CAk report

Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 43 April 2017

Neues Seminar

Fake News? Hate Speech? Manipulation? – Gezielte Angriffe auf die Reputation von Unternehmen, Behörden und Einzelpersonen erkennen, bewerten und richtig reagieren.

Gegenstand des Seminars

Ob Fake News, alternative Fakten, Hate Speech oder gezielte Verleumdungen. Social media Kanäle wie Youtube, Facebook und Twitter, aber auch Blogs und Webseiten dienen immer stärker als Kanal der Informationsbeschaffung und Kommunikationskanäle. Die Kontrolle und Prüfung der Informationen, die über diese Kanäle und Plattformen verbreiten und geteilt werden, sind oftmals schwierig.
Gleichzeitig werden die neuen Medien immer öfter dazu genutzt, um bestimmte Gruppen, Einrichtungen oder auch Einzelpersonen gezielt anzugreifen, zu diskreditieren oder zu erpressen. Vor dem Hintergrund steigender Zahlen von Verleumdung und Volksverhetzung, aber auch aus Sorge vor gezielten Manipulationen bei Wahlen, hat das Bundesministerium der Justiz und Verbraucherschutz nun einen Entwurf für ein „Netzdurchsetzungsgesetz“ vorgelegt. Dieses setzt sich zum Ziel, eine bessere Rechtsdurchsetzung im Internet zu erreichen und Falschnachrichten auf Plattformen sozialer Netzwerke sowie Hasskriminalität im Netz zu bekämpfen. Hierzu zählen u.a. Beleidigung, üble Nachrede, Verleumdung, öffentliche Aufforderung zu Straftaten, Volksverhetzung und Bedrohung.

Ziel des Seminars

In dem Seminar werden aktuelle Phänomene, die sich im Umfeld von Social Media-Netzen- und Kanälen, Bewertungsplattformen und (kommerziellen) Blogs verstärkt bemerkbar machen vorgestellt. In diesem Zusammenhang werden konkrete Problemfälle, die Behörden, Unternehmen und Einzelpersonen durch Phänomene wie Hate Speech, Informationsmanipulation und gezielte Angriffe auf die Reputation Ihrer Behörde/Ihres Unternehmens treffen können, an Praxisbeispielen erörtert.
In einem weiteren Schritt werden juristische, ermittlungstechnische und kommunikationsrelevante Maßnahmen vorgestellt, die den Teilnehmern als Leitfaden dienen können, sollten Sie Opfer von entsprechenden Kriminalitätsdelikten werden. Gleichzeitig werden die Verantwortlichkeiten (intern und extern) bei entsprechenden Phänomenen und Delikten aufgezeigt und erläutert.

Zielgruppe

Das Informations- und Sensibilisierungsseminar richtet sich an interessierte Mitarbeiter aus Rechts-, Kommunikations-, Service-, IT- und Zentralabteilungen von Unternehmen und Behörden, Versicherungen sowie Straf- und Ermittlungsbehörden.

Das Seminar „Fake News, Reputationsschäden“ findet am **13. Juni 2017 in Berlin** statt.

INHALT

CAk-SEMINARE 2017

- Social Media rechtssicher und datenschutzkonform nutzen (09.05.2017, Berlin)
- Physische und Infrastrukturelle Sicherheit (10.05.2017, Berlin)
- Grundlagen des Datenschutzes beim Outsourcing (11.05.2017, Bonn)
- Cyber Defence Simulation Training (16.05.2017 - 18.05.2017, Berlin)
- Update IT-Compliance: Rechtssichere IT-Strukturen und -Prozesse (30.05.2017, Hannover)
- IuK-Notfallmanagement für die Polizei nach BSI 100-4 (30.05.2017 - 31.05.2017, Frankfurt am Main)
- Revisionssichere Service Level Agreements (01.06.2017, Bonn)
- CYBER AKADEMIE-KLAUSUR (19.06.2017 - 21.06.2017, Würzburg)
- ISIS12 für Kommunen (20.06.2017, Berlin)

www.cyber-akademie.de

Gemeinschaftsaufgabe Cyber-Sicherheit

Bundesamt für Sicherheit in der Informationstechnik im Dialog mit Unternehmen

(CAk/stb) Voraussetzung für erfolgreiches Wirtschaften im digitalen Zeitalter ist die Sicherheit der Daten und IT-Systeme. Kleine und mittelständische Unternehmen für diese Erkenntnis zu sensibilisieren, ist eines der Ziele der Veranstaltungsreihe "BSI im Dialog mit der Wirtschaft" des Bundesamts für Sicherheit in der Informationstechnik (BSI).

In diesem Rahmen lud das BSI in der Geschäftsstelle der Industrie- und Handelskammer (IHK) in Ingolstadt Interessierte aus Wirtschaft, Behörden und Politik zur Diskussion über Cyber-Sicherheit ein. "Leider zögern gerade viele mittelständische Betriebe nach wie vor bei Investitionen in eine sichere IT-Infrastruktur und betrachten das Thema zuallererst durch die Kostenbrille", sagte Fritz Peters, Sprecher des IHK-Forums Region Ingolstadt, in seinem Grußwort. Dr. Reinhard Brandl, Mitglied des Deutschen Bundestags, betonte den Stellenwert des Themas Cyber-Sicherheit für die Politik.
BSI-Präsident Arne Schönbohm warb in einem Impulsvortrag für Kooperation zwischen Wirtschaft und Staat: "Cyber-Sicherheit ist für Unternehmen und Behörden eine Gemeinschaftsaufgabe", betonte er. Zum Angebot des BSI sagte er: "Mit unseren Veranstaltungen treten wir mit Unternehmen vor Ort in Dialog. Konkrete Hilfestellungen bieten wir mit unseren Informationsangeboten sowie mit der Allianz für Cyber-Sicherheit."
In einer Podiumsdiskussion diskutierten anschließend BSI-Präsident Arne Schönbohm, Evi Haberberger von der Zentralstelle Cybercrime am Bayerischen Landeskriminalamt, Thomas Reichert von Drivelock und Manfred Hoffmann von Hoffmann Mineral über die Herausforderungen der Digitalisierung und Möglichkeiten, IT-Systeme und Daten zu schützen. Fragen aus dem Publikum drehten sich um Mitarbeiter-Sensibilisierung und Schutz vor Cyber-Angriffen. Evi Haberberger sprach über die Schwierigkeiten im Umgang mit Cyber-Kriminalität und informierte über Kooperations- und Hilfsangebote der mit Cyber-Kriminalität beschäftigten Behörden für Unternehmen.

Münchner Cyber Dialog 2017 am 29. Juni 2017

Sichere Digitale Transformation im Fokus

Die Digitale Transformation bietet Risiken wie Chancen und muss als gemeinsame Aufgabe von Wirtschaft und Gesellschaft betrachtet werden. Cybersicherheit, Cyberabwehr und Digitalisierung sind für Behörden, aber insbesondere auch für den Mittelstand von teilweise noch immer unterschätzter Bedeutung. Unter dem Motto „Gestalteter Wandel oder administriertes Chaos? Sichere digitale Transformation in Staat, Wirtschaft und Gesellschaft“ veranstaltet die Cyber Akademie in Kooperation mit dem Behörden Spiegel, am 29. Juni 2017 den Münchner Cyber Dialog 2017. Eröffnet wird die Konferenz von Staatsminister Dr. Marcel Huber, Chef der bayerischen Staatskanzlei. Im Hauptprogramm wird u.a. Carsten Heitmann von der Robert Bosch GmbH über IT-Sicherheit in Zeiten von Digitaler Transformation sprechen. Peter Batt berichtet als IT-Direktor des Bundesinnenministeriums über aktuelle Entwicklungen im Bereich Cybersicherheit. Auf welche neuen Herausforderungen sich Staat, Wirtschaft und Gesellschaft hinsichtlich Cybersicherheit einstellen müssen, erläutert Iris Plöger, Mitglied der Hauptgeschäftsführung des BDI e.V. Neben den hochkarätigen Keynotes, werden auch vier Workshops zu Themen wie Arbeit 4.0, Robotics, Sicherheit und Digitalisierung im Energiesektor oder über die (digitale) Zukunft des Mittelstandes, veranstaltet. Weitere Informationen sowie das aktuelle Programm des Münchner Cyber Dialogs 2017 finden Sie unter www.muenchner-cyber-dialog.de.

Erklärung von Verbänden und Verbraucherzentralen.

Für starken Datenschutz

In einer gemeinsamen Erklärung sprechen sich Verbände und Verbraucherzentralen für die Wahrung des hohen Datenschutzstandards in Deutschland aus. Sie richten sich damit an Bundesregierung, Bundesrat und Bundestag, die die europäische Datenschutzgrundverordnung vom 25. Mai 2016 durch ein nationales Gesetz umzusetzen haben. Dazu hatte die Bundesregierung am 1. Februar einen vom Bundesministerium des Innern federführend verfassten Entwurf beschlossen. Dieser war bereits von Datenschutzbeauftragten von Bund und Ländern kritisiert worden.

Auf Sammlung großer Datenmengen ausgerichtete Geschäftsmodelle sollen nicht zum Anlass genommen werden, den Datenschutz zu beschränken.
Foto:CAk/KamiPhuc/ cc by 2.0/www.flickr.com

In der aktuellen Erklärung äußern sich der Bundesverband der Arbeiterwohlfahrt, der Bundesverband hauswirtschaftlicher Berufe, der Deutsche Frauenring, der Deutsche Gewerkschaftsbund, der Bundesverband Verbraucher Service sowie die Verbraucherzentralen des Bundes und der Länder Bayern, Bremen, Rheinland-Pfalz und Sachsen.
Sie weisen darauf hin, dass dem Inkrafttreten der europäischen Datenschutzgrundverordnung jahrelanges Bemühen auch seitens der Bundesregierung vorausgegangen war, damit das Datenschutzniveau in Deutschland nicht durch schwaches internationales Recht herabgesetzt würde. Nun stelle aber umgekehrt die nationale Politik die erreichten europäischen Standards zugunsten zukünftiger Wertschöpfungsmodelle infrage.
Die Verbände und Verbraucherzentralen betonen, dass Datenschutz und moderne Datenverarbeitung nicht in Widerspruch stünden. Es könnten Chancen genutzt und gleichzeitig Risiken minimiert werden. "Die bestehenden Grundsätze des Datenschutzes, die in der Europäischen Union Grundrechtscharakter haben, müssen dabei weiterhin Bestand haben: Datenminimierung, Zweckbindung, Betroffenenrechte und Einwilligung", heißt es in der Erklärung.
Ein starker Datenschutz im Sinne der EU-Grundrechtecharta und unter konsequenter Umsetzung der Datenschutzgrundverordnung müsse gewährleistet werden, um Bürger, Verbraucher und abhängig Beschäftigte "vor dem wahllosen und unkontrollierbaren Verarbeiten von personenbezogenen Daten ohne bestimmten Zweck" zu schützen. Der europäische Datenschutz und das darin gesetzte Vertrauen seien als Chance zu begreifen. Die Autoren der Erklärung fordern außerdem explizit eine gut aufgestellte und effektive Datenschutzaufsicht, ein eigenständiges Beschäftigtendatenschutzgesetz sowie wirksame Rechtsbehelfs- und Sanktionsmöglichkeiten.

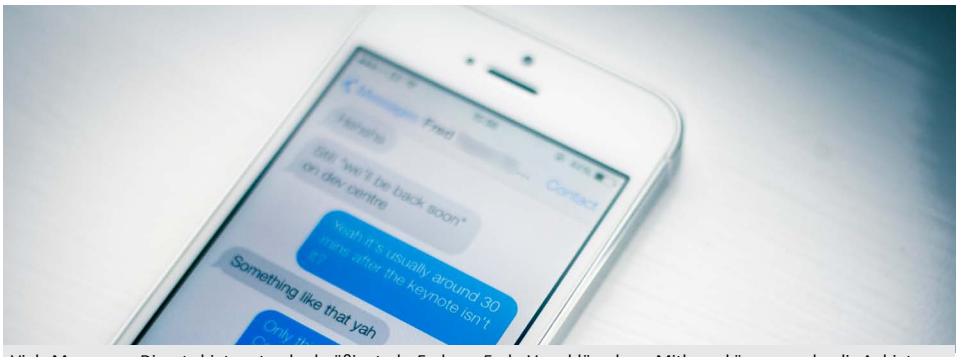
Zum Thema EU-Datenschutzgrundverordnung bietet die Cyber Akademie am **12.09.2017** ein Informationsseminar an.

Foto:CAk/©Bastian Weltjen, fotolia.com

Effektive Strafverfolgung trotz starker Kryptografie

Deutschland und Frankreich fordern EU-Regelungen zum Umgang mit verschlüsselter Kommunikation

(CAk/stb) Verschlüsselte Kommunikation, wie sie von kostenlosen Messenger-Diensten angeboten wird, stellt Ermittlungsbehörden vor große Herausforderungen im Kampf gegen Cyber-Kriminelle und Terroristen. Möglichkeiten, wie der Zugriff auf Nachrichten erleichtert werden könnte, werden derzeit von der EU-Kommission geprüft. Die Initiative dafür geht maßgeblich von den Innenministern von Deutschland und Frankreich aus.



Viele Messenger-Dienste bieten standardmäßig starke Ende-zu-Ende-Verschlüsselung. Mitlesen können weder die Anbieter noch Ermittler ohne Weiteres. Foto:CAk/William Hook/cc by-sa 2.0/www.flickr.com

In einem Brief an die EU-Kommission forderten Bundesinnenminister Dr. Thomas de Maizière und sein französischer Amtskollege Bruno Le Roux jüngst Maßnahmen zur Erhöhung der Sicherheit in Europa. Unter anderem soll der Schutz der EU-Außengrenzen verstärkt werden und Informationssysteme sollen technisch und organisatorisch ausgebaut werden, um die operative polizeiliche Zusammenarbeit in den Mitgliedsstaaten zu verbessern. Damit will man Reisebewegungen von Terroristen und Straftätern effektiv nachverfolgen bzw. verhindern können. Um Gefahren frühzeitig erkennen und abwenden und bei Straftaten ermitteln zu können, will man aber auch auf die Kommunikation von potenziellen Tätern und Tatverdächtigen zugreifen können. Daher fordern die Innenminister "rechtliche Mittel, um den Gebrauch von verschlüsselter elektronischer Kommunikation im Rahmen strafrechtlicher und administrativer Ermittlungen berücksichtigen zu können".

Anbieter in die Pflicht nehmen

Im Brief an die EU-Kommission nehmen die Innenminister Bezug auf eine deutsch-französische Erklärung und ein ausführliches Eckpunktepapier, das de Maizière und Le Rouxs Amtsvorgänger Bernard Cazeneuve bereits im Sommer 2016 vorgelegt hatten. Darin findet sich Näheres zu den geforderten rechtlichen Mitteln. Um Ermittlungen im Zusammenhang mit verschlüsselter Kommunikation zu ermöglichen, sollen die Anbieter der entsprechenden Dienste zur Zusammenarbeit mit den Sicherheitsbehörden verpflichtet werden – und zwar unabhängig davon, ob die Anbieter ihren rechtlichen Sitz innerhalb oder außerhalb der EU haben.

Wie ein Sprecher des Bundesinnenministeriums dem Behörden Spiegel mitteilte, solle die Europäische Kommission vor allem eine rechtliche Rahmengesetzgebung schaffen, die gleiche Pflichten für alle Kommunikationsdienstanbieter schafft. In Deutschland zum Beispiel regeln bislang das Telekommunikationsgesetz sowie die Telekommunikations-Überwachungsverordnung die umfangreichen Pflichten der klassischen Telekommunikationsdienstleister gegenüber den Sicherheitsbehörden – internetbasierte Messenger-Dienste dagegen fallen gemeinsam mit Webshops, Suchmaschinen und anderen Angeboten unter das Telemediengesetz und unterliegen damit nicht denselben Vorgaben.

Dass diese Trennung überholt und unsachgemäß sei, hatte de Maizière schon in Zusammenhang mit nationalen Vorschlägen zur Sicherheitspolitik betont. Für die geforderte Gesetzgebung auf EU-Ebene geht es vor allem darum, Regeln für eine effiziente Zusammenarbeit mit Kommunikationsdienstanbietern zu schaffen. Es müsse klare Ansprechpartner für Ermittlungsbehörden und klare Grundlagen für die Herausgabe von Daten und die Überwachung von Kommunikation geben, wie de Maizière und Cazeneuve im Herbst in einem weiteren Schreiben an die EU-Kommission forderten.

Doch wie will man damit das Problem der Verschlüsselung umgehen? Frankreich hatte sich im Vorfeld der deutsch-französischen Initiative für eine Verpflichtung der Dienstanbieter ausgesprochen, Wege in ihre Verschlüsselungstechnologien einzubauen, über die Ermittlungsbehörden Zugriff auf Klartextnachrichten bekommen können. Eine entsprechende Formulierung in der französischen Pressemitteilung zum gemeinsamen Eckpunktepapier der Innenminister sorgte hierzulande für Irritation, weil de Maizière solche Hintertüren wiederholt ausgeschlossen hatte. So wird in allen offiziellen Papieren und Erklärungen auch stets betont, dass Lösungen gefunden werden müssen, mit denen verschlüsselte Kommunikation berücksichtigt und zugleich die Erhältlichkeit starker und zuverlässiger Kryptographie-Systeme gewährleistet werden kann.

Verschlüsselung umgehen oder knacken?

Auf eine Kleine Anfrage der Fraktion Die Linke im Deutschen Bundestag, in der unter anderem nach den von den Innenministern geforderten rechtlichen Mitteln im Umgang mit verschlüsselter Kommunikation gefragt wurde, antwortete die Bundesregierung, es solle "ein hohes Schutzniveau der Systeme gewährleistet werden, um die Verschlüsselungstechnologien für Benutzer und Wirtschaft nicht zu schwächen." Dementgegen sieht Andrej Hunko, Bundestagsabgeordneter der Fraktion Die Linke, in dem deutsch-französischen Vorstoß "einen Generalangriff auf verschlüsselte Telekommunikation."

Hintertüren, wie von Frankreich gefordert, erwarte Hunko zwar nicht, jedoch sei mit vermehrtem Einsatz staatlicher Trojaner-Software zu rechnen. Gemeint sind Programme, die es Ermittlungsbehörden ermöglichen, Nachrichten unbemerkt direkt von Geräten abzuschöpfen und mitzulesen, noch bevor sie vom der Messenger-Software verschlüsselt und versendet werden. Diese Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) ist in Deutschland bereits möglich, genauso wie die Online-Durchsuchung, bei der nicht nur laufende Kommunikation überwacht, sondern auch der Speicherinhalt von Geräten unbemerkt durchsucht werden kann.
Eine weitere Möglichkeit verschlüsselte Kommunikation zu berücksichtigen, ohne Unternehmen zur Kompromittierung ihrer eigenen Produkte zu zwingen, besteht darin, bereits verschlüsselte Nachrichten zu entschlüsseln. Anbieter müssten dann lediglich Zugang zum Datenverkehr gewährleisten. Die Entschlüsselung müssten die Behörden selbst leisten. Hier entsprechende technische Möglichkeiten zu schaffen, ist Aufgabe der neu eingerichteten Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), die unter anderem Methoden und Produkte zur Dekryptierung für Ermittlungsbehörden erforschen und entwickeln soll.

Ziel EU-Gesetz

Ziel der Innenminister dürfte es also sein, schnell eine Rahmengesetzgebung zu schaffen, die auf EU-Ebene rechtlich regelt, was technisch möglich ist oder sein wird, und die die Zusammenarbeit der Behörden untereinander und mit den Dienstanbietern vor allem in Fällen grenzüberschreitender Kriminalität erleichtert.
Inzwischen ist die deutsch-französische Initiative sowohl in der EU-Kommission als auch im Rat für Justiz und Inneres behandelt worden. Die Kommission begrüßte die Vorschläge und kündigte neue Rahmenvorgaben zum Datenschutz für elektronische Kommunikation zur Schaffung gleicher Wettbewerbsbedingungen für alle Anbieter von Kommunikationsdienstleistungen an. Wie ein Sprecher der Kommission dem Behörden Spiegel mitteilte, sei derzeit aber keine Gesetzgebungsinitiative im direkten Zusammenhang mit verschlüsselten Kommunikation geplant.
Allerdings werde in zwei Arbeitsbereichen juristische und technische Expertise gesammelt, um Möglichkeiten zu sondieren, wie Ermittlungshindernisse durch Verschlüsselung überwunden werden können, ohne Vertrauen in digitale Dienste und deren Sicherheit zu gefährden. Dabei werde einerseits mit EU-Behörden wie Europol, Eurojust und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) und andererseits mit Vertretern von Industrie und Zivilgesellschaft zusammengearbeitet. Ergebnisse will die Kommission in der zweiten Jahreshälfte 2017 vorlegen.

Zum Thema Grundlagen der Kryptologie bietet die Cyber Akademie vom **25.04.2017 - 26.04.2017** ein Seminar in Hamburg an.

Veranstaltungshinweise

Cyber Defence Simulation Training

In dem einmaligen Schulungskonzept werden typische IT-Angriffe im Kontext von „echten“ Unternehmensnetzwerken simuliert. Jeder Teilnehmer erhält Zugriff auf eine eigene IT-Infrastruktur unter Nutzung von gängigen Standardprodukten, wie sie auch tagtäglich in Unternehmen zum Einsatz kommt.

Ziel ist es, das die Teilnehmer verschiedenste moderne Angriffe auf Unternehmensnetzwerke unter Anleitung verstehen, erkennen und ggf. abwehren.
Andreas Falkenberg, arbeitet seit vielen Jahren als professioneller White-Hat Hacker. In vielen internationalen Projekten in Europa, Asien und den USA kann er auf ein breites Erfahrungsspektrum, beginnend mit der Überprüfung von einfachen Webseiten bis hin zu Audits für Core-Banking Applikationen, zurückgreifen.
Das Training ist in 9 Kapitel und 20 Szenarien aufgegliedert. Vor jedem Kapitel erfolgt eine detaillierte theoretische Einführung in das Thema.

Termine in Berlin:
16.05.2017 - 18.05.2017
19.09.2017 - 21.09.2017

Cyber Akademie-Summer School - Entspannt lernen

In den Sommermonaten 2017 bietet die Cyber Akademie erstmalig Sommerkurse an. In der Summer School der Cyber Akademie können Interessierte die Ferienzeit nutzen, um sich intensiv mit dem Thema Informationssicherheit auseinanderzusetzen. In der wunderschönen Landschaft des österreichischen Tirols, direkt an der deutsch-österreichischen Grenze, führt die Cyber Akademie in den Monaten Juli/August die Zertifikatslehrgänge “IT-Grundschutzexperte” und “LEADAuditor” durch.

“IT-Grundschutz-Experte” erläutert den Teilnehmern die Grundsätze der Informationssicherheit auf Basis des IT-Grundschutzes, vermittelt die Implementierung des Standards in das Unternehmen oder die Behörde und bietet praktische Hinweise für die interne Auditierung und den Zertifizierungsprozess. Im Seminar “LEAD-Auditor” werden den Teilnehmern die Grundsätze der Informationssicherheit auf Basis des internationalen Standards ISO/IEC 27001 erläutert .

Termine in Leutasch:
Lead-Auditor nach ISO/IEC 27001: 17.07.2017 - 21.07.2017
IT-Grundschutz-Experte: 07.08.2017 - 11.08.2017

CAk News in 100 Sekunden . . .

Rechtsdurchsetzung in sozialen Netzwerken

Thomas Feil,
Fachanwalt für IT-Recht,
Datenschutzbeauftragter
TÜV

IMPRESSUM

Herausgeber: Cyber Akademie GmbH, Geschäftsführer: R. Uwe Proll (presserechtlich verantwortlich); Florian Lindemann; Seminarleiter: Benjamin Bauer
Geschäftsstelle: Friedrich-Ebert-Allee 57, 53113 Bonn, Telefon: 0049-228-97097-0, Telefax: 0049-228-97097-75, ↗ *www.cyber-akademie.de*
Registergericht: HRB 148255 AG Berlin (Charlottenburg)
Redaktionelle Leitung: R. Uwe Proll; **Redaktion:** Benjamin Bauer, Florian Lindemann; **Redaktionsassistenz:** Angelina Meyer (Bonn), Kerstin Marmulla, Kirsten Klenner, Sebastian Lahr (Berlin) **Programmbeirat:** Dr. Bernd Benser, Chief Business Officer GridLab GmbH; Prof. Dr. Wilfried Bernhardt, Staatssekretär a.D., Rechtsanwalt und Honorarprofessor für Internetrecht, Dr. Gerd Landsberg, Geschäftsführendes Präsidialmitglied des Deutschen Städte- und Gemeindebundes (DStGB); Dr. Philipp Amann, Europol, European Cybercrime Centre (EC3); Dr. August Hanning, Staatssekretär a.D. Bundeministerium des Innern, Präsident des Bundesnachrichtendienstes a.D.; Reinhold Harnisch, Geschäftsführer Kommunales Rechenzentrum Minden-Ravensberg/Lippe; Hans-Jürgen Hohnen, Staatssekretär a.D. Innenministerium Brandenburg; Prof. Dr. Radu Popescu-Zeletin, ehem. Leiter des Fraunhofer Instituts für Offene Kommunikationssysteme; Dieter Schneider, LKA-Präsident Baden Württemberg a.D.; Jörg Bruchmüller, Landesbezirksvorsitzender der Gewerkschaft der Polizei (GdP) in Hessen ; Dieter Schürmann, Landeskriminaldirektor im Ministerium für Inneres und Kommunales NRW