CAk report
Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 24 / September 2015

Das neue Wintersemester 2015/2016

Aktivitäten und Neuheiten der Cyber Akademie im Herbst und Winter

Die Cyber Akademie hat die Sommerpause genutzt, um das bestehende Leistungsportfolio zu überarbeiten und zu erweitern. Ab September präsentiert sich die Cyber Akademie mit einem vergrößerten Angebot an Aus- und Fortbildungsseminaren im Bereich des Datenschutzes und der IT-Sicherheit. Gleichzeitig wird sich die CAk als Veranstalter, fachlicher Partner und Aussteller auf einer Reihe von Konferenzen präsentieren. Alle Aktivitäten orientieren sich an dem Leitmotiv der Cyber Akademie, den Digitalisierungsprozess in Wirtschaft, Verwaltung und Gesellschaft zu fördern und sicher zu gestalten.

Highlight Münchner Cyber Dialog

Bereits am 22. September 2015 präsentiert sich die Cyber Akademie mit einem eigenen Fachforum zum Thema **„Hacking-Methoden in der Praxis“** und einem Stand auf dem Fachkongress **„Public IT-Security“ (PITS)** in Berlin. Am 21. Oktober 2015 veranstaltet die Cyber Akademie den **Münchner Cyber Dialog**, der die (sichere) Digitalisierung in Wirtschaft, Verwaltung und Gesellschaft thematisiert und zu dem hochrangige IT-und Sicherheitsverantwortliche aus Industrie- und Softwareunternehmen, Bund und Ländern erwartet werden. Ebenfalls im Oktober wirkt die Cyber Akademie am **Cybercrime-Kongress des Ministeriums für Inneres und Kommunales des Landes NRW** mit. Mit Blick auf das Dauerthema Cybercrime wird sich die Cyber Akademie im November intensiv mit dem Kampf gegen Kinderpornographie im Internet befassen und das **Symposium des Bündnisses White IT**, welches am 2./3. November in Hannover stattfinden wird, unterstützen.
Ein weiterer Schwerpunkt wird auf einer verstärkten Sensibilisierung der (mittelständischen) Wirtschaft hinsichtlich der Anforderungen an die Daten- und IT-Sicherheit sein. Einerseits spielt das Thema eine wichtige Rolle beim Münchner Cyber Dialog, andererseits hat die Cyber Akademie entsprechende Fortbildungen bereits in das neue Seminarprogramm aufgenommen.

Seminare

Das im Juni gestartete **Seminar zum neuen IT-Sicherheitsgesetz** erfreut sich einer positiven Resonanz sowohl bei großen und mittelständischen Unternehmen, KRITIS-Betreibern als auch Behörden. Ausgehend von den spezifischen Bedarfen und Anforderungen, die sich aus dem (neuen) regulatorischen Rahmen ergeben, hat die Cyber Akademie eine Anzahl neuer Seminare entwickelt und in das Ausbildungsprogramm aufgenommen. Hierzu gehören u.a. **Informationsmanagement Systeme in Kommunen**, **IT- und Datenschutz als Führungsaufgabe**, **Update IT-Compliance** oder auch ein **Grundlagenseminar zur Kryptologie**. Darüber hinaus wurden die Seminare der Cyber Akademie mit Tüv Rheinland geprüfter Qualifikation (**IT-Sicherheitsbeauftragter**, **Datenschutzbeauftragter**) grundlegend überarbeitet und aktualisiert.

NEU: Rubrik – Neues aus IT- und Datenschutzrecht

Vor dem Hintergrund der rechtlichen Anforderungen an die IT-Sicherheit und den Datenschutz, gestalten wir ab sofort eine **Rubrik** , die Sie über aktuelle rechtliche Entwicklungen und Entscheidungen informiert. Gleichzeitig möchten wir interessierte Leser dazu einladen, uns Themenvorschläge, Fragen oder Urteile zu übersenden, die wir in dieser Rubrik aufführen und erörtern können. Wir freuen uns über Ihre Zuschriften an **info@cyber-akademie.de**.

INHALT

Bundeswehr ordnet sich im Cyber Raum neu ..... **Seite 2**

Bundeslagebild des BKA: Herausforderung Cybercrime ..... **Seite 3**

Praxistipps der Cyber Akademie: Neues aus IT- und Datenschutzrecht ..... **Seite 4**

CAk-Seminare 2015

Datenschutz-Praxis - IT-Grundlagen für Datenschutzbeauftragte
01.10.2015, Berlin

IuK-Strategien und -Technologien
13. – 15.10.2015, München

Hacking-Methoden in der Praxis: Vorgehen des Angreifers und Schutzmaßnahmen
14. – 15.10.2015, Köln

Update IT-Compliance - Rechtssichere IT-Strukturen und -Prozesse
20.10.2015, Berlin

Sichere Webanwendungen in der öffentlichen Verwaltung - Vergabe, Entwicklung, Abnahme
29. – 30.10.2015, Berlin

www.cyber-akademie.de

Cyber Defence

Bundeswehr ordnet sich im Cyber-Raum neu

(CAk/rup) Die größte Sicherheitsorganisation der Bundesrepublik Deutschland, die Bundeswehr, stellt sich neu auf, um den Herausforderungen zur Cyber-Sicherheit perspektivisch gerecht zu werden.

Im Rahmen des Weißbuchprozesses zur Sicherheitspolitik und zur Zukunft der Bundeswehr, führten das Bundesministerium der Verteidigung und der Branchenverband Bitkom in der vergangenen Woche den Expertenworkshop "Perspektiven Cybersicherheit" in Berlin durch. Auf der Veranstaltung kündigte Bundesverteidigungsministerin Ursula von der Leyen an, dass die zersplitterten Zuständigkeiten bei der Cyber-Abwehr, aber auch der IT insgesamt, mit der 15.000 Soldaten und Soldatinnen sowie Zivilangestellte bei der Bundeswehr beschäftigt sind, zu einer neuen schlagfertigen Organisation zusammengefasst werden sollen. Im Ministerium selbst soll es dafür eine eigene Stabsstelle geben.

Quelle: Bundeswehr/Grauwinkel

Kommando für Cyber- und Informationsraum

Der eingerichtete Aufbaustab im Ministerium soll bis zum Frühjahr 2016 das Kommando Cyber-und Informationsraum, das direkt dem Ministerium unterstellt ist, auf Augenhöhe mit den anderen Teilstreitkräften organisiert haben. Dahinter stehen signifikante Ressourcen, dies nicht nur personell, sondern auch finanziell, denn mit einer Milliarde jährlicher Ausgaben für grüne (militärische) und weiße (zivile) IT ist die Bundeswehr mit Abstand der größte staatliche Betreiber eigener IT-Infrastrukturen. Für die Cyber-Abwehr Deutschlands ist dies ein signifikanter Schritt nach vorne, denn die bundeswehreigenen Ressourcen bilden den mächtigsten Block bei der Cyber-Sicherheit bei Bund und Ländern insgesamt.

Die Bundeswehr steht dabei vor der Aufgabe einer ihrer größten Modernisierungsvorhaben. Neben Luft, Wasser und Boden gilt nun der Cyber-Raum als neue Dimension militärischer Verteidigung. Die deutschen Streitkräfte stehen dabei vor einer multiplen Herausforderung, denn es gilt nicht nur die eigene IT-Infrastruktur zu schützen, hier wie bisher üblich die zivile IT, sondern besonders auch die IT in den Waffensystem selbst. Andererseits muss die Bundeswehr ihrem Verteidigungsauftrag nach Cyber-Angriffe aus dem Ausland abwehren können. Desweiteren zieht die Analogie der bisherigen militärischen Doktrin nach sich, dass dies gegenüber fremden Staaten nur dann möglich ist, wenn auch eine Abschreckung vorhanden ist. Das heißt mit anderen Worten, das die Bundeswehr nicht nur eine IT-Sicherheitsburg um Deutschland baut, sondern ihre Abschreckungsfähigkeit gegenüber einem möglichen staatlichen Angriff von außen auch dadurch dokumentiert, dass sie in der Lage ist mit Cyber-Abwehr eben auch diese Abwehrfähigkeit durch Cyber-Angriffsmöglichkeiten zu dokumentieren. Genau hierin liegt der politisch-mentale Kurswechsel, den die Ministerin nicht überdeutlich aussprechen wollte, doch der in der Analogie zu herkömmlichen militärischen Strategien und Material gemeint ist.

Defensive und offensive Fähigkeiten

Auf dem Expertenworkshop in Berlin wurde eines jedoch sehr deutlich: Cyber-Fähigkeiten sind Mittel, die defensiv wie offensiv eingesetzt werden können. Zudem war allen Experten klar, eine ernsthafte Abschreckung und Abwehr ist auch im Cyber-Raum, wie auch in den anderen militärischen Dimensionen wie Luft, Wasser und Boden nicht ohne die Fähigkeiten zu einem Gegenangriff glaubwürdig. Ein Kampfpanzer der Bundeswehr ist auch nicht per se defensiv oder offensiv, er ist ein Waffensystem das zur Verteidigung dient, gleichzeitig aber in der Lage sein muss einen Gegenangriff zu führen. Militärischer Logik folgend können also Cyber-Abwehrwaffen zwingend auch beides. So sinnvoll diese Betrachtung auch ist, so wird sich die Ministerin und ihr Haus in den nächsten Wochen einer intensiven Diskussion hierüber unterziehen müssen.

Enge Kooperation mit der Industrie

Die Bundeswehr erhebt sich nach dem Beschluss der Ministerin zum primus inter pares in Sachen Cyber-Abwehr in Deutschland. Dass die Bundeswehr mehr Gewicht, gegebenenfalls auch mehr Personal und materielle Ressourcen in die Cyber-Abwehr stecken will, wird im politischen Raum goutiert. Wenn es der Ressortchefin gelingt, die durchaus auch intern spürbaren Widerstände wegen der Umorganisation zu überwinden, ist das Verteidigungsressort auf dem besten Weg in Sachen Cyber-Abwehr die Zentralstelle in Deutschland zu werden.

Bei ihrer Rede auf dem Expertenworkshop ließ die Ministerin auch folgenden Hinweis nicht aus: Sie setzt auf eine enge Kooperation mit Wissenschaft und Industrie, um den notwendigen Bedarf an IT-Fachleute und innovativen Lösungen zu decken. Gleichzeitig sieht sie die Bundeswehr als Ansprechpartner für die Wirtschaft bei Cyber-Angriffsproblemen.

Bundeslagebild des BKA

Herausforderung Cybercrime

2013 wurden in der Polizeilichen Kriminalstatistik (PKS) bundesweit insgesamt 64.426 Fälle krimineller Handlungen im digitalen Raum verzeichnet. Das geht aus dem entsprechenden Bundeslagebild des Bundeskriminalamtes (BKA) hervor. Der daraus entstandene Schaden wird auf rund 42,6 Millionen Euro allein in der Bundesrepublik taxiert.

Weltweit dürften es jährlich sogar bis zu 400 Milliarden US-Dollar sein, schätzen Experten. Deshalb nimmt die Cyber-Kriminalität auch in der Aufgabenwahrnehmung der Sicherheitsbehörden hierzulande eine immer wichtigere Bedeutung ein. Aber auch Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft müssen die künftigen Herausforderungen des digitalen Wandels meistern. Aus diesem Grunde veranstaltet das nordrhein-westfälische Innenministerium am 21. Oktober 2015 in der Messe Düsseldorf erstmals eine Tagung zu den Anforderungen an eine erfolgreiche Abwehr und Bekämpfung der Kriminalität im digitalen Raum. Zahlreiche hochrangige und internationale Referenten widmen sich unter dem Motto „Cybercrime - Eine Herausforderung für die Innere Sicherheit“ unter anderem den allgemeinen Risiken dieser Deliktsform für Gesellschaft und Privatwirtschaft, den diesbezüglichen Erwartungen an staatliche Institutionen sowie den globalen Gefahren von Cybercrime. Die Cyber Akademie wird sich in einem eigenen Fachforum mit dem Schutz Kritischer Infrastrukturen vor Angriffen aus dem Cyber-Raum befassen und die Frage aufwerfen, wie die Kommunen diesen Herausforderungen begegnen können.

Die Veranstaltung endet mit einer Podiumsdiskussion über effektive Schutz- und Präventionsmaßnahmen gegen Cyber-Kriminalität enden. An ihr wird auch der nordrhein-westfälische Innenminister Ralf Jäger (SPD) teilnehmen. Erwartet werden rund 400 Teilnehmer, darunter beispielsweiseProfessor Dieter Kempf, Mitglied des Nationalen Cybersicherheitsrates und langjähriger Vorsitzender des BITKOM.

Weitere Informationen zur Konferenz sowie das aktuelle Programm finden Sie auch unter *www.mik.nrw.de/kongress-cybercrime/programm.html*.

Praxistipps der Cyber Akademie

Neues aus IT- und Datenschutzrecht

Vor dem Hintergrund der rechtlichen Anforderungen an die IT-Sicherheit und den Datenschutz, führt die Cyber Akademie mit dieser Ausgabe eine Rubrik ein, die Sie über aktuelle rechtliche Entwicklungen und Entscheidungen informieren wird. Gleichzeitig möchten wir interessierte Leser dazu einladen, uns Themenvorschläge, Fragen oder Urteile zu übersenden, die wir in dieser Rubrik aufführen und erörtern können. Wir freuen uns über Ihre Zuschriften an **info@cyber-akademie.de**.

Meldung der BayLDA: Bußgeld bei fehlerhafter Auftragsdatenverarbeitung

Das Bundesarbeitsgericht (BAG) hat in einem Urteil vom 19.02.02015 (8 AZR 1011/13) entschieden, dass bei der Veröffentlichung von Bildern oder Videoaufnahmen eines Arbeitnehmers die Regelungen des § 22 KUG den Vorschriften des BDSG vorgehen. Die Klage des Arbeitnehmers auf Unterlassung der Veröffentlichung und Zahlung eines Schmerzensgeldes wurde abgewiesen. Voraussetzung ist, dass eine Einwilligung im Sinne des § 22 KUG in die Veröffentlichung erteilt wurde. Mit der Beendigung eines Arbeitsverhältnisses erlischt die Einwilligung nicht, soweit sie unbefristet erteilt worden ist. Eine solche Einwilligung ist auch nicht automatisch auf die Dauer des Arbeitsverhältnisses beschränkt. Die Richter weisen weiterhin darauf hin, dass eine Einwilligung ohne Widerrufsvorbehalt nur dann widerrufen werden kann, wenn dafür ein plausibler Grund vorliegt.

Das aktuelle Urteil: Einwilligung bei der Veröffentlichung von Bildern

In einer Pressemitteilung vom 20. August 2015 teilt das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) mit, dass gegen ein Unternehmen eine Geldbuße in fünfstelliger Höhe wegen einer unzureichenden Auftragserteilung im Rahmen der Auftragsdatenverarbeitung festgesetzt worden ist. Nach Auffassung der Behörde hätten die technischen und organisatorischen Maßnahmen des Auftragnehmers (Datensicherheitsmaßnahmen) in dem Vertrag genauer beschrieben werden müssen. Stattdessen enthielt der Vertrag nur wenige pauschale Aussagen und Wiederholungen des Gesetzestextes. Dies genügte der Aufsichtsbehörde nicht. Der Präsident des BayLDA weist darauf hin, dass auch zukünftig solche Verstöße mit Geldbußen geahndet werden. Behördliche oder betriebliche Datenschutzbeauftragte sollten die Auftragsdatenverarbeitung rechtlich neu bewerten, wenn bisher die Datensicherheitsmaßnahmen der Auftragnehmer nicht im Einzelnen geprüft worden sind.

Praxistipp Datenschutz: Löschung und Sperrung von personenbezogenen Daten

Die Löschung personenbezogener Daten ist ein Kernelement des Datenschutzrechts. Für Behörden und Unternehmen stellt sich die Frage, wann, welche Daten von wem zu löschen bzw. zu sperren sind? Teilweise müssen unbestimmte Rechtsbegriffe ausgelegt werden und die Praxis zeigt, dass diese letzte Phase der Datenverarbeitung zu Beginn wenig beachtet wird. Zudem normierte der Gesetzgeber unterschiedliche Löschfristen, was ggf. einen internen Abstimmungsprozess zwischen unterschiedlichen Abteilungen oder Systemen notwendig macht.
Ohne ein Lösch- und Sperrkonzept kann eine verantwortliche Stelle dieser Herausforderung kaum gerecht werden. Die Entwicklung und Pflege eines solchen Konzepts ist zwingende organisatorische Maßnahme zur Sicherstellung eines angemessenen Datenschutzniveaus. Tipps zur Erstellung eines Lösch- und Sperrkonzepts.

Thomas Feil ist seit 1994 Rechtsanwalt. Er ist Fachanwalt für IT-Recht und Arbeitsrecht. Weitere Spezialisierungen sind das Datenschutzrecht, Urheberrecht, Wettbewerbsrecht und das Markenrecht. Haben Sie auch Themenvorschläge, Fragen oder Urteile, die wir in dieser Rubrik aufführen und erörtern können? Dann schreiben Sie uns: **info@cyber-akademie.de**.

Foto: privat

IMPRESSUM

Herausgeber: Cyber Akademie GmbH, Geschäftsführer: R. Uwe Proll (presserechtlich verantwortlich); Leiter der Cyber Akademie: 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 , Angela Götze, Sebastian Lahr (Berlin)
Programmbeirat: Dr. Bernd Benser, Chief Business Officer GridLab GmbH; Dr. Gerd Landsberg, Geschäftsführendes Präsidialmitglied des Deutschen Städte- und Gemeindebundes (DStGB); Olivier Burgersdijk, 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, Erster Polizeihauptkommissar im Polizeipräsidium Nordhessen, Landesbezirksvorsitzender der Gewerkschaft der Polizei (GdP) in Hessen ; Dieter Schürmann, Landeskriminaldirektor im Ministerium für Inneres und Kommunales NRW