten, zu identifizieren und zu verfolgen ist. Die Angriffe, auch in asymmetrischen Szenarien, entwickeln sich situationsgemäß schnell und sind nur im geringen Umfang vorhersehbar.
Als Reaktion auf die Ereignisse des 09/11 wurden folgerichtig Einrichtungen zur Informationsaufbereitung (fusion center) geschaffen, um mittels pro-aktiver Informationsaufbereitung die Abwehr zu fördern. Der Begriff "information sharing" umschreibt die Notwendigkeit, Informationen und aufbereitete Ergebnisse (intelligence) auszutauschen und die Einschränkungen unangemessener Vertraulichkeit zu brechen.
In dem Beitrag werden gesicherte Konzepte, Prozesse und Expertenmeinungen vorgestellt, die insbesondere bei der Schaffung einer geeigneten Informationsgrundlage Führern sowie Entscheidern die notwendige Unterstützung liefern können.

Sicherheitslage; Bedrohung; Gefahrenanalyse; Informationserhebung; Informationsgewinnung; Informationsaustausch; Informationsverbund; Vernetzung; Wissensmanagement; Intelligence-Arbeit; Analyseverfahren; Polizeiliche Datenverarbeitung; Informationstechnologie

ID-nummer: 20120903

Pörksen, Bernhard; Detel, Hanne

Der digitale Pranger

Psychologie Heute, 2012, 8, S. 30-33
mit 3 TAF

Manchmal reicht ein einziger Klick, und E-Mails, Fotos, Handyvideos, SMS-Botschaften und Twitter-Meldungen geraten in die falschen Kanäle. So werden innerhalb kürzester Zeit Karrieren zerstört und Schicksale besiegelt. Daten im Netz lassen sich immer leichter durchsuchen, verknüpfen, kopieren und können sich plötzlich in Dokumente der Blamage verwandeln. Längst stehen nicht mehr nur Mächtige und Prominente am Pranger. Auch Ohnmächtige -und Unschuldige werden zum Opfer grausamer Spektakel, zu den Hassfiguren eines anonymen Cybermobs - einer aggressiven Form der Selbstjustiz, eine Hexenjagd in Zeiten moderner Medien.
In dem Beitrag fragen die Verfasser, welches Muster verbindet die vielen Geschichten von Aufklärung und Enthüllung einerseits, von Bloßstellung, Denunziation und Diffamierung andererseits? Gibt es Gemeinsamkeiten zwischen dem immensen Aufklärungspotenzial und dem digitalen Pranger? Und ist die Eigenmacht des Technischen ein Grund zur Klage, ein Indiz des Niedergangs und der Zerstörung? Oder sind wir au f dem Weg zu einer Gesellschaft totaler Transparenz - in der Diktatoren langfristig keine Chancen mehr haben und der Verlust des Privatlebens als Kollateralschaden in Kauf genommen werden muss?

Cyberspace; Internetplattform; Soziales Netzwerk; Digitaltechnik; Informationsaustausch; Mobbing; Denunziation; Anonymität; Kontrollverlust

ID-nummer: 20120974

Grundwald, Roman

Strategisch, umfassend und vernetzt; Die Bundesakademie für Sicherheitspolitik und der Begriff der vernetzten Sicherheit

Homeland Security, 2012, S. 17-19
mit 3 BILD

Die Bundesakademie für Sicherheitspolitik (BAKS) ist die höchste ressortübergreifende Weiterbildungseinrichtung des Bundes auf dem Gebiet der Sicherheitspolitik. Sie untersteht der Bundesregierung, genauer: dem Bundessicherheitsrat. Der wiederum ist ein Kabinettsausschuss, dem die Bundesminister der Verteidigung, des Auswärtigen, der Finanzen, des Innern, der Justiz, für Wirtschaft, für wirtschaftliche Zusammenarbeit und der Chef des Kanzleramts angehören; den Vorsitz führt die Bundeskanzlerin. Schon wegen dieser Unterstellung geht die BAKS in ihrem Verständnis von Sicherheitspolitik weit über die klassischen Ressorts Äußeres, Verteidigung und Inneres hinaus. Sie ist keine Einrichtung des Verteidigungsministeriums, dem sie administrativ angegliedert ist, sondern eine Einrichtung der Bundesregierung. Der Bundessicherheitsrat hat die BAKS beauftragt, bei gegenwärtigen und zukünftigen Führungskräften ein umfassendes Verständnis der langfristigen sicherheitspolitischen Interessen Deutschlands zu fördern. Dieses Spitzenpersonal soll möglichst breit aufgestellt sein und Länder- bzw. Bundesressorts ebenso umfassen wie Manager der Wirtschaft, Journalisten oder Wissenschaftler. Im Kern gilt es, Entscheidungsträger aus Verwaltung und öffentlichem Leben, durchaus auch international zusammen zu bringen und weiterzubilden. Hauptthema der Lehre ist das umfassende Verständnis von Sicherheitspolitik.

Bundesakademie für Sicherheitspolitik; Aufgabenbeschreibung; Sicherheitspolitik; Vernetzung; Fortbildung

ID-nummer: 20120914

Weiler, Julia von

ROBERT - Risktaking Online Behaviour Empowerment through Research and Training; Riskantes Internetverhalten - Handlungskompetenz durch Forschung und Aus- und Weiterbildung

Kinder- und Jugendschutz in Wissenschaft und Praxis - KJuG, 2012, 3, S. 86-88

Cyber-Grooming bezeichnet die Kontaktaufnahme über das Internet, mit der Erwachsene gezielt Mädchen und Jungen ansprechen, um z.B. pornographische Bilder und Filme zu erhalten oder sich mit ihnen zu treffen, um sie zu missbrauchen. Im Rahmen der ROBERT Studie sollten Erkenntnisse aus den Erfahrungen Jugendlicher mit Missbrauchsprozessen im Internet gewonnen und Faktoren ermittelt werden, die zur Gefährdung der Jugendlichen beitragen sowie solche, die sie vor einer Gefährdung schützen.
Hierzu wurden Betroffene im Alter von 12 bis 18 Jahren aus sieben Ländern Dänemark, Großbritannien, Schweden, Estland, Italien, Deutschland und Russland interviewt. Außerdem erfolgten Befragungen in sogenannten Fokus-Gruppen, zu denen auch mögliche vulnerable Gruppen gehörten: (Gay, Lesbian, Bisexual, Transsexuell, Intersexuell); Jugendliche, die in Institutionen leben; Jugendliche mit einer Behinderung; aber eben auch Jugendliche, die keiner als vulnerabel definierten Gruppe angehören.

Internetkriminalität; Soziales Netzwerk; Kontaktaufnahme; Missbrauchsgefahr; Sexueller Missbrauch; Jugendschutz; Kinderschutz; Medienkompetenz

ID-nummer: 20120886

Rössel, Torsten

Post-Stuxnet - Update 2012; Zur Lage der Cyber-Sicherheit in der Industrie

IT-Sicherheit - Management und Praxis, 2012, 3, S. 48-50
mit 3 BILD

Die Entdeckung des über das Internet verbreiteten Computervirus "Stuxnet" im Juni 2010 war ein Weckruf, der weltweit neben den staatlichen Institutionen mit Verantwortung für kritische Infrastrukturen vor allem die Betreiber industrieller Anlagen und die Hersteller von Automatisierungstechnik gleichermaßen wachgerüttelt und ihre Sensibilisierung für das Thema Industriesicherheit schlagartig erhöht hat. Der Autor betrachtet die Entwicklung seit diesem Schadensereignis bis 2012. Leitfragen sind: Haben sich die Prognosen von damals bewahrheitet? Wie ist die Lage und wie stellt man sich angemessen darauf ein?

Computervirus; Internet; Schadensrisiko; Industriebetrieb; Automatisierung; Herstellung; Anlagenbetreiber; Manipulationsprogramm; Funktionssicherheit; Wirkungsweise; Präventivmaßnahme; Unternehmenssicherheit; Infrastruktur; Sicherheitsplanung; Technologische Entwicklung; Wirksamkeit

ID-nummer: 20120877

Steffen, Wiebke

Neue Medien und Kriminalprävention: Überlegungen zur Notwendigkeit und Strategie

Die Polizei, 2012, 7, S. 192- 195
mit 11 QU

Die neuen - digitalen - Medien sind selbstverständlich geworden und aus dem Alltag nicht mehr wegzudenken. Sie bieten ohne jeden Zweifel viele positive Anwendungsmöglichkeiten, allerdings auch problematische Bereiche, Risiken und Gefahren bis hin zur Kriminalität. Grundsätzlich gibt es alle (Kriminalitäts-)Gefahren, die außerhalb des Internets bestehen, nun auch im Internet. Damit sind die neuen Medien auch eine Herausforderung für die Kriminalprävention und die präventiven Herausforderungen eigentlich nicht anders als in der analogen Welt. Diese Gleichsetzung von digitaler und analoger Welt ist allerdings nur dann möglich, wenn Einigkeit darüber besteht, dass für die digitale Welt grundsätzlich die Regeln der analogen Welt gelten, das Internet also kein rechts- und regelungsfreier Raum ist. Denn nur dann ist das entscheidende - konstitutive - Merkmal von Kriminalprävention gegeben: Ein klares Verständnis darüber zu haben, was "erlaubt - nicht erlaubt" bzw. "erwünscht - nicht erwünscht" ist. Wenn das vorhanden ist, dann kann Kriminalprävention auch in der digitalen Welt ihre beiden grundsätzlichen Strategien verfolgen: Menschen befähigen, durch Information und Wissensverbesserung - Stichwort: Medienkompetenz - sowie Schutzmechanismen schaffen, etwa durch (sicherheits-)technische und rechtliche Regelungen.

Neue Medien; Cybercrime; Internetplattform; Nutzungsverhalten; Suchtpotential; Medienkompetenz; Präventionsstrategie; Sicherheitstechnik; Rechtliche Grundlage

ID-nummer: 20120681

Müller, Birgit

Einsatzmöglichkeiten virtueller Vertrauenspersonen, Verdeckter Ermittler und nicht öffentlich ermittelnder Polizeibeamter; Rechtliche Rahmenbedingungen und Fallvarianten aus der Praxis

Kriminalistik, 2012, 5, S. 295-302
mit 4 TAF, 26 QU

Jeder vierte Deutsche ist Mitglied bei Facebook. Für die heute 15 bis 30-jährigen ist der Austausch in Sozialen Netzwerken eine Selbstverständlichkeit; hier wird sich kennengelernt und verabredet, werden Fotos geteilt und Musik empfohlen. Wenn sich das Leben immer mehr in der virtuellen Welt abspielt, dann spielt die virtuelle Welt auch für die Aufklärung von Straftaten und die Abwehr von Gefahren eine immer größere Rolle. Nicht nur der spezialisierte IuK-Sachbearbeiter muss sich mit dieser Welt beschäftigen, sondern jeder polizeiliche Ermittler kann jederzeit mit dem Phänomen "Facebook" konfrontiert werden.
Die Autorin stellt verschiedene Fälle aus dem polizeilichen Alltag vor, in denen sich die zuständigen Beamten mit diesem neuen Medium beschäftigen und bekannte polizeiliche Maßnahmen zur Strafverfolgung in die virtuelle Welt übersetzen mussten.

Ermittlungsarbeit; Ermittlungsmaßnahme; Verdeckte Ermittlung; Soziales Netzwerk; Internet; Kommunikationsmethode; Rechtsgrundlage; Beweisverwertungsverbot; Telekommunikation; Fallbearbeitung

ID-nummer: 20120634

Kronschnabl, Stephan; Weber, Stefan

IT-Sicherheitsstandards und Notfallmanagement; Ausgewählte Ergebnisse der "Grundschutz-Studie"

KES - Die Zeitschrift für Informations-Sicherheit, 2012, 2, S. 54-58
mit 6 TAF

Standards wie der IT-Grundschutz oder ISO/IEC 27001/2 sind in vielen Organisationen das Mittel der Wahl für die Sicherung der IT-Systeme. Die Autoren stellen auszugsweise Ergebnisse aus der nunmehr vollständig vorliegenden Studie "Informationssicherheit und Notfallmanagement: Trends 2012" vor, die sich auf die allgemeine Lage und Anwendung der Standards zum Sicherheits- und Notfallmanagement konzentrieren.

IT-Sicherheit; Informationssicherheit; Sicherheitsmanagement; Sicherheitsstandard; Sicherheitslage; Umfrageergebnis

ID-nummer: 20120387

Prondzinski, Peter von

IT-Ermittlungen/Soziale Netzwerke; Checkliste

DPolBl - Deutsches Polizeiblatt, 2012, 2, S. 31

Dokument hat keinen Textteil.

Checkliste; Cybercrime; Soziales Netzwerk; Globalisierung; Cyberspace; Computerkriminalität; Lagebild; Sicherheitsaufgabe

ID-nummer: 20120632

Fedtke, Stephen

EPIS 2.0: Fremde Fürsten; Anwendung des Transparency-Korruptionswahrnehmungsindex in der Risikoanalyse eines Outsourcings systemischer IT

KES - Die Zeitschrift für Informations-Sicherheit, 2012, 2, S. 11-17
mit 1 TAB, 5 BILD, 7 QU

Outsourcing, Offshoring und Cloud-Computing verschärfen nachhaltig die Lage um extreme Risikokonzentrationen in der IT, allem voran im Finanz- und Energiebereich sowie anderen kritischen Infrastrukturen. Umso schlimmer, wenn extrem-privilegierte IT-Mitarbeiter dabei in Ländern platziert sind, deren typische Anfälligkeit in puncto Korruption, Bestechlichkeit und Kriminalität sowie Missbrauch der Staatsmacht inakzeptable Risiken implizieren. Gerade in diesem Fall besteht gegenüber der Allgemeinheit eine besonders hohe Verpflichtung zur nachhaltigen Risikoanalyse durch die Aufsichtsorgane.
Die Risikoanalyse einer systemischen IT muss den Faktor "IT im Ausland" künftig in den Überlegungen intensiver einbinden - bei vollem Erhalt der politischen Korrektheit und Einhaltung des Allgemeinen Gleichbehandlungsgesetzes (AGG). Der Korruptionswahrnehmungsindex von Transparency International bietet eine solide Grundorientierung für eine ländervergleichende Bewertung der Eintrittswahrscheinlichkeit von Szenarien, die allesamt auf dem Missbrauch einer kraft Amtes verliehenen potenziell extrem hohen Machtumsetzungsgeschwindigkeit basieren. Die Hinzunahme weiterer Indizes erhöht nachhaltig das Niveau einer objektiven Bewertung.

IT-Sicherheit; Outsourcing; Cloud Computing; Dienstleistung; Ausland; Risikoanalyse; Mitarbeiterkriminalität; Risikomanagement; Korruption; Sicherheitsüberprüfung; Compliance

ID-nummer: 20120493

Wewer, Göttrik

Sicherheit in Zeiten der Unsicherheit, oder: Internet und E-Government

Verwaltung & Management, 2012, 2, S. 88-101
mit 1 TAF, 2 TAB, zahlr. QU

Die digitalen Angebote von Regierungen und Verwaltungen werden aus Sicht des Autors nicht in dem Ausmaß angenommen, wie das von den technischen Kapazitäten her möglich wäre. Einer der wichtigsten Gründe dafür sei, dass viele Menschen sich im Internet unsicher fühlten und manche dem Staat sogar mehr misstrauten als kommerziellen Datensammlern. Ein Gefühl der Sicherheit lasse sich nicht allein über Datenschutz und Datensicherheit erzeugen, sondern nur mit einem umfassenderen Ansatz, der Rechtssicherheit, Wahlfreiheiten, Transparenz und Beteiligung einschlösse. Die Diskussion darüber, was Sicherheit im digitalen Zeitalter bedeuten könne, habe noch kaum begonnen. Ohne einen gewissen Konsens, was Staat und Bürger im Internet wollen und was sie nicht wollen, würden jedoch weder E-Commerce noch E-Government eine wesentlich höhere Akzeptanz finden.

E-Government; Staatliches Handeln; Digitalisierung; Verwaltungshandeln; Internet; Vertrauen; Bürger; Akzeptanz; Online-Verfahren; Nutzungsverhalten; Sicherheitsgefühl; Elektronischer Rechtsverkehr; Einflussfaktor; IT-Sicherheit; Datenschutz; Rechtssicherheit; Bürgerbeteiligung; Transparenz; Forderungskatalog; Politische Kultur; Technikfolgenabschätzung

ID-nummer: 20120383

Angelkorte, Florian

Phishing - Identitätsdiebstahl beim Onlinebanking; Erster Zugang zu dem Themenkomplex Phishing unter rechtlichen und praktischen Aspekten

DPolBl - Deutsches Polizeiblatt, 2012, 2, S. 18-20
mit 17 QU

Das Schadenspotential im Bereich Cybercrime ist hoch. Insbesondere beim Phishing stieg laut dem Bundeslagebild Cybercrime 2010 des BKA die ungefähre Schadenssumme von 7,1 Mio. Euro in 2008 auf 21,2 Mio. Euro im Jahr 2010. Die Fallzahlen verdreifachten sich in demselben Zeitraum von 1.778 auf 5.331 Fälle. Die Zahlen belegen, dass es für jeden Polizeibeamten unerlässlich ist, sich mit den Grundlagen dieser Variante der Cybercrime auseinanderzusetzen. Für einen ersten Einstieg werden in diesem Beitrag die Funktionsweisen von Malware, typische Tatbegehungsweisen, strafrechtliche Bewertungen sowie mögliche Ermittlungsansätze dargestellt.

Phishing; Online-Banking; Identitätstäuschung; Cybercrime; Kriminalitätsentwicklung; Schadsoftware; Datenspionage; Modus operandi; Passwort; Geldtransfer; Datenmanipulation; Computervirus; Sicherheitsmaßnahme; Ermittlungsansatz

ID-nummer: 20120381

Tencz, Reinhard

Bekämpfung der Cyber-Kriminalität; IT-Ermittlungen - Reaktion der Polizei auf die Nutzung neuer IT-Technik durch Straftäter

DPolBl - Deutsches Polizeiblatt, 2012, 2, S. 11-14
mit 3 TAF

Die Anforderungen an die Polizei in der Bekämpfung der Cyberkriminalität steigen. Sie begegnet diesen Herausforderungen auf allen Ebenen mit innovativen Leistungen in allen Bereichen der polizeilichen Aufgabenwahrnehmung.
Die zunehmende taktische und technische Komplexität bei der Bekämpfung der Cyber-Kriminalität erfordert aber auch neue organisatorische Ansätze und Lösungen. Am Beispiel des Landeskriminalamtes Baden-Württemberg wird eine mögliche aufbauorganisatorische Lösung dargestellt, die mit Einrichtung der neuen Abteilung "Cyber-Kriminalität/ Digitale Spuren" seit 1.1.2012 in der Praxis umgesetzt wurde.

Cybercrime; Polizeiorganisation; Organisationsstruktur; Polizeiaufgabe; Bekämpfungskonzept; Bekämpfungsmaßnahme

ID-nummer: 20120380

Prondzinski, Peter von

Cybercrime - Lagebild, Entwicklungen und Trends; Die Angst im Internet Opfer einer Straftat zu werden, ist gewaltig. Die Realität sieht anders aus. Dennoch ein Grund zur Sorge!

DPolBl - Deutsches Polizeiblatt, 2012, 2, S. 6-11
mit 1 TAB, 2 TAF, 26 QU

Der Autor gibt einen Überblick zum Lagebild Cybercrime:
- Diebstahl digitaler Identitäten
- Phishing
- Carding
- Botnetze
- Digitale Erpressung
- Mobile Endgeräte, Smartphones
- Social Engineering
- Angriffe auf Industrieanlagen

einschl. der Fallzahlen und der bisherigen Entwicklung.
Die von den verschiedenen Facetten des Phänomens Cybercrime ausgehenden Gefahren sind in ihrem Ausmaß und in ihren Ausprägungen nur schwer zu bewerten. Cybercrime entwickelt sich dynamisch auf unverändert hohem Niveau. Das Ausspähen von Zugangsdaten im Bereich des Onlinebankings und digitaler Identitäten wurde intensiviert. Sicherheitsmaßnahmen werden sehr schnell überwunden. In den nächsten Jahren muss mit weiter steigenden Fallzahlen gerechnet werden, insbesondere vor dem Hintergrund, dass die Täter offenbar schon jetzt über das entsprechende technische Wissen verfügen und auch mobile Sicherungssysteme angreifen können.

Cybercrime; Lagebild; Lagebeurteilung; Lagedarstellung; Entwicklungstendenz; Schadensbild; Statistische Angaben

ID-nummer: 20120379

Prondzinski, Peter von

Cyberwelt und Cyberpolizei; Im world-wide-web hat sich eine virtuelle Welt entwickelt. Dort ist reale, nicht nur virtuelle Sicherheitsarbeit erforderlich!

DPolBl - Deutsches Polizeiblatt, 2012, 2, S. 2-5
mit 2 TAB, 5 TAF, 11 QU

Nach Bewertung des Autors lauern im Internet Gefahren wie in der realen Welt. Daher dürfe der Cyberspace kein rechts- und polizeifreier Raum sein. Eine weltweite Cyber-Sicherheitsstrategie stelle die Herausforderung des 21. Jahrhunderts dar. Der Autor geht der Frage nach, wo die Polizei dort ihren Platz finden wird. Es gelte dabei zu überprüfen, ob die bisherigen Erfahrungen, Taktiken und insbesondere Maßnahmenpakete ausreichend sind, die Sicherheit im Cyberspace zu gewährleisten. Da die Technik immer schneller fortschreite und das Internet von jedem PC, fast jedem Handy oder Tablet genutzt und bedient werden können, entwickele sich auch die Kriminalität weiter. Daher gelte es, mit Fortbildung inhaltlich und technisch (Ausstattung) auf Stand zu bleiben und sich zeitnah organisatorisch und technisch den neuen Anforderungen anzupassen. Hier wäre es sehr nützlich, wenn die Kreispolizeibehörden, die das Gros der Cyberermittlungen durchzuführen hätten, auf IT-Fachleute zurückgreifen könnten, die nicht zwangsläufig Polizeibeamte sein müssten. Die Polizeien des Bundes und der Länder würden aber scheitern, wenn die Sicherheitsstruktur des Internet nicht bald die notwendigen Eingriffsbefugnisse für die Polizei vorsieht. Die Polizei brauche geeignete Befugnisse. Diese müssten, juristisch und technisch, den Anforderungen an die weltweite Vernetzung Rechnung tragen.

Cybercrime; Gefahrenpotential; Sicherheitsstrategie; Polizeiliches Handeln; Internetkriminalität; Bekämpfungsstrategie; Kriminalitätsentwicklung; Technologische Entwicklung; Soziales Netzwerk; Cloud Computing; Ermittlungsbefugnis; Infrastruktur; Computerkriminalität; Sicherheitsarchitektur; Forderungskatalog

ID-nummer: 20120291

Caffier, Lorenz

Organisierte Kriminalitätsbekämpfung in Deutschland aus Sicht des IMK-Vorsitzenden; Grußwort des Ministers für Inneres und Sport von Mecklenburg-Vorpommern, Lorenz Caffier, im Rahmen der 6. Berliner Sicherheitsgespräche

Der Kriminalist, 2012, 3, S. 16-19
Rocker, Mafia, Geldwäscher - Deutschland fest im Griff der Organisierten Kriminalität!? - 6. Berliner Sicherheitsgespräche, Berlin; BR Deutschland, 2012 [23.01.]
mit 3 BILD

Da organisierte Kriminalität nicht als solche angezeigt würde, heißt es aus Sicht des Autors für die Strafverfolgungsbehörden, organisierte Kriminalität als solche zu erkennen. Deshalb sei ein offensiver Erkenntnisgewinn unabdingbar: Das Erkennen von Tatzusammenhängen, von potenziellen und tatsächlichen Tatverdächtigen, ihren personellen Verflechtungen und von verbrechensbegünstigender Logistik, Strukturen und Abläufen sei u.a. für die Aufdeckung und Verfolgung von organisierter Kriminalität entscheidend. Um wirksam gegen die zunehmend grenz- und deliktsübergreifend agierenden kriminellen Gruppierungen vorgehen zu können, habe die Bundesregierung mit einer Reihe von Staaten bilaterale Abkommen abgeschlossen. So sei zur Bekämpfung der organisierten Kriminalität nach Art der Mafia Mitte der 1990er Jahre eine deutsch-italienische Arbeitsgruppe eingerichtet worden, die sich speziell mit diesem Phänomen befasst. Auf europäischer Ebene unterstütze das europäische Polizeiamt Europol die Mitgliedstaaten bei der Bekämpfung der grenzüberschreitenden organisierten Kriminalität. Informationen der nationalen Sicherheitsbehörden sowie aus Kooperationsbeziehungen Europols mit Drittstaaten würden dort zusammengeführt, gespeichert und ausgewertet. Die nationalen Sicherheitsbehörden erhielten durch die Tätigkeit Europols wichtige Impulse für die Bekämpfung der organisierten Kriminalität, die sich allein auf dem Weg bilateraler Polizeizusammenarbeit nicht gewinnen ließen. Mit Eurojust hätte die Europäische Union im Jahr 2002 zudem eine Einrichtung gegründet, die bei der Verfolgung schwerer grenzüberschreitender und organisierter Kriminalität die Koordinierung der laufenden Ermittlungen und Strafverfolgungsmaßnahmen zwischen den zuständigen Justizbehörden der Mitgliedstaaten der Europäischen Union fördere und verbessere. Die Richtlinie des Europäischen Parlamentes und des Rates vom 15. März 2006 verpflichte zudem jeden Mitgliedsstaat, durch ihre Telekommunikationsgesellschaften Informationen über die Verbindungen ihrer Kunden aufzeichnen zu lassen und so für die Bekämpfung der organisierten Kriminalität nutzbar zu machen.

Organisierte Kriminalität; Bekämpfungsstrategie; Netzstrukturkriminalität; Organisierte Wirtschaftskriminalität; Cybercrime; Internationale polizeiliche Zusammenarbeit; Internationale Kriminalitätsbekämpfung; Justitielle Zusammenarbeit; Europäische Union; Bilaterales Abkommen; Europol; Telekommunikationsdaten; Vorratsdatenspeicherung; Kriminalpolitik; Forderungskatalog

ID-nummer: 20120311

Kaspersky, Natalya

Wie viel Freiheit kann das Internet vertragen?

IT-Sicherheit - Management und Praxis, 2012, 1, S. 14-15

Sollte das Internet stärker reglementiert werden? Diese Frage ist längst nicht mehr nur in Fachgremien verortet, sondern hat politisch mittlerweile auch alle großen Parteien erreicht. Jüngste internationale Datenpannen, von denen Millionen Personen betroffen sind, gehören unweigerlich zu den großen Problemen, die immer öfter auch die Nachrichten prägen.
Wenn man die Hintergründe der derzeitigen Lage verstehen will, muss erkannt werden, warum die Kriminalität im Netz bis zum heutigen Tag ein so immenses und scheinbar unaufhaltsames Wachstum zu verzeichnen hat. Warum reagiert die Gesetzgebung erst jetzt, wo die durch Online-Kriminalität verursachten Schäden in die Milliarden gehen und selbst öffentliche Einrichtungen nicht vor Hackerattacken sicher sind? Warum wurde das Potenzial der neuen Kriminellen so lange unterschätzt?
Mit diesen Fragen setzt sich die Verfasserin in dem Beitrag auseinander und fordert, dass die Gesetzgebung Unternehmen und öffentliche Organisationen dazu verpflichtet ihre Sicherheitsstandards auf höchstem Niveau zu halten und auch mit Daten, deren Verlust das Unternehmen nicht schädigt, vertraulich umzugehen.

Internetkriminalität; Freiheitsrecht; Internationale Kriminalität; Anonymität; Datenschutz; Datensicherheit; Sicherheitsstandard

ID-nummer: 20120292

Ziercke, Jörg

Organisierte Kriminalität - Lagedarstellung und -bewertung; Rocker, Mafia, Geldwäscher - Deutschland fest im Griff der OK?

Der Kriminalist, 2012, 3, S. 20-23
Rocker, Mafia, Geldwäscher - Deutschland fest im Griff der Organisierten Kriminalität!? - 6. Berliner Sicherheitsgespräche, Berlin; BR Deutschland, 2012 [23.01.]
mit 2 BILD, 3 QU

OK-Tätergruppen arbeiten konspirativ, international vernetzt und abgeschottet: Sie nutzen moderne Informations- und Kommunikationstechnologien und entwickeln permanent neue Geschäftsfelder und Vorgehensweisen. Für die Polizei bedeutet dies nach Bewertung des Autors, im Einklang und vernetzt mit den Partnern in der europäischen und internationalen Sicherheitsarchitektur neuen und komplexeren Erscheinungsformen der organisierten Kriminalität zu begegnen und das vorhandene Personal auf diese Herausforderung zu konzentrieren. Neue Kooperationsformen würden praktiziert werden müssen. Durch die Zusammenarbeit von Ermittlern aus zwei oder mehreren Staaten seien die Ermittlungsergebnisse jeweils in allen beteiligten Staaten unmittelbar und ohne komplizierte Rechtshilfeersuchen verwertbar. Die Aufmerksamkeit der Strafverfolgungsbehörden müsse hinsichtlich des Vorfelds der OK und im Bereich der OK-affinen Straftaten geschärft werden. Ein Lagebild Schwerstkriminalität bzw. strukturelle Kriminalität sei hierzu in der Lage. Es könne Kriminalitätsfelder erhellen, aus dem sich Handlungsbedarf ableiten und folglich der Ressourceneinsatz optimieren lasse. Für die Beweisführung sind die Telekommunikationsüberwachung (auch die Überwachung der Internet-Telefonie) und Ermittlungen mit Hilfe von Internet-Verbindungsdaten von wesentlicher Bedeutung. Die Wurzeln von OK aufzuklären, sei ohne Eindringen in die Kommunikationsstrukturen einer kriminellen Organisation nicht möglich. Das deutliche Missverhältnis zwischen den durch OK verursachten Schäden bzw. erzielten Gewinnen und den vorläufig gesicherten Vermögenswerten zu überwinden, sei ein weiteres vordringliches Anliegen. Auch die Bekämpfung der Geldwäsche müsse weiter verbessert werden.

Organisierte Kriminalität; Lagedarstellung; Deliktstruktur; Schwerkriminalität; Netzstrukturkriminalität; Bedrohungspotential; Bekämpfungsstrategie; Internationale Kriminalitätsbekämpfung; Verbrechensgewinn; Finanzermittlung; Vermögensabschöpfung; Kriminalpolitik; Forderungskatalog

ID-nummer: 20120290

Schulz, André

Rocker, Mafia, Geldwäscher - Deutschland fest im Griff der Organisierten Kriminalität!?

Der Kriminalist, 2012, 3, S. 13-15
Rocker, Mafia, Geldwäscher - Deutschland fest im Griff der Organisierten Kriminalität!? - 6. Berliner Sicherheitsgespräche, Berlin; BR Deutschland, 2012 [23.01.]
mit 3 BILD

In der Veranstaltungsreihe "Berliner Sicherheitsgespräche" befasst sich der Bund Deutscher Kriminalbeamter (BDK) mit den Problemfeldern, die einen direkten Einfluss auf die Sicherheitslage in Deutschland haben. Im Beitrag werden die wichtigsten Themenstellungen eines "Sicherheitsgesprächs" zur Organisierten Kriminalität (OK) zusammengefasst. Der Autor stellt fest, dass die Grenzen zur Bandenkriminalität und Schwerstkriminalität fließend sind. Rauschgifthandel und -schmuggel dominierten immer noch die OK-Welt, aber auch Geldwäsche, Schleusung illegaler Migranten und Menschenhandel, Waffenhandel sowie die Verschiebung von Kraftfahrzeugen und hochwertigen Waren. In den letzten Jahren sei aber die Bekämpfung der Wirtschafts-, Korruptions-, Internet- und Computerkriminalität immer bedeutsamer geworden. Dort hätten sich Strukturen der Organisierten Kriminalität breitgemacht. Gerade das Internet böte eine solche Vielfalt von Möglichkeiten als Tatmittel, dass gemeinsam agierende und organisiert handelnde Kriminelle in unterschiedlichen Rollenverteilungen mit gleichen oder auch wechselnden Tatvarianten in kürzester Zeit Millionengewinne erzielen können.

Organisierte Kriminalität; Deliktstruktur; Bedrohungspotential; Netzstrukturkriminalität; Wirtschaftskriminalität; Internetkriminalität; Bandenkriminalität; Rockerkriminalität; Mafia; Drogenhandel; Geldwäsche; Bekämpfungsstrategie; Vermögenseinziehung; Ermittlungsverfahren

ID-nummer: 20120285

Glitza, Klaus Henning

Synergien erschließen; Physischer und elektronischer Schutz von Kreditinstituten

Protector, 2012, 3, S. 16-17
mit 2 BILD

Wenn es um kriminelle Gefährdungen geht, stehen Kreditinstitute (Banken, Sparkassen und Kreditgenossenschaften) nach Bewertung des Autors ganz oben auf der Liste der Angriffsziele. Physisches Geld wecke ebenso wie sein elektronisches Pendant vielfältige Begehrlichkeiten und Energien doloser Natur. Nur ein Kreditinstitut, das sowohl physisch als auch elektronisch optimal geschützt sei, könne deshalb als sicher gelten. Doch dies sei ein Idealzustand, der sich real nur selten widerspiegele. Physische und elektronische Schutzansätze seien noch um Welten voneinander entfernt. Und es gebe nur wenige Brückenschläge, die synergetisch wirken. Beispiele für solche integrierten Schutzansätze werden in diesem Beitrag dargestellt.

Bankensicherheit; Sicherheitssystem; Integrationsmodell; Gebäudesicherheit; Elektronische Sicherung; Mechanische Sicherung; Geldautomat; Bargeld; IT-Sicherheit; Zugangskontrollsystem; Sicherheitsplanung

ID-nummer: 20120252

Girg, Wolfram

Strafe oder Chance? IT-Security-Audit

KES - Die Zeitschrift für Informations-Sicherheit, 2012, 1, S. 52-56
mit 1 TAF

Security-Audits sollten aus Sicht des Autors elementarer Bestandteil eines Informationssicherheitsmanagements sein - teils seien sie notwendig, um Compliance-Vorgaben zu erfüllen. Allerdings würden sie für alle Beteiligten immer auch zusätzlichen Aufwand bedeuten neben dem, was im Alltagsgeschäft "gerade brennt", und würden daher bisweilen eher als Strafe empfunden. Wie Audits zur Chance würden, aus der man effektiv einen Nutzen ziehen könnte, beschreibt der Autor.

IT-Sicherheit; Sicherheitsüberprüfung; Auditierung; Informationssicherheit; Compliance; Kontrollprozess; Planungsmethode; Projektmanagement; Qualitätssicherung; Schwachstellenanalyse; Risikoanalyse; Prioritätensetzung; Geschäftsablauf; Prozessoptimierung; Managementsystem

ID-nummer: 20120227

Robertz, Frank J.; Rüdiger, Thomas Gabriel

Die Hacktivisten von Anonymous; Der schmale Grat zwischen guter Absicht und Selbstjustiz

Kriminalistik, 2012, 2, S. 79-84
mit 1 BILD, 1 TAF

Noch Mitte der 1970er Jahre stand der Archetyp des Hackers weitgehend für einen enthusiastischen Computerexperten, der brillante Problemlösungen entwickelt und andere Menschen an seinem Wissen teilhaben lässt. Mit der Entwicklung mächtiger Werkzeuge entsteht jedoch unweigerlich auch das Bestreben einiger Menschen, diese Hilfsmittel zu ihrem eigenen Gewinn auszunutzen und sich dabei von bestehenden Gesetzen und den Bedürfnissen anderer nicht abhalten zu lassen. So verhielt es sich auch mit dem Internet und der illegalen Nutzung von Hacks. Einige Hacker nutzen ihre Fertigkeiten, um politische Ziele zu verfolgen. Ein solcher Hacker, der zu politischen Zwecken Webseiten manipuliert, in fremde Netze eindringt oder Computer-Schäden verursacht, wird als Hacktivist bezeichnet.
Anonymous bildet eine ganze Bewegung solcher Hacktivisten mit ähnlichen Zielen: Anonymous ist eine nicht-hierarchische, nicht-strukturierte Gruppierung, die versucht, mit den modernsten Mitteln des Internets gegen für sie unliebsame Institutionen, Entscheidungen, Gesetze und Gruppierungen vorzugehen. Die Vielfalt von Anonymous spiegelt sich dabei auch in ihren Zielen wieder, die von Facebook und dem FBI über die mexikanische Drogenmafia bis zu Despoten im Nahen Osten reicht.

Informationsfreiheit; Hacker; Anonymität; Kommunikationsform; Motivation; Zielvorstellung; Selbstverständnis; Globalisierung

ID-nummer: 20120192

Hausö, Wendy

Viktimierungsrisiko durch Phishing - ausgewählte Studienergebnisse

Der Kriminalist, 2012, 2, S. 26-29
mit 2 BILD, 1 TAB 10 QU

Das Phishing zählt neben dem Missbrauch ausgespähter Kreditkartendaten und der missbräuchlichen Nutzung von Zugangsdaten zu Telefonanschlüssen zu den Tathandlungen des Identitätsdiebstahls. Beim Diebstahl digitaler Identitäten geht es vornehmlich darum, an verschiedene persönliche Daten und Informationen von Nutzern zu kommen, diese abzugreifen und missbräuchlich zu verwenden. Von Interesse für die Täter sind Zugangs- und Benutzerdaten zu verschiedenen Kontoarten (Online-Warenhäuser und Auktionsplattformen, Soziale Netzwerke, E-Mail-Konten, Benutzerkonten bei Dienstleistungsanbietern sowie Online-Bankdienste usw.), aber auch Kreditkartendaten wie Nummern, Gültigkeitsdauer und Sicherheitscodes. Mit den ausgespähten Daten können die Täter die verschiedenen Konten zu eigenen Zwecken missbrauchen, indem sie im Namen des Geschädigten den Konten entsprechende Geschäfte tätigen, sich den "Gewinn" jedoch selber zuleiten. Verschiedene Forschungsergebnisse deuten nach Bewertung der Autorin darauf hin, dass bei der effizienten Verhinderung von Phishing und anderen luK-Delikten das Schaffen eines Risiko- und Sicherheitsbewusstseins der Internetnutzer aller Altersgruppen ausschlaggebend ist. Um das Risikobewusstsein zu schulen und die Medienkompetenz im Bereich der Internetnutzung zu erhöhen, seien beispielsweise öffentliche Aufklärungskampagnen z. B. in Form von zielgruppengerechten Kurzfilmen, Broschüren oder Plakaten denkbar, die über Verhaltensvorbilder Interesse an der Thematik wecken, Bezüge zur eigenen Sicherheit herstellen und zur Nachahmung alternativer Verhaltensweisen beim Surfen im Internet aufrufen.

Phishing; Opferrisiko; Datenspionage; Identitätstäuschung; Passwort; Benutzeridentifizierung; Viktimisierung; Internetkriminalität; Privatperson; Sicherheitsrisiko; Forschungsergebnis; Empirische Untersuchung; E-Commerce; Online-Banking; Sicherheitsbewusstsein; Medienkompetenz; Präventivmaßnahme

ID-nummer: 20120226

Gatzke, Wolfgang

Kriminalität im Netz; Eine zentrale Herausforderung für die Polizei

Kriminalistik, 2012, 2, S. 75-78
mit 13 QU

Die deutsche Innenministerkonferenz hat am 27./28.5.2010 in ihrem Beschluss zur "Strategie zur Bekämpfung der luK-Kriminalität" festgestellt, "dass die von der luK-Kriminalität ausgehende Bedrohung derzeit eine der wesentlichen Herausforderungen im Bereich der Verbrechensbekämpfung und Prävention darstellt". Sie hat weiter ausgeführt, dass es "bei der Bekämpfung der luK-Kriminalität umfassender Anstrengungen sowohl auf Seiten der Sicherheits- und Strafverfolgungsbehörden, als auch bei allen anderen staatlichen und privaten Institutionen" bedürfe. Aus Sicht des Autors liegt es auf der Hand, dass die Kriminalität im Netz eine der zentralen Herausforderungen für die Polizei ist. Dieser Beitrag geht daher folgenden Fragen nach: Wie ist die Polizei des Landes Nordrhein-Westfalen darauf vorbereitet? Welche Phänomene spielen dabei eine Rolle? Welche Schwierigkeiten haben die Strafverfolgungsbehörden bei der Verfolgung dieser Kriminalität? Welche Erfolge? Warum sollte ein Unternehmen bei Angriffen aus dem Netz die Polizei einzuschalten?

Internetkriminalität; Ermittlungsstrategie; Cybercrime; Forensik; Fachdienststelle; Unterstützungseinsatz; Qualifikation; Informationsaustausch; Lagebilderstellung; Gefährdungseinschätzung; Nordrhein-Westfalen

ID-nummer: 20120197

Rüdiger, Thomas Gabriel

Cybergrooming in virtuellen Welten - Chancen für Sexualtäter?

Deutsche Polizei, 2012, 2, S. 29-31, 33-35
mit 5 TAF

Cybergrooming ist ein Kunstwort. Wörtlich könnte man es mit "Internetstreicheln" übersetzen. Es steht inhaltlich für die Planungs- und Anbahnungsphase, die einem sexuellen Übergriff durch eine Person auf eine/n Minderjährige/n - üblicherweise ein Kind - vorausgeht und diesen einleitet. Grooming muss dabei nicht zwangsläufig in einem direkten körperlichen Missbrauch enden, vielmehr erfasst man hierunter bereits das Einwirken mit dem Ziel Aufnahmen von sexuell geprägten Fotos/Videos von Kindern z.B. über eine im Notebook oder am Desktop PC vorhandenen Kamera (Webcam) zu erlangen oder eine eindeutige Kommunikation mit sexuellem Inhalt zu führen.
Seit einigen Jahren zeigt sich, dass Täter auch gerne insbesondere von Minderjährigen genutzte virtuelle Welten - wie Onlinespiele an Computern und Spielekonsolen - aufsuchen und gezielt Chat-Foren nutzen, die auch interaktive Spiele beinhalten. Der Autor bezieht sich daher in seinen Ausführungen beispielhaft auf die bei Minderjährigen sehr beliebte Online-Welt "Habbo Hotel".

Cybercrime; Internetforum; Videospiel; Computerspiel; Sexuelle Handlung; Sexueller Missbrauch; Kontaktaufnahme; Täterverhalten; Modus operandi; Jugendschutz; Präventionskonzept

ID-nummer: 20111071

Hange, Michael

Lebensadern schützen; Nationales Cyber-Abwehrzentrum nimmt Arbeit auf

W&S - Das Sicherheitsmagazin, 2011, 5-6, S. 16-17
mit 1 BILD

Internet-Kriminalität ist mittlerweile allgegenwärtig. Dies betrifft alle Nutzer von IT und Internet. So sind Unternehmen und staatliche Stellen zunehmend dem Risiko der Cyber-Sabotage und des Datendiebstahls ausgesetzt. Zudem werden private PCs unbemerkt manipuliert, um sie zu "Botnetzen" zusammenzuschließen und beispielsweise zum massenhaften Versenden ungewünschter E-Mails zu missbrauchen. Besonderen Schutzbedarf besitzen die kritischen Infrastrukturen, deren Ausfall dramatische Folgen für unser Gemeinwesen hätte - etwa die Steuerung der Energieversorgung oder der geregelte Ablauf von Transport und Verkehr.
Um diese Einrichtungen vor Angriffen aus dem Cyber-Raum zu schützen, ist in Fortführung bereits bestehender Einrichtungen und Maßnahmen die Cyber-Sicherheitsstrategie für Deutschland entwickelt worden.
Das Nationale Cyber-Abwehrzentrum ist ein wesentlicher Bereich der IT-Sicherheitsstrategie. Als Informationsdrehscheibe deutscher Sicherheitsstellen auf Bundesebene trägt es dazu bei, umfassende Lagebilder zu erstellen und Schutz- sowie Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle besser zu koordinieren. Das Cyber-Abwehrzentrum bildet eine Informationsplattform mit klar definierten Kontakt- und Informationswegen sowie festen Ansprechpartner.

IT-Sicherheit; Cybercrime; Sicherheitsstrategie; Abwehrmaßnahme; Sicherheitsbehörde; Sicherheitsmaßnahme; Kritische Infrastruktur

ID-nummer: 20111079

Neufert, Caroline

Initiativen zum Schutz vor Angriffen; Cyber-Sicherheit in Deutschland

IT-Sicherheit - Management und Praxis, 2011, 5, S. 46-47
mit 1 TAF

Jeder Internet-Nutzer sollte Maßnahmen zur Cyber-Sicherheit ergreifen, um seine Daten gegen Angriffe zu schützen. Was unternimmt die Regierung, um Attacken auf Bürger und öffentliche Systeme abzuwehren? Sie baut ein Cyber-Abwehrzentrum. Wie ist die neue Behörde organisiert? Welche Funktionen umfasst sie? Wie ist sie in das nationale Konzept zum Schutz vor Cyber-Angriffen eingebunden? Diesen und weiteren Fragen geht der folgende Beitrag nach.

IT-Sicherheit; IT-Sicherheitskonzept; Cybercrime; Abwehrmaßnahme

ID-nummer: 20111217

Zelin, Aaron Y.

Neues aus Cyber-Dschihadistan; Global oder lokal handeln - das ist die Debatte seit 9/11; Internationale Presse

Internationale Politik, 2011, 5, S. 130-133
mit 1 BILD

Zehn Jahre sind seit den Anschlägen auf das World Trade Center in New York und das Pentagon in Washington vergangen. In diesem Jahrzehnt hat der globale Cyber-Dschihadismus unter Aktivisten mindestens die Bedeutung erlangt, die militärische Aktionen haben. Entgegen der landläufigen Meinung aber verhält man sich in den Foren keineswegs stromlinienförmig. Die Diskussionen unter Aktivisten selbst oder über wichtige Botschaften geistlicher und politischer Autoritäten verliefen im Gegenteil zuweilen so harsch, dass die Foren vorübergehend geschlossen wurden.
Für eine ernsthafte Fragmentierung der Bewegung aber sind die Differenzen nicht groß genug, zumal sich nach einer Weile meist wieder eine generelle Linie herausbildet.
Und man ist sich einig: Der globale Dschihad ist nicht zu Ende.

Islamischer Fundamentalismus; Islamische Gruppierung; Djihadismus; Al Quaeda; Internetforum; Cyberspace; Ideologie

ID-nummer: 20111077

Klein, Hermann

Gut getarnt ins Netzwerk; Wie bedrohlich sind Advanced Evasion Techniques?

IT-Sicherheit - Management und Praxis, 2011, 5, S. 20, 22
mit 1 BILD, 1 TAF

Advanced Evasion Techniques (AETs) stellen Netzwerksicherheitssysteme vor neue Herausforderungen: AETs verändern und kombinieren Methoden zur Tarnung eines Angriffs oder Schadcodes. Dadurch können sie Attacken - von nahezu allen Netzwerksicherheitslösungen unbemerkt - ins Netzwerk schleusen. Die besondere Gefahr sind die fast unendlichen Kombinationsmöglichkeiten. Es gibt nach aktuellen Schätzungen etwa 2 hoch 180 verschiedene Varianten, mit denen Hacker einen Angriff tarnen können. Bislang bewährte Schutzmechanismen von Intrusion Prevention Systemen oder Firewalls sind damit vollkommen überfordert und greifen nicht mehr. Evasion-Techniken sind eine bekannte Methode von Hackern, Sicherheitslösungen auszutricksen. Sie tarnen oder verändern Cyber-Attacken derart, dass Sicherheitssysteme sie nicht erkennen und nicht blockieren.

Netzwerk; Hacking; Angriff; Schadsoftware; Sicherheitsdefizit; Sicherheitsleistung; Sicherheitssystem

ID-nummer: 20120137

Voncken, Guy

Cyberforensik made in Luxemburg

Schweizer Kriminalistikjournal, 2011, 15, S. 5-6
mit 2 BILD, 4 QU

Die "Section Nouvelles Technologies" ist die Abteilung für Computerforensik der Luxemburger Polizei. Auch wenn sich der kleine Betrieb in puncto Mannstärke (Zusammensetzung der Mannschaft: 3 Polizisten, 4 Ingenieure und 4 Computer-Fachkräfte) nicht mit dem Ausland messen kann, so gilt es dennoch die gleichen Aufgaben zu meistern. Dabei spielen Eigenentwicklungen eine nicht ganz unbedeutende Rolle.

Polizei; Luxemburg; Computerkriminalität; Cybercrime; Ermittlungsarbeit

ID-nummer: 20111326

Henzler, Peter

Zeitreise zur phänomenologischen und strukturellen Entwicklung der Organisierten Kriminalität und deren Bekämpfung in Deutschland

BKA - elektronische Veröffentlichung, 2011, 19 S.
Organisierte Kriminalität [Fachsymposium], Wiesbaden; BR Deutschland, 2011 [28.09.]
mit 1 QU

Beginnend Ende der 1960er Jahre mit der von den USA angestoßenen Auseinandersetzung mit dem Phänomen Organisierte Kriminalität (OK), über die Arbeiten an einer Definition für Deutschland, der Schaffung des spezifischen rechtlichen Handlungsrahmens mit dem Gesetz zur Bekämpfung der Organisierten Kriminalität (OrgKG) und der Geldwäschegesetzgebung, der Abfassung der Eltviller Empfehlungen bis zu den Vereinbarungen, Abkommen und Rechtsregelungen in der EU sowie auf der Ebene der Vereinten Nationen sind über die Jahre eine Reihe rechtlicher und kriminalstrategischer Regelungen und Leitlinien zur Bekämpfung der Organisierten Kriminalität entstanden. Besondere Bedeutung für die polizeiliche Umsetzungs- und Gestaltungsebene misst der Autor dabei den Eltviller Empfehlungen zu. Diese wurden 1999 von der Kommission Organisierte Kriminalität der AG Kripo und damit von den damals höchsten Fachverantwortlichen für die OK-Bekämpfung aus Bund und Ländern erarbeitet und niedergelegt und beschrieben basierend auf der Essenz jahrelanger Erfahrungen mit dem Phänomen diskutierte und konsolidierte Grundfunktionalitäten und Grundanforderungen an eine wirkungsvolle OK-Bekämpfung. Hierzu zählten beispielhaft die internationale Zusammenarbeit, die verfahrensintegrierten Finanzermittlungen und die Vermögensabschöpfung, die Fähigkeit, Straftaten im und unter Nutzung des Internet begegnen zu können sowie angesichts der Komplexität von OK-Verfahren die Einbindung von Experten und eine enge Abstimmung mit den Staatsanwaltschaften. In 2010 und 2011 wurden die Empfehlungen seitens der AG Kripo und der KOK einer Revision unterzogen, um sicherzustellen, dass sie angesichts der aktuellen Ausprägungen der OK weiterhin die für ihre Bekämpfung maßgebliche road map in taktisch-methodischer, technischer, personeller und organisatorischer Hinsicht darstellen. Die Arbeiten führten zu einigen wenigen Ergänzungen, die der Fortentwicklung, etwa hinsichtlich der Verwendung des Internets und der vermehrten Einbeziehung Privater, geschuldet waren, ansonsten erwiesen sich die Eltviller Empfehlungen aber aus Sicht des Autors als nach wie vor robuste Leitlinie zur Bekämpfung der OK. Von daher könne von Konstanten einer wirkungsvollen OK-Bekämpfung gesprochen werden, die in diesem Beitrag an ausgewählten Beispielen hinsichtlich ihrer aktuellen Ausprägungen und ihrer Fortentwicklung mit Blick auf heute schon erkennbare Entwicklungen beleuchtet werden.

Organisierte Kriminalität; Deliktstruktur; Bekämpfungsstrategie; Internationale Kriminalitätsbekämpfung; Ermittlungsführung; Organisierte Wirtschaftskriminalität; Geldwäsche; Internetkriminalität; Polizeiliches Handeln; Leitlinie; AG Kripo; EU-Richtlinie; Internationales Abkommen; Historische Entwicklung

ID-nummer: 20111462

Achten, Oliver M.; Pohlmann, Norbert

Mit Sicherheit mobil; Lagebild zur Bedrohung der Unternehmenssicherheit durch Smartphones & Co.

IT-Sicherheit - Management und Praxis, 2011, 6, S. 57-59
mit 1 BILD

Die Verbreitung von mobilen Geräten und die Nutzung des Mobilfunknetzes als Internetzugang schreiten schnell voran. Nach einer Studie des Marktforschungsunternehmens Gartner werden 2013 mehr als die Hälfte der Internetnutzer auch mit mobilen Geräten über Mobilfunknetze ins Internet gehen. Um auf die technischen Fortschritte von Smartphones und Tablet-PCs zu reagieren, ist es aus Sicht der Autoren zwingend notwendig, die einst für Laptops definierten Sicherheitsrichtlinien anzupassen und gegebenenfalls neue zu erstellen. Dieser Beitrag beschreibt, welche Gefahren aktuell von Smartphones und Tablet-PCs ausgehen, welche Lösungsansätze die Basis für ein hohes Sicherheitsniveau bilden und welche Probleme es bei der Realisierung gibt.

Mobiltelefon; Datenkommunikation; Unternehmenssicherheit; Mobilfunk; Internet; Sicherheitsrisiko; Geräteausstattung; Mitarbeiter; Private Nutzung; IT-Sicherheit; Vertraulichkeit; Schutzziel; Infrastruktur; Computerspionage; Sicherheitsrichtlinie

ID-nummer: 20111400

Irnich, Frank

Statistik versus Cybercrime; Bessere Betrugserkennung durch Advanced Analytics

KES - Die Zeitschrift für Informations-Sicherheit, 2011, 6, S. 66-68
mit 1 BILD

Zu den primären Zielen moderner Betrügereien zählen Finanzdienstleister, Versicherungen und Telekommunikationsunternehmen. Aber auch andere Branchen sind gefährdet: Entdeckt jemand mit genug krimineller Energie eine Betrugsoption in einem Unternehmen, so wird er diese auch ausnutzen. Gerade automatisierte Vorgänge, die keine menschliche Intelligenz involvieren, stellen hierbei ein besonderes Risiko dar - durch riesige Mengen automatisierter Transaktionen, die täglich vonstatten gehen, mangelt es niemals an anfälligen Stellen.
Gleichzeitig stellen die zunehmende Geschwindigkeit und Anzahl elektronischer Transaktionen, das massive Volumen zu untersuchender Daten, technische Einschränkungen sowie ein schier unendlicher Einfallsreichtum der Cyberkriminellen die Betrugsabwehr in Unternehmen vor immer größere Herausforderungen - klassische Ansätze zur Betrugserkennung stoßen hier inzwischen an ihre Grenzen. Hier können so genannte Advanced Analytics helfen.
In dem Beitrag werden die Leistungsmerkmale solcher Analysemodelle im Hinblick auf Betrugserkennung und -prävention dargestellt.

Betrug; Datenanalyse; Erkennungsmethode; Transaktionsanalyse; Analyseverfahren

ID-nummer: 20110175

Treude, Daniela

Möglichkeiten deutscher Strafverfolgungsbehörden bei der Bekämpfung des Skimmings

Der Kriminalist, 2011, 3, S. 7-12
mit 9 BILD, 2 TAB, 7 QU

Das Thema Skimming ist in den letzten Jahren verstärkt in den Fokus der Öffentlichkeit gerückt. Die Zahl manipulierter Automaten steigt, es gibt immer mehr Geschädigte.
Die Kreditwirtschaft reagiert mit präventiven Veränderungen an Geldautomaten und der Einführung des Chips auf Zahlungskarten. Welche Möglichkeiten haben die deutschen Strafverfolgungsbehörden bei der Bekämpfung der international organisierten Zahlungskartenkriminalität, wo sind die Grenzen und wie sieht die Zusammenarbeit mit anderen Staaten aus?

Geldkartenmissbrauch; Geldautomat; Kreditkartenmissbrauch; Tatbestand; Ermittlungsansatz; Kriminelle Organisation; Rumänien; Rechtshilfe; Strafverfolgungsmaßnahme; Internationale polizeiliche Zusammenarbeit

ID-nummer: 20110178

Temme, Olaf

Das Verhältnis der Bundeswehr zur Polizei unter besonderer Berücksichtigung der Diskussion über eine zukünftige Sicherheitsarchitektur

Der Kriminalist, 2011, 3, S. 25-30
mit 4 BILD, 24 QU

Neue Bedrohungsformen der internationalen Sicherheit sind nach der asymmetrischen Kriegsführung die Piraterie und die Proliferation von Massenvernichtungswaffen. Technologische Innovation und die Digitalisierung der Welt revolutionieren die Kampftechnik. Die Innovationen der Cyberwelt steigern das Risiko möglicher Konflikte und erfordern neue Abwehrmaßnahmen. Das Konzept der vernetzten Sicherheit, auch vor dem Hintergrund möglicher zukünftiger Konflikte, bleibt richtungsweisend für die gesamtstaatliche Sicherheitsvorsorge. Konflikte und Krisen muss vorbeugend begegnet werden, um die Auswirkungen auf Deutschland auf Distanz zu halten. Ein effektives Zusammenwirken der zivilen, militärischen, nationalen und internationalen Akteure ist gefordert. Neue Sicherheitsarchitektur muss bedeuten, dass das alte System der Aufgabendifferenzierung in ein neues System der Erfüllung gemeinsamer Aufgaben überführt wird, die von Polizei, Nachrichtendiensten, Bundeswehr, Katastrophenschutz abgestimmt werden. In dem Beitrag stellt der Autor eine interdisziplinäre Betrachtung von Bundeswehr und Polizei an.

Sicherheitsarchitektur; Sicherheitspolitik; Sicherheitslage; Bundeswehr; Militäreinsatz; Polizeiaufgabe; Aufgabenabgrenzung; Aufgabenstellung; Internationale Sicherheit; Auslandseinsatz; Zuständigkeitsregelung; Unterstützungseinsatz; Trennungsgebot

ID-nummer: 20110387

Spogahn, Nikolai; Pohlmann, Norbert

In der Cloud, aber nicht anonym! Googles Cloud-Angebot - Wie wertvoll ist uns der Datenschutz?

IT-Sicherheit - Management und Praxis, 2011, 2, S. 48-51; 3, S. 56-57
mit 3 TAF

Google, bekannt durch seine gleichnamige Suchmaschine, ist in fast allen Sparten tätig und bietet im Internet über einhundert verschiedene Dienste an. Dazu zählen Betriebssysteme, Bürosoftware, ein Web-Browser und diverse Plattformen für Kommunikation, Kollaboration, Multimedia, Organisation und Softwareentwicklung sowie Technologien für das Einstellen und Finden von Inhalten. Auch beim Cloud Computing setzt Google Akzente und wirkt beispielsweise mit dem eigenen Betriebssystem "Chrome OS" als Cloud-Client wie ein Innovationsmotor. Im Cloud Computing-Bereich "Software as a Service" (hier werden Anwendungsprogamme bei einem externen Dienstleister betrieben und vom Kunden als Online-Dienst genutzt) spielt Google mit seinen vielen Diensten eine wichtige Rolle. Außerdem mischt Google mit der "App Engine" beim "Platform as a Service"-Angebot (Bereitstellen einer virtuellen Computerplattform in der Cloud für Web-Anwendungsentwickler) mit. Der erste Teil dieses Beitrags befasst sich mit dem Geschäftsmodell von Google, den Google-Applikationen und Datenschutzrisiken aus Nutzer- und Unternehmensperspektive. Im zweiten Teil wird die Frage behandelt, wie das Sammeln und Verknüpfen von persönlichen Daten von Internet-Nutzern bei Google reglementiert werden kann.

Cloud Computing; Internet; Auftragsdatenverarbeitung; Anbieter; Outsourcing; Wirtschaftsunternehmen; Datenfernverarbeitung; Dienstleistung; Online-Verfahren; Software; Netzwerk; Risikofaktor; Computertechnologie; Datenkommunikation; Protokollierung; Personendaten; Datenweitergabe; IT-Sicherheit; Datenschutz

ID-nummer: 20110182

Glitza, Klaus Henning

Digitale Strumpfmasken; Bedrohungen für Finanzinstituten in einer vernetzten Welt

Protector, 2011, 3, S. 14-15
mit 1 BILD

Kaum ein Wirtschaftszweig ist so intensiv von IT-Risiken und internetbasierten Angriffen betroffen wie die Branche der Kreditinstitute. Für Banken und Sparkassen sind die Prämissen sichere und stabile IT-Prozesse, Vertraulichkeit von Kundendaten und gesicherte Verfügbarkeit von Leistungen eine existenzielle Frage.
Dabei haben die Kreditinstitute mit mindestens vier Herausforderungen zu kämpfen, und zwar: den generell wachsenden Bedrohungen im IT-Bereich, der massiv zunehmenden Vernetzung (innerhalb des Instituts, aber auch zu anderen Unternehmen und Kunden, zum Beispiel durch Electronic Banking), der Schwachstelle Mensch und dem Risikobild Outsourcing.

IT-Sicherheit; Kreditinstitut; Bankensicherheit; Risikoanalyse; Online-Banking; Sicherheitsbewusstsein

ID-nummer: 20111098

Gassen, Jan; Tölle, Jens

Botnetze - nur mit Mühe zu stoppen; Ungewollte Fernsteuerung von Unternehmensrechnern

WIK - Zeitschrift für die Sicherheit der Wirtschaft, 2011, 5, S. 30-32
mit 1 TAB

Botnetze bedienen sich einer speziellen Form von Schadprogrammen. Diese so genannten Bots - die in der Lage sind, selbstständig sich wiederholende Aufgaben abarbeiten zu können - werden dabei über einen versteckten Kommunikationskanal ferngesteuert. Bei diesem Kommunikationskanal handelt es sich um eine Internetverbindung, die unbemerkt von den einzelnen Bots aufgebaut wird. Als Teil eines Botnetzes wird der gekaperte Arbeitsplatzrechner zum Zombie. Neben den eigentlichen Aufgaben stiehlt er unbemerkt vertrauliche Informationen, versendet Spam, startet DistributedDenial-of-Service-Attacken oder generiert Phishing-Seiten.
Über die Betreiber der Botnetze sowie deren Herkunft ist oft nur wenig bekannt. Hierbei handelt es sich sowohl um Einzeltäter als auch um Mitglieder organisierter Kriminalität. In einzelnen Fällen gelingt es Strafverfolgungsbehörden die Betreiber eines Botnetzes zu ermitteln, woraus sich jedoch keine allgemeinen geographischen Rückschlüsse ziehen lassen.
In dem Aufsatz wird folgenden Fragen nachgegangen: Wie kann es sein, dass auch Rechner in eigentlich gut geschützten Unternehmen und Behörden Teil von Botnetzen werden? Warum sind sie so schwer zu entdecken? Und vor allem: Lässt sich das eigene Netz wieder säubern?

Unternehmenssicherheit; Hacking; Schadsoftware; Spam-E-mail; Computersabotage; Datendiebstahl; Computervirus

ID-nummer: 20111263

Siller, Helmut

Computerkriminalität

Kriminalistik, 2011, 11, S. 712-717
mit 34 QU

In den vergangenen Jahren haben sich Tat- und Tätertypologien stark und rasch verändert: Täter nutzen zunehmend modernste Technik, neuartige Kriminalitätsphänomene ersetzen immer mehr klassische Deliktformen, die einzelnen Delikte werden zudem immer komplexer. Die Bandbreite der so entstandenen Deliktarten reicht von Internetbetrug über technisch anspruchsvolle Spezialdelikte wie das Eindringen in Computersysteme bis zu Angriffen auf staatliche Infrastrukturen im Cyberterrorismus.
Mit der zunehmenden Nutzung des Internets wächst auch die Kriminalität auf diesem Sektor. Im ersten Halbjahr 2008 gab es 1118 Anzeigen, im gleichen Zeitraum des Vorjahres 2020 und von Jänner bis Juni 2011 bereits 2229. Hacking-Delikte: 105, aber bei hoher Dunkelziffer.
Der Autor untersucht das Kriminalitätsphänomen hauptsächlich an den Rechtsgrundlagen und statistischen Zahlen Österreichs.

Computerkriminalität; Deliktart; Statistische Angaben; Phishing; Hacking; Cybercrime; Rechtsgrundlage; Bekämpfungsmaßnahme; Präventivmaßnahme; Österreich

ID-nummer: 20111126

Henrichs, Axel

Ermittlungen im Internet; Zugriff auf öffentlich zugängliche oder nicht öffentlich zugängliche Informationen?

Kriminalistik, 2011, 10, S. 622-627
mit 2 TAB, LITVZ S. 627

Das Internet kann als ein virtueller Raum betrachtet werden, in dem Menschen sich u.a. informieren und miteinander in Kontakt treten. Insoweit finden sich im Netz Informationen allgemeiner Art sowie Inhalte bzw. nähere Umstände von Kommunikation. Die Möglichkeiten im Internet haben sich mit der sog. Generation Web 2.0 erheblich ausgeweitet, die Interaktion der Nutzer nimmt stetig zu. Die rechtliche Einordnung staatlicher Maßnahmen im Netz hängt insbesondere von der Zugänglichkeit dieser Daten ab. Je weiter der Kreis der tatsächlichen oder möglichen Rezipienten einer Information ausfällt, desto geringer stellt sich der (verfassungs-)rechtliche Schutz vor polizeilicher Datenverarbeitung dar. In diesem Beitrag wird die Fragestellung untersucht, wann vom Begriff der öffentlichen Zugänglichkeit von Daten ausgegangen werden kann bzw. wann (bei welcher Nutzeranzahl und bei welchen Zugangskriterien) diese Öffentlichkeitssphäre (z.B. bei einer geschlossenen Gruppe) nicht mehr gegeben ist. Zudem wird herausgestellt, welche rechtlichen Konsequenzen dies für die polizeilichen Ermittlungen im Internet nach sich zieht.

Internet; Internetkriminalität; Datenzugang; Öffentlicher Raum; Informationszugangsrecht; Ermittlungsführung; Öffentlichkeit; Rechtsbegriff; Privatsphäre; Zugriffsschutz; Staatlicher Eingriff; Polizeiliche Datenverarbeitung; Verdeckte Datenerhebung; Telekommunikationsdaten; Identifizierungspflicht; Abschottung; Internetforum; Soziales Netzwerk; Datenschutzrecht; Eingriffsermächtigung; Repressive Maßnahme; Präventivmaßnahme

ID-nummer: 20111030

Weinberger, Sharon

Stuxnet - Erstschlag im Cyberkrieg? Seit im Juni 2010 ein Computervirus weltweit hektische Aktivität auslöste, fürchten IT-Sicherheitsexperten: Der lange befürchtete >>Cyberwar<< hat begonnen - oder steht uns unmittelbar bevor.

Spektrum der Wissenschaft, 2011, 10, S. 92-94
mit 1 TAF, 2 BILD

Das im Juni 2010 im Iran entdeckte Computervirus Stuxnet war weit komplexer als alle zuvor bekannten Schadprogramme.
In speziellen Testlabors zeigte sich, dass dieses Virus von Experten entwickelt worden war, um industrielle Produktionsprozesse zu sabotieren und demonstrierte damit, dass lebenswichtige Infrastruktur, die unsere Gesellschaft mit Wasser und Energie versorgt, angreifbar ist. Und noch etwas machte Stuxnet zu etwas Besonderem: Viele industrielle Steuerungssysteme sind zum Schutz vor Hackern erst gar nicht mit dem Internet verbunden, doch der Wurm gelangte vermutlich über einen USB-Speicherstick in das Netzwerk des iranischen Unternehmens.
Stuxnet ist ein derart ausgetüftelter Wurm, dass die meisten Forscher einen Geheimdienst als Urheber vermuten. Es steht zu befürchten, dass die Ära des Wettrüstens im Cyberspace wahrscheinlich gerade erst begonnen hat.

Cybercrime; Computervirus; Schadsoftware; Informationstechnologie; Infrastruktur; Angriffsobjekt; Iran

ID-nummer: 20111029

Suhr, André

Angriffsziel Stromzähler; Elektrische Energie wird künftig an vielen Orten erzeugt, gepeichert und verbraucht. Dazu muss das Stromnetz feinmaschiger und >>intelligenter<< werden.

Spektrum der Wissenschaft, 2011, 10, S. 90-91
mit 1 TAF, 1 BILD

Energieversorgungsanlagen zählen zu den wichtigsten und zugleich kritischsten Elementen der Infrastruktur von Staaten. Damit alle Komponenten, auch die der Verteilung, stets verlässlich funktionieren, setzte man in der Vergangenheit vor allem auf Lösungen aus der Elektrotechnik. Im Zuge der Automatisierung setzen die Firmen nun zunehmend Computerintelligenz und speicherprogrammierbare Steuerungen ein - logische Schaltkreise, die nur zur Steuerung bestimmter Geräte und Prozesse dienen.
Im Zuge dieser Entwicklung wächst der Datenaustausch und - nicht anders als in anderen Wirtschaftsbereichen - die Bedeutung der cyber security, also der Sicherheit in den Kommunikationsnetzen. Neben Bedrohungsszenarien mit terroristischem Hintergrund kommt durch die Smart Grids auch die Computerkriminalität ins Spiel.
Deshalb gilt es, durch Dezentralisierung der Kommunikationsnetze, einem Angreifer den Zugang unmöglich zu machen

Elektrizität; Strom; Energieabgabe; Angriffsobjekt; Kritische Infrastruktur; Cybercrime; Netzwerk; Hacking

ID-nummer: 20110895

Schulzki-Haddouti, Christiane

Gläserne soziale Netzwerke; Fahndung in digitalen sozialen Interaktionen

Bürgerrechte & Polizei, 2011, 98, Nr. 1, S. 32-39
mit 16 QU

Nach Bewertung der Autorin ist die Netzwerkanalyse für Strafverfolger zu einer wichtigen Ermittlungsmethode geworden. Die bei den Anbietern von Social Media gespeicherten Datenmassen böten ein reiches Reservoir, das zu Ermittlungen in einer rechtlichen Grauzone verführen könne. Gleichzeitig überträfen neue Analysemethoden die herkömmlichen Formen der Ermittlung an Effizienz bei weitem; insbesondere, weil sie eine Verknüpfung personenbezogener Daten aus Social Media-Diensten mit solchen aus verschiedensten anderen Quellen ermöglichen würden: Aus dem Internet, aus Telekommunikationsverbindungen und diversen Datenbanken, zu denen die Polizei Zugang habe. Für Polizeien (und Geheimdienste) würden die neuen Methoden das Versprechen enthalten, versteckte soziale Netzwerke zu rekonstruieren. Inwieweit damit tatsächliche Verbindungen realitätsnah abgebildet werden könnten, sei eine andere Frage. Angesichts der Tatsache, dass das Forschungsgebiet noch relativ jung ist, liege es nahe, dass die Gefahr groß ist, dass unbeteiligte Personen in die Ermittlungen hineingezogen und Verdachtsfälle konstruiert werden, die einer näheren Überprüfung nicht standhalten. Ein reflektierter wie auch vorsichtiger Umgang mit diesen mächtigen Ermittlungswerkzeugen sei daher angebracht. Eine entsprechende Begleitforschung stehe noch aus.

Soziales Netzwerk; Datenauswertung; Netzwerkanalyse; Internet; Merkmalsvergleich; Gruppenbeziehung; Strukturanalyse; Rekonstruktionsmethode; Kommunikationsstruktur; Personendaten; Überwachungsmethode; Fahndungsmittel; Verbindungsdaten; Polizeiliche Beobachtung; Cybercrime; Strafverfolgungsbehörde; Datenschutzrecht; Forschungsaufgabe

ID-nummer: 20110938

Huber, Martin

Kampf um die Unverwundbarkeit; Informationsschutz in Zeiten der elektronischen Kriegsführung

IT-Sicherheit - Management und Praxis, 2011, 4, S. 20-22
mit 1 BILD

Schwachstellen in Schutzmaßnahmen sind nach Bewertung des Autors eine Realität, mit der wir uns arrangieren müssen. Kein System oder eine Einzelmaßnahme böte einen hundertprozentigen Schutz. Daher müssten alle Bausteine der Sicherheitsarchitektur eines Unternehmens so miteinander verknüpft werden, dass etwaige Unzulänglichkeiten an einer Stelle durch eine andere Stelle kompensiert werden. Gerade beim Informationsschutz sehe die Realität jedoch meist anders aus. Das Thema würde häufig nur auf technischer Ebene angegangen und liegt daher in der alleinigen Verantwortung der IT-Abteilung. Dabei könne ein Schutz gegen die zunehmende Bedrohung durch Wirtschaftsspionage der ausländischen Nachrichtendienste nur durch eine interdisziplinäre Zusammenarbeit aller Unternehmensbereiche gewährleistet werden.

Informationsschutz; Wirtschaftsspionage; Unternehmensschutz; Datenspionage; IT-Sicherheit; Schwachstellenanalyse; Angriff; Datendiebstahl; Hacker; Infrastruktur; Netzwerk; Datenverschlüsselung; Passwort; Verschlüsselungsverfahren; Algorithmus; Organisationsplanung; Sicherheitsarchitektur; Sicherheitsmaßnahme

ID-nummer: 20110969

Ebert, Andreas

Aktuelle Herausforderungen in der Informationssicherheit; Lösungsansatz für den Schutz Kritischer Infrastrukturen

Homeland Security, 2011, 2, S. 25-27
mit 3 BILD

Zwei Faktoren beeinflussen heute maßgeblich die Informationssicherheit. Zum einen die Konvergenz digitaler Technologien und die weiter zunehmende Abhängigkeit von ihnen. Zum anderen die heute relative Einfachheit, mit der digitale Technologien angegriffen werden können. Um den neuen und immer komplexeren Herausforderungen in der Informationssicherheit begegnen zu können, verfolgt RWE den Ansatz, seine IT-Sicherheitsmaßnahmen integriert, konsequent und umfassend aufzusetzen.
Integriert: Informationssicherheit ist Aufgabe und Teil der Konzernsicherheit. Damit agiert die Informationssicherheit unabhängig von der IT und den Prioritäten des CIO. Dennoch bedeutet diese ablauforganisatorische Trennung nicht in Konkurrenz mit der IT-Abteilung zu treten, sondern vielmehr in einer Win-Win-Situation die Sicherheitsherausforderungen anzugehen und sich gegenseitig in der Lösungsfindung zu ergänzen.
Konsequent: RWE versteht Informationssicherheit als Prozess über alle Stufen der Informationsgewinnung und -verarbeitung, unabhängig vom Medium, gleich ob Papier oder digital.
Umfassend: Über alle digitalen Technologien hinweg werden Menschen, Prozesse und Technologien über alle Schritte des "Information life cycle" in die Betrachtung einbezogen. Informationssicherheit im RWE-Konzern umfasst die "klassische IT", Telekommunikation, SCADA bzw. Prozesssteuerungssysteme sowie Medien- und Gebäudetechnik.

Kritische Infrastruktur; Informationstechnologie; Informationssicherheit; IT-Sicherheit; Sicherheitsrisiko; Soziales Netzwerk; Unternehmenssicherheit

ID-nummer: 20111028

Seewald, Maik G.

Ganzheitliche Hackerabwehr; Wenn die Anlagen der Energiewirtschaft mit immer mehr Computerintelligenz ausgestattet werden, müssen die Betreiber sie stärker miteinander vernetzen. Das aber bietet Hackern neue Angriffspunkte.

Spektrum der Wissenschaft, 2011, 10, S. 88-89
mit 1 BILD

Um eine verlässliche Energieversorgung auf lange Sicht zu ermöglichen, muss die Stromverteilung noch stärker automatisiert, ihre Kraftwerke und Verbraucher sowie Schalt- und Umspannanlagen noch besser aufeinander abgestimmt werden, als es heute schon der Fall ist. Das erfordert "intelligentere" Steuersysteme als bislang - daher die Bezeichnung "Smart Grids" für solche Netze. Damit vollzieht sich ein Paradigmenwechsel: von isolierten Systemen hin zu hochgradig über Kommunikationsnetze verbundenen Installationen. Diese Entwicklung birgt aber auch Risiken. Gelingt es Hackern, an einem Endpunkt in das Netz einzudringen, können sie Informationen stehlen oder das Stromnetz manipulieren - mit gravierenden Folgen.
Diesen Herausforderungen trägt nur ein "ganzheitlicher" Ansatz Rechnung. So müssen Programmierer und Ingenieure bei der Entwicklung neuer Komponenten Sicherheitsanforderungen von Beginn an mitdenken - und zwar für den gesamten Lebenszyklus des jeweiligen Produkts. Experten sind sich einig, dass als technische Grundlage einer umfassenden Sicherheitsarchitektur der als Internetprotokoll (IP) bekannte Kommunikationsstandard fungieren sollte.

Energieabgabe; Elektrizität; Infrastruktur; Kritische Infrastruktur; Computertechnologie; Computermissbrauch; Hacking; Kommunikationsnetz; Steuerungsfähigkeit; Sicherheitsnetz; IT-Sicherheitskonzept

ID-nummer: 20111059

Krimmel, Harald; Waschke, Matthias

Nichts geht mehr?! (D)DoS-Angriffe - Technik. Erkennung und Abwehr-Maßnahmen

KES - Die Zeitschrift für Informations-Sicherheit, 2011, 5, S. 73-76, 78-81
mit 3 TAF

Ziel einer DDoS-Attacke ist es, dass ein Netzwerk oder Dienst über das Internet nicht mehr erreichbar oder zumindest stark gestört ist. Die Vielzahl potenzieller Angreifer stellt heute für Unternehmen und öffentliche Einrichtungen ein fast unkalkulierbares Risiko dar - unkalkulierbar auch deswegen, weil viele Unternehmen und Organisationen die vorhandenen Risiken massiv unterschätzen, sich ihrer nicht bewusst sind oder sie schlicht ignorieren. Konnte man bei früheren DDoS-Attacken noch von Angriffen auf vereinzelte Branchen ausgehen, hat sich in den letzten Jahren gezeigt, dass jedes Unternehmen und jede öffentliche Einrichtung ein potenzielles Opfer ist. Angreifern geht es um Geld, Erpressung, Schädigung von Konkurrenten, Vandalismus oder sogar die "Kriegsführung" über das Internet. Anders als früher braucht man heute weder profunde Software-Kenntnisse noch teure Hardware - ein einfaches Netbook reicht meist vollkommen aus, der Rest ist in Leitfäden auf einschlägigen Internetseiten schnell zu lernen.
Die Autoren beleuchten das Gefährdungspotential und zeigen mögliche Erkennungs-, Schutz- und Abwehrmaßnahmen auf.

Cybercrime; Computersabotage; Hacking; Erpressung; Unternehmenssicherheit; IT-Sicherheit; Sicherheitsmaßnahme

ID-nummer: 20111027

Nicol, David M.

Angriff auf das Stromnetz; Computerviren haben bereits gezielt industrielle Steuerungssysteme infiziert. Als Nächstes könnte das Stromnetz in das Fadenkreuz von Saboteuren geraten.

Spektrum der Wissenschaft, 2011, 10, S. 82-86
mit 3 TAF, 1 BILD

Das Stuxnetvirus, das im Sommer 2010 in gesicherte Anlagen zur Urananreicherung des Iran eindrang, hat der Welt vor Augen geführt, dass industrielle Anlagen das Ziel von Hackern sein können und dass ein von Experten für Industrieautomatisierung entwickeltes Virus in technischen Infrastrukturen erheblichen Schaden anrichten kann. Deutlich wurde auch wie wenig Sicherheitsexperten darauf vorbereitet sind. Besondere Sorge bereitet die Versorgungsinfrastruktur, von der moderne Staaten existenziell abhängig sind. Elektronische Intelligenz steuert heutzutage sämtliche Abläufe im Energienetz, von den Generatoren der Kraftwerke über die verschiedenen Stufen der Stromverteilung bis zu jenen Transformatoren, welche die Spannung auf das Niveau der zu den Häusern führenden Leitungen absenkt. Die meisten dieser Rechner verwenden gängige Betriebssysteme wie Windows oder Linux - obwohl sie spezialisiert und keine Universalcomputer wie handelsübliche PCs sind. Das macht sie angreifbar.
Weil ein ausgetüftelter Angriff Simulationen zufolge einen großen Teil des Stromnetzes lahmlegen könnte, werden die Sicherheitsvorkehrungen derzeit erhöht. Viele Experten sehen so genannte Hash-Funktionen als Lösung an.

Computervirus; Schadsoftware; Hacking; Sabotage; Angriff; Industriegesellschaft; Netzwerk; Cyberterrorismus; Infrastruktur; Elektrizität; Strom

ID-nummer: 20110941

Wagner, Friederike

Verschlüsselte Botschaften; Sicherheitsmaßnahmen für geschäftskritische Daten

IT-Sicherheit - Management und Praxis, 2011, 4, S. 28-29
mit 2 BILD, 1 TAF

Gehen Daten aufgrund von kriminellen Angriffen verloren, droht den betroffenen Unternehmen ein hoher wirtschaftlicher Schaden. Dabei gefährden interne wie auch externe Quellen die sensiblen Daten. Wer sein Netzwerk regelmäßig überprüft und beispielsweise E-Mails mit geschäftskritischen Inhalten verschlüsselt, begegnet nach Meinung der Autorin den Attacken wirkungsvoll. Auf der sicheren Seite stünden die Firmen, die rechtzeitig ein umfassendes Konzept für ihre IT-Sicherheit einführen. Technische und organisatorische Maßnahmen werden im Rahmen einer Sicherheitsanalyse zum Schutz personenbezogener und weiterer Daten wie Unternehmenskennzahlen überprüft. Aus Sicht eines externen Angreifers lassen sich über Penetrationstests weitere Sicherheitslücken aufdecken und schließen. Zu einem umfassenden IT-Sicherheitskonzept gehören auch klar definierte Zugriffsberechtigungen: Welcher Mitarbeiter darf welche Aktion mit welchem Dokument ausführen? Ein weiterer wichtiger Aspekt ist die sichere und vertrauliche Übertragung von geschäftskritischen Daten. Zu einem umfassenden Sicherheitskonzept gehört auch die Verschlüsselung der Daten auf Speichersystemen wie etwa den Festplatten. Speicher in mobilen Geräten wie etwa einem Notebook stehen oben auf der Prioritätenliste, denn hier ist die Gefahr eines Verlusts oder Diebstahls besonders groß.

Informationsschutz; IT-Sicherheitskonzept; Organisationsplanung; Risikoanalyse; Gefährdungsgrad; Audit; Unternehmensschutz; Datenspionage; IT-Sicherheit; E-mail; Datenträger; Schwachstellenanalyse; Angriff; Datendiebstahl; Hacker; Datenverschlüsselung; Verschlüsselungsverfahren; Zugriffskontrolle; Sicherheitsarchitektur; Sicherheitsmaßnahme

ID-nummer: 20110940

Niemantsverdriet, Jelle

Datenverletzungen und Industriespionage verhindern; Basis-Best-Practices für IT-Sicherheit

IT-Sicherheit - Management und Praxis, 2011, 4, S. 26-27
mit 1 BILD

Industriespionage betrifft zahlreiche Branchen, insbesondere Firmen, die über geistiges Eigentum verfügen und bei denen sich der Einsatz von Technologie auf das Geschäft Insgesamt auswirkt. Grundsätzlich kann man sagen, solange geschäftskritische Daten generiert, übertragen und gespeichert werden, werden Unternehmen im Visier von Kriminellen sein, die mit diesen Informationen Geld machen wollen. Die Cyber-Kriminalität entwickelt sich ständig weiter; permanent werden von Hackern rund um den Globus neue Taktiken entwickelt.
Unternehmen sind daher gefordert, verstärkt auf ihre Sicherheitsvorkehrungen zu achten, um unberechtigten Zugriff auf geschäftlich vertrauliche Informationen zu verhindern. Das Rezept gegen Sicherheitsverletzungen besteht im Einsatz simpler, grundlegender Sicherheitspraktiken.

IT-Sicherheit; Unternehmenssicherheit; Industriespionage; Konkurrenzspionage; Datensicherheit; Hacker

ID-nummer: 20111303

Hange, Michael

Informationsdrehscheibe gegen Cyber-Angriffe

Die Polizei, 2011, 12, S. 351-352

Das Nationale Cyber-Abwehrzentrum hat seit April 2011 den Auftrag, Informationen der beteiligten Behörden über IT-Sicherheitsvorfälle auszutauschen, zu bewerten und Handlungsempfehlungen zu erarbeiten. Mittlerweile fungieren zahlreiche IT-Systeme als Lebensadern für den Staat, die Wirtschaft und unsere Gesellschaft - ihr Ausfall hätte dramatische Folgen für unser Gemeinwesen. Die Standardisierung in der Informationstechnologie, aber auch das Internet haben eine neue Qualität der Verwundbarkeit geschaffen, der der Staat mit seiner Cyber-Sicherheitsstrategie begegnet. Ein Element der Strategie ist das Nationale Cyber-Abwehrzentrum. Der Autor gibt einen Überblick über die Sicherheitsstrategie.

Cybercrime; Abwehrmaßnahme; IT-Sicherheit; IT-Sicherheitskonzept; Datensicherheit; Sicherheitsstrategie; Nationale Sicherheit

ID-nummer: 20111398

Schaaf, Christian; Oelmaier, Florian

Ganzheitliche Pentests und Audits; Interdisziplinäre "Spionage"-Penetrationstests und -Audits zur Abwehr von Cyberwar-Bedrohungen

KES - Die Zeitschrift für Informations-Sicherheit, 2011, 6, S. 20-23
mit 3 TAF

Angreifer bedienen sich zur Wirtschaftsspionage heute einer umfassenden Mixtur sowohl von IT-Attacken als auch klassischer Szenarien wie Einbruch, Erpressung oder Social Engineering. Die Erfahrung aus verschiedenen Spionage-Penetrationstests der Autoren hat gezeigt, dass viele Unternehmen zu wenig Zeit darauf verwenden, alle "Schlupflöcher" zu identifizieren und die Mitarbeiter entsprechend zu sensibilisieren. In vielen Fällen wird es den Tätern zu einfach gemacht und schon ein scharfer Ton am Telefon, um den Mitarbeiter einzuschüchtern, führt nicht selten zur Herausgabe eines Passworts - oder das forsche Auftreten am Werkstor zum Öffnen des Zugangs. Ein Spionage-Penetrationstest zeigt oft sehr deutlich, wie die verknüpfte Nutzung aller Ressourcen das Eindringen oft spielend einfach ermöglicht.
Neben dem ganzen Repertoire der IT-Sicherheit muss ein Spionage-Penetrationstest weitere Aspekte beleuchten. Grundsätzlich sind alle Angriffe auf sicherheitskritische Prozesse zu erfassen, die bei der Verteidigung von Wettbewerbsvorteilen eines Unternehmens eine Rolle spielen. Der Startpunkt eines Spionage-Penetrationstests ist daher eine Analyse aller möglichen Angriffspfade und -szenarien.
Um erfolgversprechend zu arbeiten, muss auch die Spionageabwehr im ganzheitlichen Sinne der Sicherheit einen kreativen Mix von Maßnahmen umsetzen - spezielle Pentests oder Audits können hier helfen.

Wirtschaftsspionage; Spionageabwehr; Unternehmenssicherheit; Unternehmensschutz; Cybercrime; IT-Sicherheit; Kommunikationsnetz

ID-nummer: 20110950

Robertz, Frank J.

Herausforderung Cybercrime

Deutsche Polizei, 2011, 9, S. 28-33
mit 2 BILD, 2 TAF, 4 QU

Entgegen klassischen Straftaten ist durch die Begehung von Cybercrimes meist keine direkte Interaktion mit dem Opfer mehr nötig und die Begehung der Taten ist problemlos über Ländergrenzen hinweg möglich. Eine automatisierte Vorgehensweise erlaubt dabei eine große Zahl von Opfern und die Ermittlung bzw. Verfolgung der Täter wird so erheblich erschwert. Selbst das Streuen krimineller Ideen oder die bloße Aufforderung zu einer Straftat erreichen im Internet ungeahnte Dimensionen.
Mit seinen Möglichkeiten zur Begehung immer neuer Formen von Straftaten bildet Cybercrime eine Kernherausforderung für die heutige und zukünftige Polizeiarbeit. Zudem gilt es, der Bevölkerung eindringlich die Gefahren des Cybercrime zu verdeutlichen und dabei auch ihr eigenes Verantwortungsgefühl zu stärken. Neben Informationsmaterialien und aktiven Vermittlungsversuchen wären dabei auch das Wissen und die Möglichkeiten aller Bürger zur effektiven Vorbeugung vor Cybercrime zu verbessern.
Der Verfasser erläutert Phänomenologie des Cybercrime und stellt aktuelle Abwehrmaßnahmen, wie das das Nationale Cyber-Abwehrzentrum des Bundes vor.

Cybercrime; Informations- und Kommunikationstechnologie; Internetkriminalität; Computerkriminalität; Computermanipulation; Industriespionage; Mobbing; Cyberterrorismus; IT-Sicherheit; BSI

ID-nummer: 20110937

Karden, Wilfried

Weltkrieg um Informationen; Wirtschaftsspionage und IT

IT-Sicherheit - Management und Praxis, 2011, 4, S. 18-19
mit 1 BILD

Wirtschaftsspionage ist die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. So definieren es die deutschen Sicherheitsbehörden. Damit ist klar, wo die Abgrenzung zu Konkurrenzausforschung/-ausspähung und Industriespionage liegt: Hier handelt es sich um eine Aktion, die ein Unternehmen gegen ein anderes betreibt. Wirtschaftsspionage hat heute ein alarmierendes Ausmaß erreicht, doch nach Meinung des Autors können Unternehmen die Bedrohung durchaus in den Griff bekommen. Die Frage bleibt jedoch: Was genau ist Wirtschaftsspionage, wie wirkt sie im Alltag von Unternehmen, wer sind die Angreifer, ihre Methoden und wie können Unternehmen sich schützen? Wirtschaftsspionage bedeutet in seiner Wirkung nichts anderes als Diebstahl bei Unternehmen: In jedem Unternehmen gibt es Kenntnisse, die zumindest für einen definierten Zeitraum nicht an unbefugte Dritte gelangen sollen. Genau auf dieses Wissen haben es die Angreifer bei der Wirtschaftsspionage abgesehen. Hierbei kann es sich ebenso um Produkt-Neuentwicklungen handeln wie um Kunden-, Angebots- oder Personaldaten, Gehaltsvereinbarungen oder Ähnliches. Das verbindende Element ist, dass es sich hierbei um das unternehmenskritische Know-how handelt (die entscheidenden fünf Prozent aller Unternehmensdaten). Dieses Wissen ist in den IT-Systemen der Unternehmen unterwegs oder ruht in ihren Datenbanken. Genau dieses unternehmensrelevante Know-how ist auf engen und schnelllebigen Märkten jedoch interessant für eine Vielzahl von Angreifern. Wirtschaftsspionage hat heute ein alarmierendes Ausmaß erreicht, doch nach Meinung des Autors können Unternehmen die Bedrohung durchaus in den Griff bekommen, indem die in diesem Beitrag kurz beschriebenen Schutzmaßnahmen umgesetzt werden.

Wirtschaftsspionage; Unternehmensschutz; Datenspionage; IT-Sicherheit; Angriff; Sensitive Daten; Informationsschutz; Nachrichtendienst; Datendiebstahl; Hacker; Computervirus; Infrastruktur; Netzwerk; Datenverschlüsselung; Sicherheitsmaßnahme

ID-nummer: 20110964

Seitz, Norbert

Neue Herausforderungen und Entwicklungen beim Schutz Kritischer Infrastrukturen; Staatliche und unternehmerische Sicherheitsvorsorge

Homeland Security, 2011, 2, S. 8-10

Die Gewährleistung des Schutzes der Kritischen Infrastrukturen ist eine Kernaufgabe staatlicher und unternehmerischer Sicherheitsvorsorge und fester Bestandteil der Sicherheitspolitik unseres Landes. Von besonderer Bedeutung ist dabei die partnerschaftliche Zusammenarbeit von Staat und Wirtschaft, da ca. 80% der Kritischen Infrastrukturen in Deutschland privatwirtschaftlich betrieben werden. Mit der 2009 von der Bundesregierung beschlossenen "Nationale Strategie zum Schutz Kritischer Infrastrukturen" - der KRITIS-Strategie - wurde zum ersten Mal eine Gesamtstrategie des Bundes zum Schutz Kritischer Infrastrukturen erarbeitet. Alle Akteure - staatlicherseits wie privatwirtschaftlich - sind aufgerufen, die Strategie umzusetzen und damit das Schutzniveau für Kritische Infrastrukturen zu erhöhen. Die Strategie fordert dazu auf, im Dreiklang von Prävention, Reaktion und Nachhaltigkeit zu handeln.
Der Autor, Abteilungsleiter im BMI, stellt Schutzkonzepte und Leitfäden vor.

Krisenmanagement; Bevölkerungsschutz; Kritische Infrastruktur; Sicherheitspartnerschaft; IT-Sicherheit; Schutzkonzept; Bundesministerium des Innern; BSI

ID-nummer: 20110495

Bär, Wolfgang

Phishing und materielles Strafrecht

Der Kriminalist, 2011, 6, S. 17-20
mit 2 BILD, 24 QU

Unter "Phishing" werden alle Vorgehensweisen zusammengefasst, bei denen Täter über gefälschte WWW-Adressen versuchen, an die Zugangsdaten für Online-Dienste eines Internet-Nutzers zu gelangen. Der Begriff selbst ist ein englisches Kunstwort, das ich an fishing ("Angeln", "Fischen"), auch password fishing, anlehnt und damit bildlich das "Angeln nach Passwörtern mit Ködern" umschreibt. Zu diesem Zweck werden von den Tätern unterschiedlichste technische Wege beschritten. Die bisher gebräuchlichste Begehungsform besteht darin, dass der Internet-Nutzer über eine E-Mail, die den Eindruck erweckt, von der Bank oder einem anderen Anbieter von Online-Diensten zu stammen, dazu aufgefordert wird, einen Hyperlink anzuklicken, um so auf eine bestimmte, vom Täter eingerichtete Web-Seite zu gelangen. Auf dieser Seite ist die Aufforderung zu lesen, die eigenen Zugangsdaten für Online-Banking (PIN und TAN) oder zunehmend auch für andere Angebote (eBay, Facebook usw.) einzugeben. Sobald der Betroffene seine Daten eingegeben hat, werden diese vom Täter zwischengespeichert und später dazu verwendet, um zulasten des Internet-Nutzers vermögens schädigende Transaktionen vorzunehmen. Ob und wie diese Vorgehensweisen der Täter durch das materielle Strafrecht erfasst werden, wird in diesem Beitrag aufgezeigt.

Phishing; Modus operandi; Computerbetrug; Täuschungshandlung; E-mail; Online-Banking; Passwort; Datenspionage; Tatbestandsmerkmal; Strafbarkeitsbedingung; Materielles Strafrecht; StGB P 263; StGB P 263 a; Internetkriminalität

ID-nummer: 20110613

Schipp, Sebastian; Mähler, Dominique

Mauerwerk für kritische Infrastrukturen; Staatliche Strategien zum Schutz behördlicher Informations- und Kommunikationsbestände

IT-Sicherheit - Management und Praxis, 2011, 3, S. 66-69
mit 1 BILD, 4 TAF

Die hochentwickelten Industriegesellschaften sind stärker als je zuvor von der Verfügbarkeit leistungsfähiger Infrastrukturen, wie zum Beispiel Stromversorgung oder Kommunikationsinfrastrukturen, abhängig.
Aus diesem Grunde hat die Europäische Union hat im Dezember 2008 eine Richtlinie für den Schutz kritischer Infrastrukturen (EPSKI) verabschiedet. Ziel ist es, kritische europäische Infrastrukturen vor Störungen durch sämtliche denkbaren Risiken besser zu schützen. Der Schwerpunkt der Richtlinie liegt zurzeit auf der Verbesserung der Kommunikation und betrifft nur die Sektoren Energie und Verkehr. In Deutschland hat die Bundesregierung im Juli 2005 den "Nationalen Plan zum Schutz der Informationsinfrastrukturen" (NPSI) als übergreifende Strategie zur IT-Sicherheit beschlossen. Abgeleitet aus dem NPSI sind der Umsetzungsplan KRITIS (UP KRITIS) und der Umsetzungsplan Bund (UP Bund) entstanden. Der UP Bund gilt für alle Ressorts und Bundesbehörden und soll mittel- bis langfristig Informationssicherheit auf hohem Niveau in der gesamten Bundesverwaltung garantieren. Der UP KRITIS beschreibt Prozesse und Maßnahmen, die von den Betreibern kritischer Infrastrukturen umgesetzt werden sollten.

Infrastruktur; Industriegesellschaft; Informationssicherheit; Cybercrime; IT-Sicherheitskonzept; Industriebetrieb; Schutzkonzept; Krisenmanagement; Risikomanagement; Gefahrenanalyse

ID-nummer: 20120588

Degenhardt, Werner

112-Internet; Auf dem Weg zum IT-Notrufsystem

BSI-Veröffentlichung, 2011, S. 435-444
Sicher in die digitale Welt von morgen; 12. Deutscher IT-Sicherheitskongress des BSI, Bonn; BR Deutschland, 2011 [April]
mit 4 TAF, 1 QU

Strategien zur Verbesserung der "Cyber Security" nehmen den Benutzer in der Regel als eine der Schwachstellen wahr, die Angriffe auf die Informationsinfrastruktur erleichtern oder überhaupt erst ermöglichen. Awareness-Initiativen wollen den Benutzer durch die Verbesserung der Verfügbarkeit von Information stärken und sein Sicherheitsverhalten verbessern. Ein IT-Notrufsystem mit situationsangemessener Hilfe führt nach Bewertung des Autors hier zu besseren Ergebnissen in einem ohnehin von Informationsüberlastung geprägten Umfeld. Das im Beitrag beschriebene IT-Notruf-System werden zum Zeitpunkt der Veröffentlichung des Beitrags in einer Entwicklungsversion in der Fakultät für Psychologie und Pädagogik der Ludwig-Maximilians-Universität München (LMU) im Benutzertest evaluiert, gleichzeitig werden Communities of Practice und eine Wissensdatenbank aufgebaut.

EDV-Einsatz; Fehlermanagement; Menschliches Handeln; IT-Sicherheit; Notrufsystem; Expertensystem; Nutzungsverhalten; Wissensmanagement; Situationsanalyse; Gefahrenprognose; Künstliche Intelligenz; Selbsthilfe; Softwareschutz; Infrastruktur; Sicherheitsleitsystem

ID-nummer: 20110538

Anonym

Stromversorger im Dunkeln; Steigende Zahlen von Cyberangriffen auf Versorgungsunternehmen

W&S - Das Sicherheitsmagazin, 2011, 3, S. 10-11
mit 1 TAF

Nach der in diesem Beitrag berichteten, von der IT-Sicherheitsfirma McAfee beim Center for Strategic and International Studies (CSIS) in Auftrag gegebene Studie werden 80 Prozent der Energieversorgungsunternehmen durch Cyberattacken angegriffen, und 25 Prozent erfahren Erpressungsversuche durch Hacker. Demnach seien die Betreiber der Infrastrukturen zur Versorgung mit Strom, Öl, Gas und Wasser durch Angriffe von Internetkriminellen so stark gefährdet wie niemals zuvor.

Cybercrime; Computersabotage; Infrastruktur; Strom; Wasser; Gas; Kritische Infrastruktur; Angriff; Wirtschaftsunternehmen; Erpressung; Computervirus; Hacker; Gefahrenpotential; Sicherheitslage; Internetkriminalität; Industriebetrieb; Befragungsergebnis

ID-nummer: 20110388

Arends, Holger; Kranawetter, Michael

Informationssicherheit ganzheitlich managen; Modell für ein unternehmensweites Security-Bewusstsein

IT-Sicherheit - Management und Praxis, 2011, 2, S. 52-55
mit 1 BILD

Umfassend, weitsichtig und weit vorausschauend - diese drei Adjektive beschreiben die meist vernachlässigten Punkte im Umgang mit Informationssicherheit. Die Kernproblematik liegt in der Tatsache, dass in vielen Firmen die Arbeit der Sicherheitsverantwortlichen isoliert abläuft.
Wer jedoch Informationssicherheit umfassend, weitsichtig und weit vorausschauend betreiben will, muss möglichst viele Aspekte und Zusammenhänge berücksichtigen. Dabei geht es um die Erkennung von Ursprüngen und Zielen, um Eigenschaften und Zuordnungen, direkte und indirekte Beziehungen und Querbeziehungen, Regeln und Normen ebenso wie um Rahmenbedingungen, Nutzenabwägungen und Anwendungsaspekte.

Informationssicherheit; Informationsmanagement; IT-Sicherheitskonzept; Unternehmenssicherheit; Wirtschaftsspionage; Sicherheitsstrategie; Compliance

ID-nummer: 20110494

Kindler, Waldemar

Bedeutsame Handlungsfelder der Sicherheitspolitik aus Sicht des Landespolizeipräsidenten von Bayern, Waldemar Kindler; Rede vom 6.4.2011 anlässlich der Verleihung der 9. Ehrenkriminalmarke an den bayerischen Landespolizeipräsidenten durch den BDK-Bezirksverband Köln mit seinem Bezirksvorsitzenden und stv. BDK-Landesvorsitzenden NRW, Rüdiger Thust [fing.]

Der Kriminalist, 2011, 6, S. 13-17
mit 3 BILD, 2 QU

Kindler, der seit einigen Jahren auch Vorsitzender des AK II der Ständigen Konferenz der Innenminister- und Senatoren ist, beleuchtete in seiner Rede einige bedeutende Aspekte der Sicherheitspolitik, positionierte sich aber besonders auch in Fragen der Kriminalpolizei eindeutig. In fünf Handlungsfelder (Islamistischer Terrorismus, Grenzenloses Europa, luK- und Wirtschaftskriminalität, Personalressourcen und TK-Verbindungsdaten) teilte er sein Statement auf.

Sicherheitspolitik; Islamistischer Terrorismus; Europa; Europäische Integration; Cybercrime; Wirtschaftskriminalität; Personallage; Telekommunikationsdaten; Verbindungsdaten

ID-nummer: 20110577

Witt, Bernhard C.

CSI Cyberspace; Anforderungen an die Durchführung IT-forensischer Untersuchungen

KES - Die Zeitschrift für Informations-Sicherheit, 2011, 3, S. 51-56
mit 1 BILD, 2 TAF, 15 QU

IT-Forensik ist als streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen anzusehen. Für das methodische Vorgehen solcher Analysen bestehen zahlreiche Anforderungen, insbesondere durch den Datenschutz. Das beginnt bereits bei der Bestimmung eines konkreten Anfangsverdachts und erstreckt sich über die Einbeziehung zentraler Funktionen im eigenen Haus bis hin zur sorgsamen und geschützten Dokumentation und gegebenenfalls der Auswahl geeigneter Dienstleister.

IT-Sicherheit; Informationssicherheit; Forensische Untersuchung; Untersuchungsverfahren; Anforderungskatalog; Anfangsverdacht

ID-nummer: 20110445

Albrecht, Hans Jörg

Grooming, das Internet und die Schließung von Sicherheits- und Strafbarkeitslücken

MschrKrim - Monatsschrift für Kriminologie und Strafrechtsreform, 2011, 2, S. I-IV
mit 23 QU

Die Furcht vor der Viktimisierung von Kindern durch den fremden Pädophilen treibt die Debatten über Grooming an. Sie hat zu Gesetzen und Praktiken geführt, die vor dem Hintergrund empirischer Forschung als überzeichnend, wenig hilfreich und als Ausdruck einer diffuse Furcht bedienenden common-sense-Politik gelten können.
Der Verfasser führt aus, dass zwar bislang nur wenige repräsentative Untersuchungen durchgeführt worden, die sich mit Risiken von Kindern und Jugendlichen, nach der Initiierung von Kontakten über das Internet, Opfer von Sexualstraftaten - sei es on- oder offline - zu werden, befassen, aus einer amerikanischen Untersuchung zu Fällen sexuellen Missbrauchs, die ihren Ausgangspunkt in der Herstellung von Internetkontakten hatten, sich allerdings, ergibt, dass die Opfer ganz überwiegend zwischen 13 und 15 Jahre alt waren. Keines der Opfer war jünger als 12 Jahre. Die Täter waren zu 76 % älter als 26 Jahren. Die meisten Online-Kontakte von jungen Menschen betreffen ihre eigene Altersgruppe und sind erwartungsgemäß nicht-sexueller Art sowie den Eltern bzw. Erziehungsberechtigten bekannt. Kontaktaufnahmen zu jungen Menschen, die sexuellen Charakter oder sexuelle Anspielungen beinhalten, gehen ganz überwiegend (> 90 %) von anderen Jugendlichen oder Heranwachsenden aus.
Zudem stellt er die Frage, warum die Pönalisierung der Vorbereitung des sexuellen Missbrauchs auf das Internet beschränkt und nicht auf die reale Welt ausgedehnt worden ist?

Internetkriminalität; Internetforum; Chatprogramm; Kontaktaufnahme; Minderjähriger; Sexueller Missbrauch von Kindern; Vorfeldkriminalität; Kinderschutz; Jugendschutz; Strafbarkeitsbedingung; StGB P 176

ID-nummer: 20120591

Schumacher, Astrid; Mehrfeld, Jens

De-Mail - Infrastruktur für sichere elektronische Kommunikation

BSI-Veröffentlichung, 2011, S. 469-485
Sicher in die digitale Welt von morgen; 12. Deutscher IT-Sicherheitskongress des BSI, Bonn; BR Deutschland, 2011 [April]
mit 6 TAF, 16 QU

Gegenwärtig wird unter dem Begriff "De-Mail" eine sichere und vertrauenswürdige Infrastruktur für elektronische Kommunikation über das Internet aufgebaut. Per De-Mail können Nachrichten und Dokumente zuverlässig und integer in einem sicheren Kommunikationsraum versendet werden. Gemäß § 1 De-Mail-Gesetz sollen De-Mail-Dienste einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen. De-Mail erhöht die Sicherheit der elektronischen Kommunikation im Vergleich zur herkömmlichen Kommunikation, wobei der De-Mail-Kontoinhaber ein Maximum an Sicherheit bei einem Minimum an Aufwand erhält.

Elektronischer Datenaustausch; Kommunikationsmittel; Kommunikationsmethode; Internet; E-mail; Infrastruktur; Informationsverbund; Sicherheitsgewährleistung; Rechtslage; IT-Sicherheit

ID-nummer: 20120590

Probst, Thomas; Hansen, Marit

De-Mail und Datenschutz - Gesetzliche Anforderungen, Zertifizierung und Verbesserungspotential

BSI-Veröffentlichung, 2011, S. 455-468
Sicher in die digitale Welt von morgen; 12. Deutscher IT-Sicherheitskongress des BSI, Bonn; BR Deutschland, 2011 [April]
mit 11 QU

De-Mail-Dienste sollen eine verlässliche E-Mail-Infrastruktur schaffen. Anbieter von De-Mail kann nur werden, wer in einem Überprüfungsverfahren nachgewiesen hat, dass er die spezifizierten Anforderungen an IT-Sicherheit, Datenschutz und Interoperabilität erfüllt.
Der Beitrag stellt die gesetzlichen Anforderungen an IT-Sicherheit und Datenschutz dar und beschreibt das Überprüfungsverfahren für den Datenschutz-Nachweis. Außerdem diskutieren die Verfasser, welche Verbesserungspotentiale für De-Mail-Dienste bestehen und wie diese auch ohne spezifische Vorgaben im Hinblick auf Datenschutzkonformität überprüft werden können.

E-mail; IT-Sicherheit; Datenschutz; Zertifizierung; Gesetzentwurf; Technische Richtlinie; BDSG; TKG; BSI; Prüfverfahren; Verschlüsselungsverfahren

ID-nummer: 20111461

Lannert, Detlef

Ein Lehrbeispiel für IT-Sicherheit? Der Staatstrojaner

IT-Sicherheit - Management und Praxis, 2011, 6, S. 14-15
mit 1 BILD

Beim sogenannten Staatstrojaner handelt es sich um eine klassische Spionage-Software, die mit einer "Hintertür" kombiniert ist. Da die Staatstrojaner-Software nach Bewertung des Autors offensichtlich die wichtigen für sicherheitskritische IT-Anwendungen geltenden Schutzziele nicht erfüllen kann, stelle sich einerseits die Frage, weshalb dieses Produkt so deutlich hinter dem Stand der Technik zurückbleibt, den viele proprietäre wie auch OpenSource-Programme mittlerweile erreicht haben. Die behördlichen Auftraggeber würden kritisch prüfen müssen, ob sie die Entwicklung der Software mit dem nötigen Know-how begleitet haben; "Positivtests", also einfache Funktionstests der fertigen Programme, könnten nicht die Sicherheit des implementierten Gesamtsystems gewährleisten. Auf der anderen Seite bleibe noch zu untersuchen, ob eine Software, die in "feindlicher" Umgebung hohe Anforderungen an Sicherheit und Zuverlässigkeit erfüllen muss, überhaupt realisierbar ist. Durch Reverse Engineering und Manipulationen der System- und Netzwerkumgebung könne solch ein Programm immer wirksam angegriffen werden, solange nicht im Zusammenwirken von Hardware und Betriebssystem dem Besitzer eines PCs die Kontrolle über sein Gerät völlig entzogen wird.

Computerspionage; Strafverfolgungsbehörde; Telekommunikationsüberwachung; Computervirus; Hacking; Quellensicherung; Internet; Einsatzwert; Schwachstellenanalyse; Datenverschlüsselung; Schutzziel; IT-Sicherheit; Anforderungsstruktur

ID-nummer: 20120139

Stutz, Kay

Eine neue Generation von Computerviren

Schweizer Kriminalistikjournal, 2011, 15, S. 11-12
mit 1 TAF

Eine neue Generation Computerviren, die normale Homecomputer befallen bedroht die IT-Welt. Es handelt sich um eine neue Art, wie diese sich vor Antivirus-Programmen effizient verstecken können.
Das Zauberwort hat drei Buchstaben, "FUD" diese Abkürzung das steht für "Fully Undetectable" heißt übersetzt so viel wie komplett unerkennbar. Ein Schädling, den man in der Fachsprache als FUD bezeichnet wird von zwanzig, dreißig oder sogar vierzig verschiedenen Antivirusprogrammen nicht als Solcher erkannt; sprich von keiner gängigen Antivirus Software.
Es ist relativ einfach, einen bestehenden Virus "FUD", also gänzlich unerkennbar für Antivirensoftware, zu schreiben. Dies geschieht über einen sogenannten FUD Crypter. Ein FUD Crypter nimmt einen bestehenden Computer-Schädling, z.B. einen Trojaner und verschlüsselt ihn so, dass er nicht mehr von aktuellen Antivirensoftware erkannt wird. Das heißt konkret, man kann einen für die eigenen Zwecke "etablierten" Schädling zum Einsatz bringen, welche ohne einen FUD Crypter sofort von der Antivirus Software erkannt werden würde.

Schadsoftware; Computervirus; Virensuchprogramm; Personalcomputer; IT-Sicherheit

ID-nummer: 20120585

Karge, Sven

Hilfe im Kampf gegen Botnetze: Das Anti-Botnet-Beratungszentrum

BSI-Veröffentlichung, 2011, S. 289-292
Sicher in die digitale Welt von morgen; 12. Deutscher IT-Sicherheitskongress des BSI, Bonn; BR Deutschland, 2011 [April]
mit 1 TAF

Seit September 2010 betreibt eco - Verband der deutschen Internetwirtschaft e.V. das Anti-Botnet-Beratungszentrum mit technischer Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik und finanzieller Förderung des Bundesministeriums des Innern. Am Anti-Botnet-Beratungszentrum beteiligen sich außerdem zahlreiche Internetzugangsanbieter und Hersteller von Anti-Viren-Software. Internetnutzer bekommen unter www.botfrei.de umfassende Informationen, wie sie ihren Rechner gegen Schadprogramme schützen, und können mit dem DE-Cleaner, der kostenfrei zum Download bereitsteht, ihr System auf Infektionen überprüfen. Eine telefonische Beratungshotline für Kunden der teilnehmenden Internetzugangsanbieter hilft zusätzlich Internetnutzern, die mit dem Angebot auf der Website allein nicht zurechtkommen.

Schadsoftware; Botnet; Netzwerk; Internet; Internetkriminalität; Beratungsstelle; Sicherheitsberatung

ID-nummer: 20120581

Morgner, Frank; Oepen, Dominik; Müller, Wolf; Redlich, Jens-Peter

Mobiler Leser für den neuen Personalausweis

BSI-Veröffentlichung, 2011, S. 227-240
Sicher in die digitale Welt von morgen; 12. Deutscher IT-Sicherheitskongress des BSI, Bonn; BR Deutschland, 2011 [April]
mit 1 TAF, 1 TAB, 19 QU

Durch die Einführung des neuen Personalausweises am 1. November 2010 steht erstmals mit dem elektronischen Identitätsnachweis eine im großen Umfang privat nutzbare Anwendung für eine RFID Chipkarte in Deutschland zur Verfügung. Mobiltelefone mit geeigneter NFC-Schnittstelle können als "Mobiler Leser" für den neuen Personalausweis genutzt werden und stellen eine sinnvolle Alternative zu den bisher spezifizierten Geräteklassen dar. Wichtige Anforderungen, wie lokale PIN-Eingabe, Durchführung des PACE-Protokolls, Anzeige von Informationen über den Dienstanbieter und seiner Berechtigungen sind Standard- und Komfortleser entlehnt und können auch auf einem Mobiltelefon umgesetzt werden. Zusätzlich sind die Anzeige des Auslesezwecks, eine Zertifikatsprüfung auf Aktualität, autarkes PIN-Management und eine temporäre PIN realisierbar. Der mobile Leser kann außerdem Skimming-Versuche an anderen (lokalen) Terminals erkennen und verhindern. Ein Profil "Mobiler Leser", das erforderliche und optionale Anforderungen bzw. Funktionen spezifiziert und Interoperabilität sowie "zero-footprint"-Nutzung in wechselnden Einsatzumgebungen gewährleistet, wird angestrebt. Im Vergleich zu dedizierten Lesegeräten resultieren aus einem allgemeineren Betriebssystem und vielgestaltigen Schnittstellen des Mobiltelefons neue Angriffsvektoren, die beachtet werden müssen. Ein spezieller Lesermodus des Mobiltelefons könnte diese Bedrohungen jedoch stark einschränken.

Elektronisches Dokument; Elektronisch signiertes Dokument; Identitätsnachweis; Authentifizierung; Personalausweis; Internet; Radio Frequency Identification; Mobiltelefon; Chipkarte; Online-Banking; PIN; Skimming

ID-nummer: 20120738

Holtmann, Philip

Die Nutzung des Internet durch islamistische Terroristen

Jahrbuch Terrorismus,
Jahrbuch Terrorismus 2010, 2011, S. 55-79
mit 8 TAF, 25 QU

Seit Beginn des Irakkriegs 2003 hat sich die jihadistische Medienpräsenz im Internet rasant vervielfacht. Ungefähr zehn zentrale arabische Diskussionsforen haben direkte Verbindungen zu al-Qaidas Medienrepräsentanten und gelten deshalb unter Jihadisten als besonders autoritativ. Mitglieder diskutieren und verbreiten darauf terroristische Ideen, die eine Martyriums-Kultur verherrlichen und strategische Vorgaben für Anschläge liefern. Sympathisanten greifen dies auf und überfluten damit das Internet. Die Mitglieder der virtuellen Bewegung koordinieren und organisieren gemeinsame Medienaktivitäten. Zahlreiche Anschläge und Anschlagsversuche weltweit zeigen, dass Radikalisierung genauso physisch wie virtuell stattfindet. Virtuelle Jihadisten bilden eine zunehmend selbstständigere Bewegung, die immer mehr Anhänger anzieht. Durch die massenhafte Teilnahme von anonymen Sympathisanten lässt sich die Medienarbeit al-Qaidas im Internet nur sehr schwer bekämpfen. Eine zentrale Organisation oder Vernetzung fehlt - meistens werden einzelne Individuen verhaftet, was den Cyberjihad nur kurzfristig behindert. Dieses Phänomen zeitigt auch schwerwiegende Auswirkungen in Deutschland. Deutsche Jihadisten versuchen mehr und mehr Mitglieder durch Propaganda zu rekrutieren, die im Internet zu sehen ist. Rund zehn Prozent der arabischen Websites haben eine islamische Orientierung, die auf ein starkes Zusammenspiel von Kultur und Religion auch in der virtuellen Welt des Internets hindeuten. Das Unterwandern islamischer Mainstream-Webseiten gehört zur Medienstrategie von al-Qaidas Anhängern. Schätzungen sprechen von 5.000 bis 50.000 terroristischen Webseiten. Das genaue Ausmaß des jihadistischen Webs ist unklar, weil Websites ständig gehackt und geschlossen werden sowie neu entstehen. Viele Sites haben jihadistische Inhalte, dienen aber nicht ausschließlich dem Jihad, was bei einer computergenerierten Erfassung zu sehr hohen Ergebnissen führt.

Islamistischer Terrorismus; Internet; Djihadismus; Propaganda; Medieneinsatz; Soziales Netzwerk; Kommunikationsstruktur; Anwerbung; Videofilm; Sympathiewerbung; Al Quaeda; Terroristisches Umfeld; Internetplattform; Islamismus; Jugendlicher; Radikalisierung; Attentäter; Führungsmittel

ID-nummer: 20110166

Pohlmann, Norbert; Linnemann, Markus

Ein Erfahrungsbericht; Live-Hacking-Performance als Sensibilisierungsmaßnahme

IT-Sicherheit - Management und Praxis, 2011, 1, S. 54-57

Die größte Gefahr für schützenswerte Daten, Unternehmensnetzwerke und den heimischen Computer ist nicht etwa die Technik, sondern der Mensch vor dem Bildschirm. Der Anwender ist mit der Menge an Technologien und digitalen Möglichkeiten überfordert und macht Fehler. Ihm fehlt die Sensibilität für das Thema IT-Sicherheit. Die Firmen, Behörden und Institutionen sind aufgefordert, ihre Mitarbeiter zu schulen, weil eine sichere IT alleine nicht ausreicht. Mit einer Live-Hacking-Performance hat das Institut für Internet-Sicherheit eine Möglichkeit gefunden, bei den Anwendern auf unterhaltsame Weise ein Verständnis für das Thema IT-Sicherheit zu erzeugen, indem live gezeigt wird wie Angriffe ablaufen.

IT-Sicherheit; Datensicherheit; Datenspionage; Unternehmenssicherheit; Internetforum; Hacking; Mobiltelefon; Computervirus; Passwort; Online-Banking; Szenario; Mitarbeiterinformation; Erfahrungsbericht; Sicherheitsbewusstsein

ID-nummer: 20110129

Priebe, Reinhard; Hartwig, Marc Arno

Cyberkriminalität und die neue Strategie der inneren Sicherheit für die Europäische Union

Kriminalistik, 2011, 2, S. 67-69
mit 13 QU

Das Bundeskriminalamt berichtete im Mai 2010, dass die Zahl der gemeldeten Fälle von Computer-, Internet- und Informationskriminalität 2009 um rund ein Drittel auf 50254 Delikte gegenüber dem Vorjahr gestiegen sei. Im selben Monat teilte das Bundesamt für Sicherheit in der Informationstechnik mit, dass Cyber-Angriffe eine neue Dimension der Gefährdung und zwar in Quantität und Qualität erreicht haben.
Die Europäische Union ist angesichts dieser Herausforderungen gefordert, ihren Beitrag zur Beseitigung der gewaltigen Probleme, vor die uns die Cyberkriminalität stellt, zu leisten.
In dem Beitrag werden die Maßnahmen skizziert, die auf europäischer Ebene getroffen wurden bzw. derzeit diskutiert werden, um der Bedrohung wirkungsvoll entgegenzutreten.
So ist die Europäische Kommission u.a. bestrebt, bis 2013 die Einrichtung eines Europäischen Cybercrime Centers voranzutreiben. Diese Einrichtung umfasst die Realisierung nationaler Meldeplattformen, über die im Internet verübte Straftaten angezeigt werden können, sowie die Verwirklichung einer europäischen Plattform, an die relevante Meldungen/Anzeigen von den Mitgliedsstaaten übersandt werden können.

Cybercrime; Cyberspace; Internetkriminalität; Kriminalitätsentwicklung; Gefahrenanalyse; Europäische Union; Europäische Kommission; Internationale polizeiliche Zusammenarbeit; Justitielle Zusammenarbeit

ID-nummer: 20110131

Heubrock, Dietmar; Böttcher, Max Hendrik

"Scamming" - Betrug durch vorgetäuschte Heiratsabsichten in Internet-Partnerschaftsportalen

Kriminalistik, 2011, 2, S. 75-81
mit 14 TAF, 2 QU

Die heute so selbstverständlichen Errungenschaften der digitalisierten Informationsgesellschaft haben nicht nur den Handel mit Waren bzw. die Handhabung von Geld revolutioniert und neue Kriminalitätsformen ("cyber crimes") hervorgebracht, sondern sie haben auch die zwischenmenschlichen Beziehungen grundlegend geändert. Nicht nur das scheinbar unverbindliche Chatten in Foren, Video-Chats oder die sehr populären Sozial Networks sind als Kommunikationsformen entstanden und haben wiederum neue Gefahren mit sich gebracht. Selbst die Partnersuche geschieht heute immer weniger in der realen und stattdessen zunehmend in der virtuellen Welt.
Der Beitrag informiert über eine weitgehend unbekannte Betrugsform, die sich in der Folge der Partner-Internetsuche in Internet-Portalen entwickelt hat, das "Scamming" (zu deutsch: Vorschussbetrug) oder der sog. Internet Love Scam". Damit ist eine Kontaktanbahnung unter Alias-Identitäten gemeint mit dem Ziel, von der Partner suchenden Person unter Angabe vorgetäuschter Gründe hohe Geldbeträge zu erschleichen. Im Grunde handelt es sich hierbei um die Internet-basierte Variante des früheren "Heiratsschwindlers"

Internetkriminalität; Internetforum; Chatprogramm; Kontaktpflege; Kontaktaufnahme; Betrug; Beziehungsdelikt; Identitätstäuschung; Geldtransfer

ID-nummer: 20110167

Benzmüller, Ralf

Ein Blick in die Höhle des Löwen; Underground Economy (Teil 1: Organisationsstruktur, Teil 2: "Waren" und "Dienstleistungen", Teil 3: Das Problem mit der "Beute")

IT-Sicherheit - Management und Praxis, 2011, 1, S. 68-69; 3, S. 63-65, 4, S. 64-66
mit 7 BILD

Lange vorbei sind die Zeiten, als die Hacker-Szene noch aus zumeist männlichen Heranwachsenden bestand, die aus Spaß und technischem Interesse im Netz unterwegs waren. Daher ist die Bezeichnung Hacker für die neue Generation, die sich in dieser "Underground Economy" bewegen, auch schlichtweg falsch. Es handelt sich bei ihnen um Verbrecher mit technischem Wissen, ohne Unterschied zu Tresorknackern oder anderen gewöhnlichen Kriminellen.
In dieser Untergrundwirtschaft findet man heute alles, was es auch in einer "richtigen" Wirtschaftsumgebung gibt: Hersteller, Händler, Dienstleister, "Betrüger" und die Kunden. Erhältlich ist alles, was das kriminelle Herz begehrt - von Kreditkarten über gefälschte Dokumente in jeder nur erdenklichen Ausführung, bis hin zum kompletten Skimming-Equipment für mehrere tausend Euro, um Datendiebstahl an Geldautomaten zu betreiben. Des Weiteren ist zu beobachten, dass immer mehr "professionelles" Equipment in den Untergrundforen gehandelt wird. Gemeint sind Dinge wie Kreditkartenrohlinge, die man im Wunschdesign bestellen kann. Die Preise reichen hier von rund 50 bis 150 Euro pro Kartensatz.
Der dreiteilige Aufsatz gibt einen Überblick über die Szene und ihre Strukturen, die gehandelten "Waren" und "Dienstleistungen" und die Liquidierung der "Beute". Dabei zeigt sich ganz eindeutig, dass es sich hier um keine harmlose Minderheit handelt, sondern um organisierte Betrüger und Diebe.

Cybercrime; Internetkriminalität; Hacking; Internetforum; Handeltreiben; E-Commerce; Online-Banking; Kreditbetrug; Spam-E-mail; Phishing; Schattenwirtschaft

ID-nummer: 20110289

Hsieh, Shuo Chun

E-Mail-Überwachung zur Gefahrenabwehr; Präventiv-polizeilicher Zugriff auf Internet-basierte Telekommunikation als neue polizeirechtliche Problematik im Digitalzeitalter am Beispiel der E-Mail-Überwachung zur Gefahrenabwehr

Schriften zum Recht der Inneren Sicherheit, 2011, Bd 17, 263 S.
mit LITVZ S. 245-263

Die allgemeinen Gefährdungslagen des Internets - wie z.B. die Verbreitung terroristischer Inhalte, von Kinderpornographie oder von Schadsoftware (Trojaner) - sind mit hinreichender Wahrscheinlichkeit geeignet, polizeiliche Schutzgüter zu schädigen. Dies hat zur Folge, dass die Polizei im Digitalzeitalter auch für die Abwehr von Gefahren zuständig ist, die aus der Nutzung des Internets resultieren. Der E-Mail-Verkehr stellt eine der wichtigsten und häufigsten Internet-basierten Telekommunikationsarten dar. Daher entwickelt sich die Problematik präventiver E-Mail-Überwachung zum Zwecke der Gefahrenabwehr zu einem zentralen Thema des aktuellen Polizeirechts.
Die Untersuchung behandelt systematisch die Rechtsfragen der präventiv-polizeilichen E-Mail-Überwachung. Der Verfasser berücksichtigt dabei insbesondere die landesrechtlichen Grundlagen dieser verdeckten polizeilichen Maßnahme zur Informationserhebung. Die Arbeit analysiert sowohl verfassungsrechtliche als auch verwaltungsrechtliche Zweifelsfragen.

Telekommunikation; Telekommunikationsrecht; Telekommunikationsüberwachung; Internet; Internetkriminalität; E-mail; Überwachungsbefugnis; Überwachungsmaßnahme; Polizeirecht; Präventivmaßnahme; Gefahrenabwehr; Gefahrenabwehrrecht; Ermächtigungsgrundlage; Grundrecht; Verfassungsrecht; Verwaltungsrecht

ID-nummer: 20110218

Schönbohm, Arne

Cybercrime und Cyberwar

CD Sicherheits-Management, 2011, 1, S. 90-95
mit 2 BILD

Estland wurde 2007, Georgien in 2008, Kirgisien in 2009 und Irans Nuklearprogramm im Jahr 2010 mit massiven Attacken aus dem Web konfrontiert. All diese Länder befanden sich zum jeweiligen Zeitpunkt in Konflikten mit anderen Ländern. Bei den Angriffen geht es darum, das gesellschaftliche und wirtschaftliche Leben innerhalb eines Staates zum Erliegen zu bringen und die Wirtschaft erheblich zu beschädigen. Inzwischen werden die Angriffe im Netz schon nicht mehr unter den Begriff Cybercrime gefasst - man spricht bereits von Cyberwar. Der Autor stellt Maßnahmen vor, um Risiken und Gefahren vorzubeugen.

Cybercrime; Internetkriminalität; Computervirus; Schadsoftware; Hacking; Sicherheitslage; Infrastruktur; Wirtschaftsspionage; Wirtschaftsschaden; Sicherheitsbehörde

ID-nummer: 20110020

Difraoui, Asiem El; Steinberg, Guido

Der Feind in unserem Netz; Wie bekämpft man Al-Kaida & Co. im virtuelle Raum?

Internationale Politik, 2011, 1, S. 20-25
mit 1 BILD, 6 QU

Mit der dschihadistischen Invasion des Internets ist es Al-Kaida & Co. gelungen, eine zweite Front im Kampf gegen den Westen und seine Verbündeten in der islamischen Welt zu eröffnen. E-Commerce, E-Science, E-Dschihad: Dass Dschihadisten die vielfältigen Möglichkeiten des Internets für ihre Zwecke nutzen würden, war vorhersehbar. Heute ist es praktisch unmöglich, ihre Präsenz im Netz zu zerstören - doch mit den richtigen Strategien kann der Verbreitung des E-Dschihads zumindest entgegengewirkt werden.
Es ist praktisch unmöglich, die dschihadistische Präsenz im Web komplett zu beseitigen. Das Propagandamaterial wird in rasanter Geschwindigkeit von Sympathisanten heruntergeladen und als E-Mail an hunderte Empfänger und Webseiten verschickt.

Internet; Terrororganisation; Al Quaeda; Cyberspace; Cyberterrorismus; Täterstrategie; Islamistischer Terrorismus; Medieneinfluss; Propaganda

ID-nummer: 20110130

Hube, Diana

Die Strafbarkeit des "Cyber-Groomings" - eine Betrachtung im Lichte gesellschaftspolitischer Forderungen

Kriminalistik, 2011, 2, S. 71-74
mit 30 QU

Sexualstraftaten an Kindern gehören zu den im höchsten Maße emotional besetzten strafrechtlichen Inhalten. Elektronische Kommunikationsformen via Internet bieten hier die Möglichkeit einfacher und anonymer Kontaktaufnahme für Erwachsene mit sexuellen Absichten, um bei einem späteren Treffen Missbrauchshandlungen zu begehen. Durch mediale Thematisierung dieser Gefahren wurde jüngst erneut die Debatte um die Strafbarkeit dieses sogenannten "Cyber-Groomings" ausgelöst. Ausgangspunkt ist hier der § 176 Abs. 4 Nr. 3 StGB, der im Jahre 2004 in das Strafgesetzbuch eingefügt wurde. Verbreiteter Ansicht nach kriminalisiert dieser die hier in Rede stehende Kontaktanbahnung in Internet-Chaträumen. Das ist jedoch nicht unbestritten und wird darüber hinaus im hohen Maße - sowohl grundsätzlich, als auch hinsichtlich der konkreten Normausgestaltung - kritisiert.
Der Beitrag versteht sich als Bestandsaufnahme und plädiert für einen nicht allzu schnellen und lauten Ruf nach einer weiteren Ausdehnung gesetzgeberischen Tätigwerdens.

Internetkriminalität; Chatprogramm; Kinderschutz; Kontaktaufnahme; Sexuelle Handlung; Sexueller Missbrauch von Kindern; Tatbestandsmerkmal; StGB P 176; StGB P 11 Abs 3; Vorfeldkriminalität

ID-nummer: 20110893

Holzberger, Mark

Wer gegen wen? Gremiendschungel zur Bekämpfung der Cyberkriminalität

Bürgerrechte & Polizei, 2011, 98, Nr. 1, S. 12-21
mit zahlr. QU

Im Februar 2011 beschloss die Bundesregierung ihre "Cyber-Sicherheitsstrategie für Deutschland". Diese will eine möglichst effektive Zusammenarbeit der Bundesbehörden unter Einbindung der Privatwirtschaft erreichen. Hierfür wurden drei Modelle entwickelt: Erstens wurde im Mai 2011 auf ministerieller Ebene ein "Nationaler Cyber-Sicherheitsrat" (NCSR) gebildet. Dieser soll "strukturelle" Fragen erörtern und "präventive" Instrumente bzw. zwischen Staat und Wirtschaft "übergreifende Politikansätze" koordinieren.
Zweitens hat auf Ebene der Bundesbehörden am 1. April 2011 das Nationale Cyber-Abwehrzentrum (NCA) seine Arbeit aufgenommen. Hier geht es um die "operative Zusammenarbeit staatlicher Stellen zur Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle".
Drittens wurde Ende März 2011 als einzige direkte Kooperationsplattform zwischen Sicherheitsbehörden und der Wirtschaft in diesem Kontext im Bundesministerium für Wirtschaft und Technologie die "Task Force IT-Sicherheit in der Wirtschaft" eingerichtet. Beteiligt sind neben BSI und BfV elf Unternehmen bzw. Dachverbände (wie der Industrie- und Handelskammertag). Die Task Force soll insbesondere kleine und mittlere Unternehmen für das Thema IT-Sicherheit "sensibilisieren".
Auf europäischer Ebene wurde 2010 die "Digitale Agenda für Europa" vorgelegt. Danach soll bis 2012 eine Plattform zur Bekämpfung der Cyberkriminalität eingerichtet und noch in diesem Jahr eine Durchführbarkeitsstudie für ein entsprechendes Europäisches Zentrum vorgelegt werden. Ferner will man die EU-weiten Einsatzübungen zur Cybersicherheit fortführen. Strategisches Ziel ist es, "international koordinierte Aktionen gegen Computerkriminalität und sicherheitsrelevante Angriffe gezielt durchführen" zu können.
Die Koordination der polizeilichen Bekämpfung von Cyberkriminalität in der EU erfolgt bis auf weiteres im Wesentlichen durch Europol. Hierfür hat Europol 2009 zunächst eine Europäische Cybercrime-Plattform (ECCP) eingerichtet.
Der Verfasser legt in dem Beitrag dar, warum seiner Ansicht nach, die Zirkel, in denen Polizei und Geheimdienste (aber auch Militärs) sich bundes- bzw. europaweit treffen, um ihren Kampf gegen die "Cyberkriminalität" zu koordinieren, unübersichtlich und intransparent sind.

Cybercrime; IT-Sicherheit; Cyberterrorismus; Sicherheitsstrategie; Koordinierungsstelle; Kooperationsprinzip; Sicherheitsbehörde; Privatwirtschaft; BSI; Bundeskriminalamt; Bundespolizei; Bundeswehr; Verfassungsschutz; Nachrichtendienst; Anlassunabhängige Recherche; Abwehrmaßnahme; Europäische Kommission; Europol

ID-nummer: 20110778

Franz, Reiner; Klatte, Michael

Süßes oder Saures?! Trends bei Malware und ihrer Abwehr

KES - Die Zeitschrift für Informations-Sicherheit, 2011, 4, S. 52-55

Sogenannte "Malware", also Schadprogramme wie Computerviren und "Trojaner", ist nach Einschätzung der Autoren eine stetige Bedrohung, die sich zunehmend auch auf Smartphones und andere zuvor weniger befallene Systeme ausbreitet. Die Autoren geben einen Überblick über die Lage und Ratschläge, um die eigene IT-Sicherheitssituation zu verbessern.

Schadsoftware; Computervirus; Abwehrmaßnahme; Mobiltelefon; Betriebssystem; Hacking; Netzwerk; Virensuchprogramm; Gefahrenlage; IT-Sicherheit; Checkliste

ID-nummer: 20110892

Monroy, Matthias; Busch, Heiner

Digitaler Untergrund; Kriminalisten und Kriminalisierte wetteifern im Web 2.0

Bürgerrechte & Polizei, 2011, 98, Nr. 1, S. 3-11
mit zahlr. QU

Im alle zwei Jahre publizierten "Threat Assessment an Internet Facilitated Organised Crime" (iOCTA) von Europol wird analysiert, wie das Internet als Kommunikationsmittel, Informationsquelle, Marktplatz, Ort zur Suche nach Gleichgesinnten und Finanzdienstleister dient. Im Focus von Europol stehen vor allem organisierte Kriminelle, die mit neuen digitalen Möglichkeiten ihre "offline organisierte Kriminalität" befördern: Herstellung von und Handel mit Drogen, Menschenhandel, Produktpiraterie, Steuerbetrug mit so genannten "Karussellgeschäften", Währungsfälschung, Waffenhandel oder Kinderpornografie. Online-Glücksspiele helfen laut Europol, das beschaffte Geld weltweit und damit schwer nachvollziehbar in geregelte Finanzströme zu überführen. Auch illegalisierte Migration wird laut Europol vom Internet begünstigt.
Das Internet hat spezifische neue Formen der Delinquenz hervorgebracht. Die Autoren befinden jedoch so unbezweifelbar das ist, so sicher ist auch, dass die polizeilichen und militärischen Warnungen insbesondere deshalb überzogen sind, weil sie Krieg, Terrorismus und Kriminalität, aber auch Hacker und demokratische Netzaktivistlnnen, die hier die Möglichkeit zur Offenlegung und Verbreitung staatlicher Geheimnisse sehen, zu einem ungenießbaren Brei verrühren.

Internet; Internetkriminalität; Cybercrime; Kriminalitätsphänomen; Deliktart; Bekämpfungskonzept; Bekämpfungsmaßnahme

ID-nummer: 20110890

Kargar, Darius

Einloggen in ungeschützte Funknetzwerke zur kostenfreien Internetnutzung - Keine strafrechtlichen Konsequenzen für so genannte "Schwarzsurfer"? Beschluss des LG Wuppertal vom 19.10.2010 - Az. 25 Qs 10 Js 1977/08 - 177/10, 25 Qs 177/10

Polizeispiegel, 2011, 9, S. 23-24
mit 1 BILD, 13 QU

Funknetzwerke bergen stets die Gefahr, dass sich unbefugte Dritte in das ungesicherte WLAN-Netz einwählen und zu Lasten des Inhabers des Funknetzwerkes kostenfrei surfen. Im Rahmen des Beschlusses des LG Wuppertal stellt sich die Frage, ob das Einwählen in ein kostenfreies Netzwerk ein strafrechtlich relevantes Verhalten darstellt.
Im Ergebnis wird festgestellt, dass ein Schwarzsurfer, der sich in ein ungesichertes WLAN-Netz eines Dritten einwählt, straffrei ausgehen dürfte.

Funknetz; IT-Sicherheit; Datensicherheit; Datenzugriff; Strafbarkeit; Rechtslage; Telekommunikationsnetz

ID-nummer: 20110819

Hellenthal, Markus

"Zukunft Sicherheit - und nun?" Vortrag auf der vom BDK mitveranstalteten Geldwäschetagung in der Thomas-Morus-Akademie in Bensberg [fing.]

Der Kriminalist, 2011, 9, S. 26-29
mit 1 BILD

Mit Blick auf die Rechtsstaatsgarantie und die Sorge von Bürgern in Zeiten komplexer und schwieriger werdender Bedrohungslagen geht es um die Frage, wie wir mit den stets verbleibenden Unsicherheiten umgehen, ohne einerseits Lähmung und andererseits in Panik zu verfallen.
Im Rahmen der Fachtagung stellt der Autor hierzu drei Thesen auf:
These 1 - Bewährte Strukturen und Architekturen können sich überleben.
These 2 - Wie erreichen wir Ressourceneffizienz?
These 3: Sicherheit neu und ganzheitlich denken.
Das bedeutet, eine zukunftgerichtete Sicherheitsarchitektur basiert auf einer nahtlosen Kommunikation und integrierten Zusammenarbeit öffentlicher und ggf. auch privater Sicherheitsorganisationen über bestehende geographische und organisatorische Grenzen hinweg. Dies setzt in Zeiten knapper Mittel einen effizienten und intelligenten Ressourceneinsatz voraus.

Sicherheitsarchitektur; Sicherheitspolitik; Sicherheitsbehörde; Kooperationsprinzip; Effizienzsteigerung; Rechtsstaatsprinzip; Kompetenzsteigerung; Gemeinsame Ermittlungsgruppe

ID-nummer: 20110163

Gaycken, Sandro

Krieg der Rechner; Warum es so schwierig ist, sich vor militärischen Cyberangriffen zu schützen

Internationale Politik, 2011, 2, S. 88-95
mit 2 BILD

Von Staaten getragene Übergriffe auf IT-Systeme werden immer zahlreicher, effizienter und gezielter. Eine Entwicklung mit gravierenden sicherheitspolitischen Konsequenzen, die sich mit konventionellen Schutzstrategien wie Abwehr und Abschreckung nicht beherrschen lässt. Warum die klassischen Schutzkonzepte versagen erläutert der Autor anhand der verantwortlichen Strukturprinzipien des Cyberwar. Er unterstreicht, dass eine solide Kenntnis der neuartigen Cyberkriege und ihrer Besonderheiten unerlässlich ist. Der Krieg der Rechner muss als neues Phänomen verstanden werden. Dazu gehört zunächst einmal die Einsicht in die strukturellen Besonderheiten und in die daraus folgende Notwendigkeit einer teilweisen "Entnetzung".

Cybercrime; Cyberterrorismus; Datenspionage; Datenmanipulation; Computervirus; Hacking; Informationstechnologie; IT-Sicherheit; Technikfolgenabschätzung; Nachrichtendienst; Militär; Staatskriminalität

ID-nummer: 20110688

Warnecke, Volker; Knabe, Oliver

Abofallen und Simlockentfernung; Ermittlungstaktische Erfahrungen und rechtliche Bewertung spezieller Formen der IuK-Kriminalität

Kriminalistik, 2011, 7, S. 448-453
mit 2 TAF, 32 QU

Das Tatmittel Internet bietet Tätern eine unüberschaubare Vielzahl neuer Möglichkeiten für kriminelle Aktivitäten. Die Gefahr liegt vor allem darin, dass solche Straftaten schneller, anonymer und mit wesentlich größerem "Opferpotential" begangen werden können. Die Fallzahlenentwicklung der letzten Jahre im Bereich der Computerkriminalität bzw. Vermögens- und Fälschungsdelikte mit dem Tatmittel Internet ist augenfällig. Die Bekämpfung der auf der Informations- und Kommunikationstechnik basierenden Kriminalität stellt somit seit Jahren einen stetig ansteigenden, bundesweiten Schwerpunkt der Ermittlungsarbeit der Polizei dar.
In dem Beitrag wird aus zwei Umfangsverfahren des Zentralen Kriminaldienstes Göttingen berichtet, die einige spezielle Vorgehens- und Verhaltensweisen dieser besonderen Täterklientel deutlich machen und die zu einem richtungweisenden Urteil des Landgerichtes Göttingen geführt haben.

Cybercrime; Internetkriminalität; Mobiltelefon; Computerbetrug; Betrug; Modus operandi; E-Commerce; Ermittlungstaktik; Ermittlungsverfahren; Tatbestand; Rechtslage; Gerichtsurteil

ID-nummer: 20101496

Dreo Rodosek, Gabi

Cyber Defence - Abwehr in der virtuellen Welt; Teil 1: Der Paradigmenwechsel - Teil 2: Überwachungsmöglichkeiten der Kommunikationsinfrastrukturen heute - Teil 3: Future Internet - neuen Technologien folgen neue Bedrohungen

IT-Sicherheit - Management und Praxis, 2010; 2011, 6, S. 60-61; 1, S. 66-67; 2, S. 60-61
mit 1 BILD

Unser Leben spielt sich zunehmend in der virtuellen Welt ab. Wir nutzen bereitwillig die Chancen und Möglichkeiten, die sich hier bieten - es ist aber auch höchste Zeit, den dort vorhandenen Gefahren zu begegnen. Cyber Defence, die Abwehr in der virtuellen Welt, ist ein Schlagwort, unter dem sich verschiedenste Ansätze subsumieren lassen, um Bedrohungen mit Mitteln der Informationstechnik entgegenzuwirken.
Im ersten Tei des Beitrags wird insbesondere auf den sich augenblicklich vollziehenden Paradigmenwechsel hinsichtlich der anzugreifenden Ziele eingegangen. Der daraus resultiert, dass vorhandene Bedrohungen aus der Informations- und Kommunikationstechnologie (IKT) in neue Gebiete wie beispielsweise Energieversorgung, Automobilindustrie oder industrielle Steuerungsanlagen Einzug halten.
Der Stand der Technik zur Erkennung von Cyber-Angriffen und die Überwachungsmöglichkeiten des heutigen Internets sind Gegenstand des zweiten Teils. Den Abschluss bildet ein Ausblick auf die Herausforderungen im Bereich der IT-Sicherheit im Internet der Zukunft. Es werden die Sicherheitsbedrohungen skizziert, die unter anderem als Konsequenz neuer Technologien, der hohen Mobilität sowie der immensen Anzahl und Heterogenität von vernetzten Geräten zu erwarten sind.

Cyberspace; Cybercrime; Informations- und Kommunikationstechnologie; Informationstechnologie; IT-Sicherheit; Infrastruktur; Gefahrenlage; Überwachungstechnik; Sicherheitssystem; Datennetz; Datensicherheit; Datensammlung; Datenanalyse; Schadsoftware; Verschlüsselungsverfahren; Cloud Computing; Technologische Entwicklung

ID-nummer: 20101205

Fabian, Ralf

Sicherheit in virtuellen IT-Welten; Identity Federation im Zeitalter des Cloud Computings

IT-Sicherheit - Management und Praxis, 2010, 5, S. 54-55
mit 1 TAF

Unbeantwortete Fragen zur IT-Sicherheit verhindern so manches Mal ein klassisches Outsourcing. Mit zunehmender Virtualisierung der Server, Speicher und Netzwerke in der Ära des Cloud Computings müssen die Fragen nach der IT-Sicherheit beantwortet werden. Hier kristallisiert sich das Konzept der "Identity Federation" als tragfähiger Kompromiss heraus, der die unterschiedlichen Sicherheitsinteressen von Unternehmen sowie von ihren Service-Providern und Kunden im E-Business unter einen Hut bringt.

IT-Sicherheit; Datensicherheit; Provider; Sicherheitsstandard; Vertrauensschutz

ID-nummer: 20101495

Hawellek, Christian; Jlussi, Dennis

Good Practice bei IT-Sicherheitsaudits; Security Tools vs. Computer-Strafrecht

IT-Sicherheit - Management und Praxis, 2010, 6, S. 50-51
mit 1 BILD

Für Unternehmen und deren Mitarbeiter in der IT-Sicherheit ist die Frage, ob ihr Handeln strafbar ist, existenziell. Dies gilt gleichermaßen für Kunden, denn professionelle IT-Sicherheitsaudits sind wichtiger Bestandteil des betrieblichen Informationsschutzes und nicht zuletzt des unternehmerischen Risikomanagements. Gerade realitätsnahe Simulationen von Angriffen unter Einsatz sogenannter "Hackertools" sind dabei wichtige Mittel zur Gewährleistung der Penetrationssicherheit. Der Umgang mit derlei Tools allerdings kann bereits gefährlich nah am Bereich der Strafbarkeit liegen. Was genau ist also strafbar - und wie lassen sich Strafbarkeitsrisiken minimieren?

Hacking; Schadsoftware; Computerspionage; Zweckbestimmung; Sicherheitsüberprüfung; Simulationsverfahren; Netzwerkanalyse; Einsatzbereich; Strafbarkeitsbedingung; StGB P 202 c; Datennetz; Einwilligung; Nutzanwendung

ID-nummer: 20101509

Fedtke, Stephen

Epische Macht; "Extremely Privileged IT Staff" (EPIS) erfordert spezielle Zuverlässigkeits- oder Sicherheitsüberprüfungen

KES - Die Zeitschrift für Informations-Sicherheit, 2010, 6, S. 6-8, 10-13
mit 1 BILD

Für volkswirtschaftlich und gesellschaftlich kritische, "systemrelevante" Unternehmen und Institutionen ist das mit besonders hoch privilegierten IT-Mitarbeitern (Extremely Privileged IT Staff, EPIS) verbundene Risiko aus Sicht des Autors inakzeptabel. Die EPIS-Mitarbeiter seien aufgrund ihrer faktischen Macht und hohen "Machtumsetzungsgeschwindigkeit" gesondert zu behandeln und ähnlich wie Piloten und Kernkraftwerksmitarbeiter auf ihre persönliche Zuverlässigkeit hin zu überprüfen. Das Fehlen solcher Prüfungen sei bei der heutigen Weltsicherheitslage, dem hohen Grad an technischer und servicebezogener Vernetzung und globaler Verteilung, dem hohen opportunistischen Zeitgeist sowie der Wichtigkeit einer permanent verfügbaren IT für eine funktionierende globalisierte Weltwirtschaft gesellschaftlich nicht hinnehmbar. Das Einführen einer Sicherheits- oder Zuverlässigkeitsüberprüfung für EPIS-Mitarbeiter müsste auch eine Validierung aussagekräftiger Indikatoren aus dem persönlichen Umfeld umfassen. Als Option oder Pflicht würde dies allen EPIS-relevanten Institutionen eine regelmäßige und standardisierte Risikoüberprüfung ihrer "mächtigen" IT-Mitarbeiter ermöglichen. Für die Mitarbeiter wäre dies umgekehrt ein wertvoller Entlastungsnachweis um die eigene Person. Cloud- oder Outsourcing-Kunden könnten mit Service-Anbietern eine EPIS-konforme Belegschaftsklassifizierung vertraglich festschreiben, Versicherungen könnten dies in ihren Prämien würdigen.

Unternehmenssicherheit; Mitarbeiterkriminalität; Spezialisierung; Risikofaktor; Computerspionage; Zugangskontrolle; Zugriffskontrolle; Sicherheitsüberprüfung; IT-Sicherheit

ID-nummer: 20101358

Hübert, Rainer

Business Resilience Management; Widerstandsfähigkeit von Unternehmen

Schriftenreihe der Plattform Menschen in komplexen Arbeitswelten e.V.,
Sicheres Handeln lernen - Kompetenzen und Kultur entwickeln -, 2010, S. 211-230
mit 5 TAF, 2 QU

Im hochentwickelten und vermeintlich sicheren Westeuropa stellt sich für Unternehmen selten die Frage, warum sie in die Krisen- und Katastrophenprävention und damit in die Widerstandsfähigkeit und Stabilität ihrer Organisation investieren sollten. Insbesondere vor dem Hintergrund, da sie seit vielen Jahren von keinen großen Naturkatastrophen heimgesucht wurden. Ein Blick auf die Zahlen der weltweit gemeldeten Naturkatastrophen und Katastrophen durch Technikversagen ergeben jedoch ein anderes Bild und raten zum Umdenken.
Vor diesem skizzierten Hintergrund stellt sich die Frage, welche Möglichkeiten haben Organisationen, sich gegen die Auswirkungen existenzbedrohender Katastrophen und Krisen zu schützen?
Als Antwort hat sich im vergangenen Jahrzehnt Business Resilience entwickelt: Ein ganzheitliches Konzept, das ein Unternehmen nicht nur darauf vorbereitet, umfangreiche, ungewollte und ungeplante Ressourcenverluste ohne existenzbedrohende Schäden für das Unternehmen wegstecken zu können. Bei Business Resilience geht es auch darum den ganzen Organismus "Unternehmen" so auszubilden, dass es auch dann eine ernsthafte Bedrohung übersteht, wenn es sich vorher nicht explizit darauf vorbereitet hat.

Unternehmensschutz; Unternehmenssicherheit; Unternehmerrisiko; Risikomanagement; Naturkatastrophe; Katastrophenschutz; IT-Sicherheit; Krisenmanagement; Managementsystem; Sicherheitsstandard; Sicherheitsmanagement

ID-nummer: 20100199

Hand in Hand zu mehr Sicherheit; Interview mit Udo Helmbrecht

KES - Die Zeitschrift für Informations-Sicherheit, 2010, 1, S. 6-8
mit 1 BILD

Seit 2004 gibt es die European Network & Information Security Agency (ENISA), die vorrangig für die Organe und Einrichtungen der Europäischen Union und ihrer Mitgliedstaaten tätig ist. Die ENISA ist "die Antwort der EU auf die Sicherheitsfragen der Europäischen Union" und soll daher auch generell eine Vorreiterrolle bei der Informationssicherheit in Europa einnehmen.
Seit Herbst 2009 ist der frühere BSI-Präsident Dr. Udo Helmbrecht Direktor dieser EU-Agentur, die heute mit keinem geringeren Ziel antritt als Europas Informationsgesellschaft zu sichern. Dazu stehen der Organisation rund 60 Mitarbeiter und ein jährliches Budget von rund 8 Mio. € zur Verfügung.
In dem Interview beschreibt Dr. Helmbrecht seine Ziele sowie aktuelle Chancen und Risiken der europäischen Informations-Sicherheit.

Europäische Union; Informationssicherheit; Informationsgesellschaft; Informations- und Kommunikationstechnologie; IT-Sicherheitskonzept; Sicherheitsaufgabe; Sicherheitsauftrag

ID-nummer: 20101203

Loomans, Dirk

BSI-Grundschutz in der Wolke; Cloud Computing im Lichte einer Bundesbehörde

IT-Sicherheit - Management und Praxis, 2010, 5, S. 45-47
mit 1 BILD, 3 QU

Datenverarbeitung durch Dritte ist immer ein heikles Thema. Es müssen organisatorische Regelungen getroffen werden, wenn Daten im Auftrag verarbeitet werden. Das Anmieten von Cloud-Services fällt unter den Begriff Outsourcing-Vorhaben, für das der Grundschutz Gefährdungen und Maßnahmen kennt. Service Level Agreements, die die Sicherheitsleistung des Providers eindeutig festlegen, sollten vereinbart werden. Wenn darüber hinaus die Verarbeitung personenbezogener Daten ausgelagert wird, ist ein wichtiges Datenschutz- und Informationssicherheits-Kriterium betroffen, denn gemäß §11 Abs. 1 S. 1 BDSG ist grundsätzlich der Cloud-Kunde für seine ausgelagerten Daten verantwortlich:
Tatsächlich jedoch ist das Thema Cloud Computing noch nicht explizit in die Maßnahmen- und Gefährdungskataloge des BSI aufgenommen. Dies bedeutet aber nicht, dass der Grundschutz automatisch als Sicherheitsstandard für das Cloud Computing entfällt. Vielmehr hat das BSI hierfür einen Leitfaden auf Basis des IT-Grundschutz (BSI-Standard 100-3) herausgegeben, der eine umfassende Risikoanalyse auch für ein solch komplexes Thema wie das Cloud Computing erlaubt.

Öffentliche Verwaltung; IT-Sicherheit; Informationstechnologie; Personendaten; Datensicherheit; Outsourcing; BSI; Risikoanalyse; Sicherheitsstandard

ID-nummer: 20101359

Bargstedt, Uwe

Human Factors im Rechenzentrum; Lernen für sicheres Change Management in der IT

Schriftenreihe der Plattform Menschen in komplexen Arbeitswelten e.V.,
Sicheres Handeln lernen - Kompetenzen und Kultur entwickeln -, 2010, S. 231-255
mit 3 TAB, 1 TAF, LITVZ S. 253-255

Der IT-Betrieb im Rechenzentrum (RZ) ist kein klassisches Hochrisikoumfeld. Die Risiken im RZ betreffen weniger dessen Umgebung als vielmehr die IT-gestützten Geschäftsprozesse im Unternehmen. IT-Störungen geschehen trotz redundantem Technikeinsatz und verursachen hohe finanzielle Schäden. Durch das IT-Change Management können Fehler implementiert werden, die zeitlich verzögert die IT-Verfügbarkeit einschränken. Aufgrund der skizzierten hohen Kosten von IT-Stillständen (downtime) lohnt sich ein gewisser Aufwand bei der Optimierung der IT-Produktionsprozesse. Die Bedeutung des Humanfaktors ist dabei bisher nicht ausreichend gewürdigt worden. Im Artikel wird das Konzept der "Gemeinsamen Achtsamkeit" aus der High Reliability Theory auf das Change Management im IT-Betrieb angewendet. Es ergeben sich Hinweise für das individuelle, teambezogene und organisationale Lernen im Rechenzentrum.

Informationstechnologie; Kommunikationstechnologie; IT-Sicherheit; IT-Sicherheitskonzept; Rechenzentrum; Sicherheitsanalyse; Sicherheitsgewährleistung; Change Management; Fehlermanagement

ID-nummer: 20101157

"Wer die Kosten nicht scheut, kann sich sicher fühlen"; Kritische Infrastruktur "Internet"; Interview Claus Schaffner - Holger Skurk

WIK - Zeitschrift für die Sicherheit der Wirtschaft, 2010, 5, S. 12-15
mit 2 TAF, 1 QU

Mitte letzten Jahres hatte das Bundeskabinett die „Nationale Strategie zum Schutz kritischer Infrastrukturen“ (KRITIS) verabschiedet. Eines ihrer Hauptziele ist dabei der Schutz der Informationsstrukturen gegen Störungen und Ausfällen, ob technischer Natur oder durch gezielte Angriffe. Eine Lebensader dieser Strukturen ist das Internet und technische Störungen gibt es auch hier. Unmittelbar von Ausfällen betroffen wären Unternehmen, die am Tropf des Internets hängen. Es ist davon auszugehen, dass Provider oder etwa Internetunternehmen sich ausreichend vor Ausfällen geschützt haben, doch wie steht es um die Aufrechterhaltung des Geschäftsbetriebs von „Nicht-IT“-Unternehmen?
Claus Schaffner hat sich für WIK zu diesem Thema mit Holger Skurk, BITKOM, unterhalten.

Kritische Infrastruktur; Informationstechnologie; Cybercrime; Internet; Sicherheitsmaßnahme; Gefährdungsgrad; Wirtschaftsunternehmen

ID-nummer: 20100998

Hickisch, Kurt

"Tatort Internet" - BDK und fachkundige Referenten zeigen auf der Fachtagung Kripo Inter Wege zur Bekämpfung der Internetkriminalität auf

Der Kriminalist, 2010, 7-8, S. 17-19
BDK-Fachtagung Tatort Internet; 6. General Police Equipment Exhibition & Conference - GPEC, Leipzig; BR Deutschland, 2010 [04.05.-05.05.]
mit 5 BILD, 2 QU

Das Internet hat sich zum größten Tatort entwickelt", stellte der sächsische Staatsminister des Innern, Markus Ulbig, in seinem Grußwort bei der Eröffnung der vom Bund Deutscher Kriminalbeamter am 04.05. und 05.05.2010 in der Messe Leipzig im Rahmen der GPEC veranstalteten Fachtagung "Tatort Internet" fest. Über das Internet werden gezielte Angriffe auf Unternehmen und Regierungen durchgeführt, über soziale Netzwerke werden Opfer bis zum Mord gesucht, Menschen zu Terroristen ausgebildet und Anleitungen zum Selbstmord gegeben. Der Nutzer bedenkt zu wenig, dass potenziell eine Milliarde Menschen eine über das Internet geführte Kommunikation mitverfolgen könnten.
Der Autor berichtet über die einzelnen Vorträge der Tagung.

Internet; Internetkriminalität; Internetforum; Soziales Netzwerk; Bekämpfungsmaßnahme; Präventionsprojekt; Strafverfolgung; Strafverfolgungsmaßnahme; Rechtshilfeverfahren

ID-nummer: 20101154

Kreitlow, Jörn

Strategie zur Bekämpfung der IuK-Kriminalität

Die Polizei, 2010, 10, S. 290-296
mit 2 BILD, 14 QU

Informations- und Kommunikationskriminalität hat sich in ihrer Phänomenologie in den vergangenen Jahren stark verändert. Durch eine zunehmende Technisierung der globalen Gesellschaft und der damit verbundenen nahezu flächendeckenden Nutzung moderner Medien und Kommunikationsformen haben diese auch Einzug in klassische, teilweise seit Jahrzehnten existierende Phänomenbereiche gehalten. Es besteht dringender Handlungsbedarf sowohl auf Seiten der Sicherheits- und Strafverfolgungsbehörden als auch bei allen anderen staatlichen und privaten Institutionen, nicht zuletzt um einem drohenden Vertrauensverlust in dieses zukunftsträchtige Medium entgegenzuwirken. Eine wirksame Strategie zur Bekämpfung der IuK-Kriminalität muss daher alle betroffenen Akteure (Sicherheits- und Strafverfolgungsbehörden, Justiz, Wirtschaft, Verbände, Wissenschaft und Forschung), deren Sichtweisen des Problemfeldes sowie deren Handlungsmöglichkeiten einbeziehen. Eine Bund-Länder-Projektgruppe (BLPG) der Kommission Kriminalitätsbekämpfung (KKB) hat daher strategische Ziele und Handlungsempfehlungen entwickelt, mit deren Umsetzung die IT-Sicherheit und die Bekämpfung der IuK-Kriminalität in Deutschland spürbar verbessert werden können. Die Ausführungen geben inhaltlich die wesentlichen Ergebnisse der Bund-Länder Projektgruppe wieder, an der unter Vorsitz und Geschäftsführung des Bundeskriminalamtes (BKA) die Länder Baden-Württemberg, Berlin, Hamburg, Niedersachsen, Nordrhein-Westfalen und Sachsen vertreten waren. Der Bericht der Projektgruppe und die darin enthaltenen Handlungsempfehlungen wurden durch die polizeilichen Gremien zur Kenntnis genommen und für geeignet gehalten, dem Phänomen Cybercrime entgegenzuwirken. Die Handlungsempfehlungen befinden sich in der Umsetzung.

Cybercrime; Phänomenologie; Phishing; E-Commerce; Bekämpfungsstrategie; Ermittlungsarbeit; Ermittlungsführung; IT-Sicherheit; Informationsaustausch; Sicherheitsbehörde; Strafverfolgungsbehörde; Grenzüberschreitende Zusammenarbeit; Präventivmaßnahme; Handlungsempfehlung

ID-nummer: 20101201

Klügel, Christian

Recht und Unrecht im Kampf gegen Spam; Spam verhindern = Rechtsschutz mindern?

IT-Sicherheit - Management und Praxis, 2010, 5, S. 20-21
mit 1 BILD, 9 QU

Im rechtlichen Sinne bezeichnet Spam unerwünschte E-Mails, die zumeist werbenden Inhalts sind und massenhaft versandt werden. Gerade in Unternehmen potenzieren sich die Auswirkungen von Spam durch verschiedene Faktoren derartig, dass die Tauglichkeit der E-Mail als Kommunikationsmedium in Frage steht. Ein Unternehmen kann primär durch den Einsatz von Spam-Filtern seinem Interesse an IT-Sicherheit, einem reibungslosen Betriebsablauf und einem möglichst geringen Administrationsaufwand gerecht werden.
Die Implementierung von E-Mail-Filtern in Unternehmen kann jedoch auch zu einer Verletzung des Fernmeldegeheimnisses gemäß § 206 Abs. 2 Nr. 2 StGB sowie zu einer unzulässigen Datenunterdrückung gemäß § 303a Abs. 1 StGB führen. Management und leitende Angestellte, also Geschäftsführung, sowie Systemadministratoren laufen bei rechtswidriger Filterung, auch wenn die Aufgabe delegiert wurde, wegen § 14 StGB immer Gefahr, der Strafverfolgung ausgesetzt zu sein. Empfohlen wird Einführung einer unternehmensinternen Filterlösung, die im Einvernehmen mit den Mitarbeitern und/oder mit dem Betriebsrat einzurichten ist und in deren Planung der Datenschutzbeauftragte frühzeitig einbezogen wird.

Spam-E-mail; Sicherheitsmaßnahme; IT-Sicherheit; Fernmeldegeheimnis; StGB; Datenschutzrecht

ID-nummer: 20101070

Prof. Dr. Schmidbauer, Polizeipräsident von München, beantwortet kriminalpolitische und kriminalpolizeiliche Fragestellungen; Interview Ralf Gaßner - Wilhelm Schmidbauer

Der Kriminalist, 2010, 9, S. 19-26
mit 1 BILD

Die Interviewpartner thematisieren Bürgerrechte und Freiheit, Vorratsdatenspeicherung, Online-Durchsuchungh, Straftaten im Internet, Computerkriminalität, Wirtschaftskriminalität, polizeiliche Gefahrenabwehr, grenzüberschreitende Zusammenarbeit, Schleierfahndung, die bayerische Polizei und die polizeiliche Öffentlichkeitsarbeit.

Polizeiarbeit; Polizeibefugnis; Polizeirecht; Bürgerrecht; Freiheit; Rechtslage

ID-nummer: 20101063

Anonym

Lagebericht zur Informations-Sicherheit

KES - Die Zeitschrift für Informations-Sicherheit, 2010, 4, S. 26-30, 32-34; 5, S. 12-16, 18-20; 6, S. 14-21
mit 26 TAB, 23 TAF

Nur selten findet man verlässliche und neutrale Zahlen zur Informations-Sicherheit im deutschsprachigen Raum - noch seltener konkrete Angaben zu aufgetretenen Schäden und Budgets. Die Grundlage für die vorliegenden Daten haben in den vergangenen Monaten 135 Teilnehmer an der diesjährigen <kes>/Microsoft-Sicherheitsstudie im Rahmen einer selbstkritischen Bestandsaufnahme durch die Arbeit mit dem Studien-Fragebogen gelegt.
Der erste Teil der Auswertung befasst sich vor allem mit der aktuellen Risikosituation. Im zweiten Teil geht es überwiegend um Strategie und Management der Informationssicherheit sowie Kenntnisstand und Weiterbildung. Der dritte und letzte Teil der Auswertung behandelt konkrete Maßnahmen zur Informationssicherheit sowie die Nutzung von Dienstleistungen.
Die Kernaussagen der jeweiligen Abschnitte werden zusammengefasst.

Informationssicherheit; IT-Sicherheit; Datensicherheit; Sicherheitsmangel; Sicherheitsmanagement; Sicherheitsmaßnahme; Sicherheitsrisiko; Unternehmenssicherheit; Wirtschaftsspionage; Sabotage; Hacking; Computervirus; Wirtschaftsschaden; Schadensereignis; Schwachstellenanalyse; Untersuchungsergebnis

ID-nummer: 20100997

Tun Hussein, Dato Seri Hishammuddin

Internetkriminalität in einer globalen Welt - Rede des malaysischen Innenministers auf der BDK-Fachtagung Kripo Inter

Der Kriminalist, 2010, 7-8, S. 14-16
BDK-Fachtagung Tatort Internet; 6. General Police Equipment Exhibition & Conference - GPEC, Leipzig; BR Deutschland, 2010 [04.05.-05.05.]

In seiner Rede auf der BDK-Fachtagung Kripo International verdeutlichte der malaysische Innenminister seine Sicht auf die Bedrohungen durch die Internetkriminalität. Dabei sprach er auch Kriminalitätsphänomene wie den internationalen Terrorismus, Menschenhandel und Kinderpornografie an und unterstrich, dass globale Kooperation und regionale Koordination der richtige Weg ist, die Kriminalität des einundzwanzigsten Jahrhunderts zu bekämpfen - denn globale Probleme bräuchten globale Lösungen.

Internetkriminalität; Globalisierung; Neue Technologie; Gesellschaftlicher Wandel; Internationale Kriminalität; Internationale Sicherheit

ID-nummer: 20100870

Sicherheit ist eine Führungsaufgabe; Interview Dirk Loomans - Stefan Mutschler

IT-Sicherheit - Management und Praxis, 2010, 3, S. 13-16
mit 2 BILD

Loomans & Matz hat sich darauf spezialisiert, Unternehmen und Behörden bei der Konzeption und Umsetzung einer effektiven und kostengerechten Sicherheit in ihrer Organisation zu unterstützen. Wichtige Eckpfeiler dabei sind Managementsysteme für Informationssicherheit, Datenschutz und das Business Continuity Management.
IT-SICHERHEIT sprach mit Dr. Dirk Loomans, verantwortlich für den Bereich Informationssicherheit, über aktuelle Herausforderungen und Chancen im Zusammenhang mit ISM-Systemen.

Informationssicherheit; IT-Sicherheit; Unternehmensschutz; Unternehmenssicherheit; Unternehmensberatung; Spionageabwehr; Sicherheitsmanagement

ID-nummer: 20100431

Schneider, Heiko

Das Internet als Strukturelement des modernen Terrorismus

Polizei-heute, 2010, 2, S. 38-43
mit 1 BILD, 56 QU

Berichte über die Nutzung des Internets durch terroristische Organisationen sind in der heutigen Zeit fester Bestandteil der nationalen wie internationalen Presse- und Medienlandschaft. Die Instrumentalisierung des World Wide Web und sonstiger Internetdienste zu Zwecken terroristischer Propaganda, Rekrutierung, Radikalisierung und Anschlagsplanung ist angesichts veränderter terroristischer Strukturen und einer globalen Reichweite dieses Mediums nach wie vor besonders Besorgnis erregend. Nach den versuchten Bombenanschlägen auf deutsche Regionalzüge im Sommer 2006, bei denen die Täter auf Internet-Bauanleitungen zurückgriffen, setzten auf allen Ebenen fortwährende Diskussionen um eine bessere Bekämpfung terroristischer Aktivitäten im Internet ein. Hier anknüpfend gibt dieser Beitrag zunächst einen phänomenologischen Überblick um den staatlichen Handlungsbedarf zu verdeutlichen. Im Weiteren wird dann auf wesentliche Problemfelder der Ermittlungsarbeit, aktuelle sicherheitspolitische Initiativen sowie Erfolg versprechende Kontroll- und Ermittlungsansätze eingegangen.

Internet; Kommunikationsmittel; Internationaler Terrorismus; Netzwerk; Ideologie; Propaganda; Sicherheitspolitik; Sicherheitsbehörde; Medienverantwortung; Cyberterrorismus; Ermittlungsarbeit

ID-nummer: 20100730

Ulbig, Markus

Tatort Internet - Kriminalitätsbekämpfung am Scheideweg - Ausbildungsoffensive zur Kripo 2.0 ohne Alternative; Grußwort des Staatsministers Markus Ulbig, Innenministerium des Freistaates Sachsen

Der Kriminalist, 2010, 6, S. 11-12
BDK-Tagung kripo-inter 2010, Leipzig; BR Deutschland, 2010 [04.05.]
mit 1 BILD

Das Internet hat sich mit zunehmender Verbreitung zum größten Tatort weltweit entwickelt. Es befördert Kriminalität in den Bereichen Kinderpornografie, Verbreitung fremdenfeindlicher und rassistischer Inhalte und Verletzung der Rechte des geistigen Eigentums. Zudem hat das Internet auch ganz neue Kriminalitätsphänomene aufkommen lassen, wie etwa im Bankenbereich. Aufgrund der Anonymität und der weltweiten Vernetzung gestaltet sich die Strafverfolgung oft besonders schwierig. Handlungsansätze für den Staat liegen zum einen in einer besseren Aufklärung der Bürger über die Gefahren im Netz, zum anderen in einer umfassenden Fortbildung der Polizei und Sicherheitsbehörden.

Internet; Internetkriminalität; Erscheinungsform; Polizeiarbeit

ID-nummer: 20100995

Wer schlau ist, leistet sich gut bezahlte Hacker...; Interview Gunnar Porada - Claus Schaffner

WIK - Zeitschrift für die Sicherheit der Wirtschaft, 2010, 4, S. 29-30

Das Besondere am "Google-Hack" war nur die öffentliche Wirkung. Experten gehen davon aus, dass Angriffe dieser Qualität mittlerweile tagtäglich geschehen - sie fallen nur nicht auf, denn Unternehmen und Organisationen machen es staatlichen und privaten Hackern viel zu leicht, meint Hacking-Experte Gunnar Porada im Gespräch mit WIK-Mitarbeiter Claus Schaffner. Wer genau genug hinsieht, wird zu jedem gegebenen Zeitpunkt die Datenspuren von Hack-Attacken, Wirtschaftsspionage-Versuchen und auch staatlichen Cyber-Schnüfflern finden

Hacker; Hacking; Unternehmensschutz; IT-Sicherheit

ID-nummer: 20100592

Knop, Katharina von

Risiken beherrschen - Chancen nutzen; Lösungen zum nachhaltigen Schutz der Unternehmenswerte von Banken

IT-Sicherheit - Management und Praxis, 2010, 2, S. 24-27
mit 4 TAF

In der Entwicklung von Straftaten und Schadensereignissen bei Banken lassen sich derzeit vier Trends identifizieren.
1. Trend: Zunahme der wirtschaftskriminellen Handlungen (Betrug, Unterschlagung, Datendiebstahl, Industriespionage, Korruption)
2. Trend: Zunahme der Reputationsschäden, die durch Straftaten und Schadensereignisse erlitten werden
3. Trend: Zunahme der öffentlichen Sensitivität für Schadensereignisse bezogen auf Compliance-Vorfälle und Missbrauch personenbezogener und sensitiver unternehmerischer Daten
4. Trend: Loyalität der Mitarbeiter hat abgenommen und Mitarbeiterfluktuation hat zugenommen.
Eine Lösung der Missstände besteht in der Ausgestaltung der Konzernsicherheit. Auf der Grundlage der gesetzlichen und aufsichtsrechtlichen Vorschriften wird eine Konzernsicherheitsstrategie entwickelt, die konsequent die Inhalte der Geschäftsstrategie, der Risikostrategie, der IT-Strategie und der Personalstrategie fortgeschreibt. Die Konzernsicherheitsstrategie wird in den Strategieprozess der Bank implementiert. Nur so können Geschäftsziele optimal unterstützt und primäre Unternehmenswerte geschützt werden.

Bankpersonal; Bankwesen; Unternehmenssicherheit; Unternehmenskriminalität; Risikomanagement; Risikoanalyse; Compliance; Strategieentwicklung; Sicherheitskonzept; IT-Sicherheit

ID-nummer: 20100432

Schneider, Heiko

Terrorismus im Internet: Kontroll- und Ermittlungsansätze

Polizei-heute, 2010, 2, S. 44-50
mit 3 BILD, 40 QU

Im Zeitalter moderner Kommunikation stehen die Sicherheitsbehörden vor neuen Herausforderungen. Eine ist zweifelsohne die Kanalisierung terroristischer/extremistischer Aktivitäten im World Wide Web. Mit Einrichtung des Gemeinsamen Internetzentrums als Kooperationsplattform verschiedener Sicherheitspartner befindet sich Deutschland auf einem vielversprechenden Weg, das schier unbeherrschbare Internet gerade vor dem Hintergrund der Terrorismusabwehr ein Stück weit "sicherer" zu machen, wenngleich auch ein hundertprozentiger Schutz vor einer Instrumentalisierung des Mediums durch islamistische Terroristen nicht zu erreichen sein wird.
Für die Zukunft gilt allerdings, die eingeleiteten Bemühungen im Kampf gegen den Internetterrorismus grenzüberschreitend zu bündeln, fortzuführen und damit den terroristischen Organisationen ein wesentliches logistisches Instrument streitig zu machen. Dies muss allerdings im Bewusstsein dessen geschehen, dass verstärkte Kontrollmaßnahmen auch zu einem Wettlauf zwischen Sicherheitsbehörden und Fanatikern führen wird. Zudem ist im Spannungsverhältnis Freiheit und Sicherheit ein besonderes Augenmaß sowie eine gesunde Balance zwischen einer zweifelsohne notwendigen Kontrolle und der damit einhergehenden Begrenzung persönlicher Freiheitsrechte vonnöten.

Internet; Internationaler Terrorismus; Cyberterrorismus; Netzwerk; Kommunikationsmittel; Ermittlungsansatz; Ermittlungsarbeit; Sicherheitsbehörde; Früherkennung; Überwachungsmaßnahme; Interpol; Europol; Gemeinsames Terrorismusabwehrzentrum; Internationale Zusammenarbeit; TKG

ID-nummer: 20100220

Schulz, Sönke E.

Cloud Computing in der öffentlichen Verwaltung?

Verwaltung & Management, 2010, 1, S. 36-41
mit LITVZ S. 40-41

"Cloud Computing" - so heißt ein Trend der Informations- und Kommunikationstechnologie. Noch wird seitens der öffentlichen Verwaltung kaum auf dieses neue Angebot zurückgegriffen. Aufgrund der angespannten Haushaltslage und der mit der Nutzung einer "Cloud" verbundenen Einsparpotentiale sicher aber eine verlockende Option, allerdings verbunden mit spezifischen Rechtsfragen des Einsatzes im öffentlichen Sektor. Die Einsatzoptionen werden skizziert - verbunden mit der Vision einer privaten "Cloud" in Verantwortung der öffentlichen Hand, die beispielsweise kaum datenschutzrechtlichen Bedenken unterliegt. Bereitgestellte Software nutzt der Anwender in der Regel webbasiert, wodurch z.B. auch die Möglichkeit eröffnet ist, Dokumente mit einem weltweiten Nutzerkreis kollaborativ zu bearbeiten. Cloud computing besteht im Wesentlichen aus den Komponenten "Infrastucture as a Service", "Software as a Service" und "Platform as a Service"" und kann definiert werden als gemeinsame Nutzung von Hard- und Software- sowie Rechenkapazitäten, die nicht mehr lokalisierbar, sondern weltweit auf verschiedenen Servern nachfrage- und einzellfallabhängig zur Verfügung gestellt werden. Cloud Computing ermöglicht eine Reduktion der Kosten. Trotz Cloud Computing bleibt eigenverantwortliche Aufgabenerledigung möglich. "Cloud Computing" - Virtualisierung als Herausforderung für den Datenschutz. Ein Shared-Services-Center für IT hat Vorteile für die öffentliche Verwaltung.

Öffentliche Verwaltung; Informationstechnologie; Kommunikationstechnologie; Dienstleistung; IT-Sicherheit; Datenschutz; EDV-Anlage; EDV-Einsatz; Dezentralisierung; Modernisierung; Zukunftsorientierung; Hardware; Infrastruktur

ID-nummer: 20100054

Henrichs, Axel; Wilhelm, Jörg

Polizeiliche Ermittlungen in sozialen Netzwerken; Neue Antworten auf neue Herausforderungen?

Kriminalistik, 2010, 1, S. 30-37
mit 2 TAF, 3 TAB, 46 QU

Das Internet stellt sich heute als Informations-, Kommunikations- und Handelsplatz dar, das Generationen übergreifend genutzt wird. Neue Geräte und variablere Nutzungsmöglichkeiten befeuern neben dem zügigen Ausbau der Netzinfrastruktur zudem kontinuierlich die Verbreitung dieser Neuen Medien. Die Technik steht an der Schwelle zu einem "New Generation Network", in dem jedem Teilnehmer an jedem Ort sämtliche Nutzungsmöglichkeiten kostengünstig zur Verfügung stehen. Durch die Verbreitung der Social Network Services (SNS) haben sich neben den polizeilichen Datenbeständen zahlreiche von Privaten für eigene Zwecke betriebene "Datenbanken" etabliert. Darin sind umfangreiche personenbezogene Daten mit Zustimmung der Betroffenen enthalten, die überwiegend öffentlich zugänglich sind. In der virtuellen Welt des Internet findet vieles von dem statt, was auch in der realen Welt auf strafbare Handlungen bzw. Gefahrenlagen hinweist. Dementsprechend finden sich zahlreiche für die Polizei relevante Spuren. Die Kombination der in den polizeilichen DV-Systemen gespeicherten Datenbestände mit den Daten in den SNS ergibt einen taktischen und operativen Mehrwert von erheblichem Ausmaß. Die rechtliche Einordnung der "neuen Ermittlungsmaßnahmen" ist zwangsläufig noch relativ unbestimmt. Sie bemisst sich nach den Befugnisnormen der Repression (StPO) und Prävention (POG) sowie den Öffnungsklauseln des TKG und TMG. Das BVerfG hat in seiner wegweisenden Entscheidung relativ niedrigschwellige Kriterien für Grundrechtseingriffe festgelegt. Das geltende Recht beinhaltet neben zahlreichen Ermächtigungen jedoch auch Regelungslücken in Repression und Prävention. Künftig wird auch zu klären sein, wie einzelne Problemstellungen, z.B. der Begriff der Öffentlichkeit, der polizeiliche "Zutritt" zu den Netzwerken oder das verdeckte Vorgehen praxisorientiert und (verfassungs-)rechtlich belastbar aufgelöst werden können.

Internet; Internetforum; Netzwerk; Neue Medien; Informationssystem; Cybercrime; Kriminalitätsbild; Kriminalitätsphänomen; Tatmittel; Polizeiarbeit; Strafverfolgung; Polizeiliche Ermittlung; Deliktart; Ermittlungsarbeit; Eingriffsrecht; Grundrechtseingriff; Informationsgesellschaft; Kommunikationsform; Kommunikationsnetz; Konsumhäufigkeit; Konsumverhalten; Medienkonsum; Medieneinfluss; Personendaten; Rechtsgrundlage

ID-nummer: 20100011

Cranor, Lorrie Faith

Computer an der Angel; Um sensible Daten wie Passwörter und Bankverbindungen im Internet auszuspähen, setzen Kriminelle auf raffinierte Techniken - und auf einen naiven Umgang der Nutzer mit elektronischer Post

Spektrum der Wissenschaft, 2010, 1, S. 90-95
mit 3 BILD, 3 TAF

Als Phishing bezeichnet man das Ausspähen sicherheitsrelevanter Informationen wie Passwörter oder Bankverbindungen. Phisher verleiten ihre Opfer durch fingierte Mails dazu, sensible Daten in Abfragemasken einzugeben. Alternativ versuchen sie, deren Computer mit Spionagesoftware zu infizieren. Da Phishing menschliche Schwächen ausnutzt, verspricht eine Kombination von Schulung und anerkannter Sicherheitssoftware den besten Schutz.

Phishing; IT-Sicherheit; Internet; Cybercrime; Deliktart; Datendiebstahl; Datenmissbrauch; Trainingsprogramm; Bekämpfungsansatz

ID-nummer: 20100203

Fischer, Daniel

WLAN-Sicherheit in deutschen Unternehmen und Behörden

KES - Die Zeitschrift für Informations-Sicherheit, 2010, 1, S. 66-70, 72
mit 5 TAF, 1 TAB, 9 QU

Wireless Local-Area-Networks (WLANs) gehören mittlerweile in vielen Unternehmen und Behörden zum Standard. WLANs ermöglichen höhere Mobilität, mehr Flexibilität und sind im Vergleich zu drahtgebundenen Vernetzungen schneller und kostengünstiger zu implementieren. Der größte Kritikpunkt an WLANs ist ihre oft mangelhafte Sicherheit.
Eine aktuelle Studie der TU Ilmenau hat die Sicherheit von Wireless Local-Area-Networks (WLANs) in deutschen Unternehmen und Behörden untersucht. Ziel dieser empirischen Untersuchung war es herauszufinden, welche Maßnahmen deutsche Unternehmen und Behörden zur Sicherung ihrer WLANs aktuell einsetzen. Des Weiteren wurde ermittelt, warum Maßnahmen nicht genutzt werden und welche Zusammenhänge es zwischen unternehmensspezifischen Merkmalen und der Bekanntheit sowie dem Einsatz einzelner Sicherheitsmaßnahmen gibt.
Der Autor stellt die wesentlichen Ergebnisse der Studie vor.

Informationstechnologie; Informationstechnik; IT-Sicherheit; Datensicherheit; Sicherheitsmaßnahme; Sicherheitsmanagement; Verwaltungsbehörde; Unternehmen

ID-nummer: 20100201

Anonym

Malware-Trends - Bedrohung; Von dünnem Eis und dicken Fischen

KES - Die Zeitschrift für Informations-Sicherheit, 2010, 1, S. 58-60
mit 1 BILD

Dass Windows 7 heuer sowohl gesteigerte Marktanteile als auch neue Sicherheitslücken und Angriffe erfahren wird, dürfte selbstverständlich sein - doch auch verbreitete Client-Software bleibt im Fokus: Die Hauptursache für Malware-Attacken im Jahr 2010 werden Sicherheitslücken in beliebten Programmen sein. Diese Lücken werden sowohl bei Windows 7 auftauchen als auch in Fremdsoftware, wie den Programmen von Adobe oder Apple. Aufgrund der Popularität von Adobe-Anwendungen, allem voran Acrobat Reader und Flash, erwarten beispielsweise die McAfee Labs, dass das Ausnutzen von Schwachstellen 2010 häufiger in Adobe-Software als in Microsoft-OfficeAnwendungen zu beobachten sein wird. Im Dezember 2009 hatte es bereits ein PDF-Exploit überraschend an die Spitze der Malware-Bedrohungen geschafft: BitDefender meldete, dass über 12 % der weltweiten Infektionen auf das Konto von "PDF-JS.Gen" und somit einer Schwachstelle in Adobes PDF-Javascript-Engines gingen. Problematisch sei in diesem Licht nicht zuletzt ein fehlendes Standardverfahren für Security-Patches und andere wichtige Updates in Applikationen, beklagt Norman: Die Vielzahl der Prozeduren stelle eine besondere Herausforderung für Administratoren und Anwender dar. Da Malwareautoren neue Schwachstellen heute sehr schnell ausnutzen, sei zudem eine noch raschere Reaktion der Anbieter bei der Bereitstellung von Patches und Workarounds erforderlich.

Schadsoftware; Computerkriminalität; Bedrohungspotential; Informationstechnik; IT-Sicherheit; Computermissbrauch; Computermanipulation; Computervirus; Sicherheitsmaßnahme; Zukunftsperspektive; Prognose

ID-nummer: 20100058

Hoch, Jules S.

Kinderpornografie; Kriminalpolizeiliche Ermittlungsarbeit im Internet

Kriminalistik, 2010, 1, S. 53-55
mit 13 QU

Viele Pädosexuelle nutzen das Internet, einen digitalen Sozialraum, um sich weltweit mit Gleichgesinnten zu vernetzen, Erfahrungen auszutauschen, einschlägige Bilder und Videos zu tauschen bzw. zu handeln und mit einer neuen, virtuellen Identität in Chatrooms oder sozialen Netzwerken Kinder und Jugendliche anzusprechen oder gar Kontakte anzubahnen. Die Liechtensteiner Landespolizei hat schon über mehrere Jahre einen Ermittlungsschwerpunkt im Bereich ‚Cyber Policing' und ‚Cyber Crime', wobei speziell die Verfolgung von Kinderpornographie im Fokus steht.
Es wurde eine IT-Forensik Einheit mit spezialisierten IT-Ermittlern bei der Kriminalpolizei geschaffen sowie ein IT-Labor mit aufwändiger Spezialtechnik (Hard- und Software) eingerichtet. Aufgabe dieser kriminalpolizeilichen IT-Einheit ist es, verdachtsabhängige Ermittlungen im Internet durchzuführen, digitale Spuren- und Beweise im Internet zu sichern sowie sichergestellte Tatmittel (Computer, externe Festplatten, DVD, Handys etc.) zu analysieren und hinsichtlich strafbarer Inhalte auszuwerten. Da die Personalressourcen ein verdachtsunabhängiges Internet-Monitoring nicht zulassen, hat die Landespolizei im Oktober 2006, gestützt auf den trilateralen Polizeikooperationsvertrag, eine Verwaltungsvereinbarung mit dem Schweizer Bundesamt für Polizei abgeschlossen.
Die kriminalpolizeiliche Praxiserfahrung zeigt, dass man bei fast jedem des sexuellen Missbrauchs verdächtigten Mann Kinderpornografie sicherstellt und umgekehrt auch bei einem kleineren Teil der Kinderpornoverdächtigen sexuelle Übergriffe auf Unmündige bzw. Vorbereitungshandlungen dazu feststellt. Die Strafverfolgungsbehörden sind daher in jedem Fall von Kinderpornographie aufgefordert, eine Eskalationsentwicklung oder ein Rückfallrisiko in Betracht zu ziehen und im Sinne der vorbeugenden Kriminalitätsbekämpfung die erforderlichen und rechtlich möglichen Massnahmen zu setzen.

Kinderpornographie; Kinderschutz; Internet; Ermittlungsarbeit; Kriminalpolizeiliche Auswertung; Erfahrungsbericht; Liechtenstein

ID-nummer: 20100765

Edelheim, Carsten

Abzocke im Internet; Die Cybergangster hecken immer neue Tricks aus - durchaus mit Erfolg

CD Sicherheits-Management, 2010, 3, S. 84-91
mit 2 BILD

Der Autor erläutert die gängigen Internetbetrügereien und die damit verbundenen lukrativen Abzockmethoden.

Cybercrime; Internetkriminalität

ID-nummer: 20100189

Pfeiffer, Sascha

Wie Unternehmen Bedrohungen durch Social Media abwenden; Facebook, Twitter und Co

IT-Sicherheit - Management und Praxis, 2010, 1, S. 18-19
mit 2 TAF

Auch in Unternehmen werden Schutztechnologien benötigt, die sich individuell anpassen lassen. Dazu gehört im Umgang mit sozialen Netzwerken beispielsweise Data Loss Monitoring. Mit einer derartigen Lösung stellt ein Unternehmen sicher, dass bestimmte Informationen die Unternehmensgrenzen nur auf genehmigten Wegen verlassen. Darüber hinaus sollten Firmen exakt konfigurierbare Zugangs- und Zugriffsbeschränkungen einführen. Damit erhalten nur Mitarbeiter Zugang zu bestimmten Websites und Anwendungen, die diesen auch wirklich benötigen und im Umgang mit diesen Tools besonders geschult sind. Unternehmen, die in der heutigen sozial vernetzten Welt flexibel operieren wollen, stehen nun vor der Herausforderung, einen einheitlichen Ansatz für den individuellen Umgang der Mitarbeiter mit dem Web 2.0 zu entwickeln. Dieser verbindet dann Verschlüsselung, Zugangs- und Zugriffskontrollen, Data Monitoring und umfassenden Schutz vor Schadprogrammen.

Netzwerk; Internet; Wirtschaftsunternehmen; Software; Schadensrisiko; Schadensverhütung; Schadsoftware; Kriminalitätsphänomen

Übersicht über die bisher erschienenen Bände der COD-Literatur-Reihe:

- Band 24 Bekämpfung des Rechtsextremismus – eine gesamtgesellschaftliche Herausforderung
  2012, 141 Seiten
- Band 23 60 Jahre BKA: Im Spannungsfeld zwischen Freiheit und Sicherheit
  2011, 65 Seiten
- Band 23 Rechtsextremismus (Ergänzung)
  2011, 45 Seiten
- Band 22 Gewaltphänome – Strukturen, Entwicklungen und Reaktionsbedarf
  2010, 160 Seiten
- Band 21 Weltweite Brennpunkte der Kriminalität – Auswirkungen auf Deutschland
  2009, 155 Seiten
- Band 20 Wirtschaftskriminalität und Globalisierung – die Polizei vor neuen Herausforderungen
  2008, 83 Seiten
- Band 19 Tatort Internet – eine globale Herausforderung für die Innere Sicherheit
  2007, 187 Seiten
- Band 18 Illegale Migration
  Gesellschaften und polizeiliche Handlungsfelder im Wandel
  2006, 185 Seiten
- Band 17 Neue Allianzen gegen Kriminalität und Gewalt
  Ganzheitlicher Ansatz zur Kriminalitätsbekämpfung – national und international
  2005, 61 Seiten
- Band 16 Netzwerke des Terrors – Terror der Netzwerke
  2004, 83 Seiten
- Band 15 Informations- und Kommunikationskriminalität
  2003, 75 Seiten
- Band 14 Aktuelle Phänomene der Gewalt
  1993, 311 Seiten
- Band 13 Rechtsextremismus
  Erscheinungsformen Entwicklungstendenzen
  1993, 70 Seiten

- Band 12 Standortbestimmung und Perspektiven der polizeilichen Verbrechensbekämpfung
  1992, 84 Seiten

- Band 11 Verbrechensbekämpfung in europäischer Dimension
  1991, 147 Seiten

- Band 10 Organisierte Kriminalität in einem Europa durchlässiger Grenzen
  1990, 158 Seiten

- Band 9 Technik im Dienste der Straftatenbekämpfung
  Teil 1: Polizeitechnik (1985-1989)
  Teil 2: Kriminaltechnik (1987-1989)
  1989, 210 Seiten

- Band 8 Ausländerkriminalität in der Bundesrepublik Deutschland
  1988, 130 Seiten

- Band 7 Wirtschaftskriminalität Teil 2: 1983-1987
  1988, 254 Seiten

- Band 6 Kriminalitätsbekämpfung als gesamtgesellschaftliche Aufgabe
  1987, 275 Seiten

- Band 5 Macht sich Kriminalität bezahlt?
  Aufspüren und Abschöpfen von Verbrechensgewinnen
  1986, 29 Seiten

- Band 4 Gewalt und Kriminalität
  1985, 475 Seiten

- Band 3 Internationale Verbrechensbekämpfung
  - Europ. Perspektiven -
  1984, 249 Seiten

- Band 2 Wirtschaftskriminalität
  1983, 275 Seiten

- Band 1 Polizeiliche Datenverarbeitung
  1982, 297 Seiten

Alle Bände der COD-Literatur-Reihe stehen auf der Homepage des Bundeskriminalamtes (http://www.bka.de) zum Download zur Verfügung.