CAk report

Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 31 /April 2016

Neues Seminar der Cyber Akademie

Best Practices IT-Audit: Rechtliche Risiken in der IT

Am 24. Mai 2016 veranstaltet die Cyber Akademie das Seminar Best Practices IT-Audit: Was ein Prüfer über IT und Recht wissen muss in Berlin.

Immer mehr Wirtschaftsprüfer, Rechnungshöfe, Innenrevisionen und andere Kontrollinstanzen müssen sich zunehmend mit juristischen Fragestellungen rund um die Informationstechnologie, das Internet und neue Medien befassen. Das neue, seit dem 25.7.2015 geltende IT-Sicherheitsgesetz zeigt deutlich, dass Unternehmens- und Behördenleitungen sich nicht darauf verlassen können, dass die IT-Abteilung alle technischen, organisatorischen und juristischen Fragen und Risiken im Griff hat.

Das Seminar greift die Problematik auf und behandelt die Themen „Datenschutz“ und „IT-Sicherheit“ und stellt Verbindungen zwischen den Grundsätzen der Ordnungsmäßigkeit der Buchführung auf und informiert über technische und organisatorische Aspekten des IT-Betriebs und der Informationssicherheit. Durch die steigende Digitalisierung von Geschäftsprozessen sind Fragen der Ordnungsmäßigkeit elektronischer Buchführung auch für Prüfer von immer größerer Relevanz.

Das Seminar richtet sich gezielt an Prüfer, die rechtliche Aspekte im Zusammenhang mit der IT-Abteilung prüfen und bewerten müssen, sei es aus Sicht eines Wirtschaftsprüfers, eines Rechnungshofes oder einer internen Kontrollinstanz.
Weitere Informationen sowie die aktuelle Seminarbroschüre finden Sie hier.

Weitere Termine und Orte:

- 24. Mai 2016, Berlin
- 6. September 2016, Düsseldorf
- 24. November 2016, Hamburg

INHALT

CAk-SEMINARE 2016

Hacking-Methoden in der Praxis: Vorgehen des Angreifers und Schutzmaßnahmen
03.–04.05.2016, Stuttgart

Grundlagen der Kryptologie
10.–11.05.2016, Bonn

Das neue IT-Sicherheitsgesetz
19. 05.2016, Düsseldorf

EU-Datenschutzgrundverordnung
31.05.2016, München

BSI-Grundschutz in der Praxis
31.05.–01.06.2016, Berlin

ITSVO-EKD – Informationssicherheit in Einrichtungen der evangelischen Kirche
31.05.–31.05.2016, Hannover

www.cyber-akademie.de

Münchner Cyber Dialog 2016

Deutschland sicher vernetzt!? – Sichere Digitalisierung in Staat, Wirtschaft und Gesellschaft

Am 30. Juni 2016 veranstalten Cyber Akademie und Behörden Spiegel zum dritten Mal den Münchner Cyber Dialog, um mit hochrangigen Vertretern aus Politik, ITK-Wirtschaft, Industrie und (Sicherheits-)Behörden über die sichere Digitalisierung in Deutschland zu diskutieren.

In diesem Jahr werden CIOs aus Industrie und Verwaltung, Vertreter aus Bundes- und Landespolitik, IT-Sicherheitsverantwortliche, Unternehmensvorstände und Geschäftsführer in München zusammenkommen, um sich über den strategischen Faktor IT-Sicherheit für die zukunftsorientierte Entwicklung der deutschen Wirtschaft, Industrie und Verwaltung in Zeiten der Digitalisierung auszutauschen.

Industrie 4.0 und Internet of Things (IoT)

Die diesjährige Hannover-Messe findet ganz im Zeichen der Digitalisierung in der industriellen Fertigung statt. Pünktlich zur Messe hat die EU-Kommission ihre Maßnahmen zur Digitalisierung der Industrie und zur digitalen Transformation der europäischen Wirtschaft vorgelegt. Deutschland und die USA sind zwei der führenden Nationen bei Industrie 4.0, also dem Zusammenwachsen von ITK, dem Internet und der klassischen Fertigungsindustrie. Während deutsche Unternehmen in traditionellen Industriebereichen oftmals führend sind, kommen die Weltmarktführer der ITK-Branche zu großen Teilen aus den USA. (Nicht nur) in Deutschland verbinden Unternehmen und Politik große Hoffnungen mit der Entwicklung von der klassischen zur vernetzten Produktion. Deutschland verfügt über eine industrielle Basis, einen innovativen Mittelstand und eine vergleichsweise gute IT-Infrastruktur. Ein Nachteil ist jedoch, dass mit der Vernetzung auch die Angriffsmöglichkeiten zunehmen.

Professionalisierung der Angreifer

In der Tat werden Unternehmen, staatliche Institutionen und Forschungseinrichtungen in Deutschland und seinen europäischen Partnerstaaten immer häufiger Ziel von Cyber Attacken. Diese können kriminellen oder nachrichtendienstlichen Ursprungs sein. Erst jüngst warnte das Bundesamt für Verfassungsschutz (BfV) vor nachrichtendienstlichen Aktivitäten aus Russland, die auf Politik, Industrie und Forschung abzielten. Ziel der elaborierten Angriffe seien die Informationsgewinnung und die Know-how-Abschöpfung für die eigene Wirtschaft. Schwerpunkte würden u.a. auf Energie- und Militärtechnik, aber auch auf Luft-und Raumfahrt darstellen. Der Schaden, der durch Cyber-Attacken entsteht, wird allein für Deutschland auf bis zu 50 Mrd. Euro beziffert.

Defizite in Deutschland

Gerade der starke Mittelstand und die vielen „hidden champions“ in Deutschland sind interessante Angriffsziele für Cyber Kriminelle und staatlich gelenkte Angriffe. Doch nicht nur die kleinen und mittelständigen Unternehmen (KMU) in Deutschland, auch die Kommunen und viele Betreiber Kritischer Infrastrukturen haben Nachholbedarf bei der Digitalisierung und benötigen Unterstützung bei der Erhöhung ihres IT-Sicherheitsniveaus. Dieses haben nicht erst die Angriffe mit Krypto-Trojanern u.a. auf Krankenhäuser, Kommunen und Behörden deutlich gemacht. Auf der anderen Seite ist zu konstatieren, dass Deutschland nicht nur Opfer von Angriffen wird, sondern seine oft nicht hinreichend geschützte Infrastruktur auch Ausgangspunkt und Mittel von Attacken ist.

Münchner Cyber Dialog 2016

Mit Blick auf den schnell voranschreitenden Digitalisierungsprozess in allen Sektoren und der wachsenden Cyber Bedrohungslage steht der der Erfahrungsaustausch zwischen Industrie, IKT-Branche und Politik/Verwaltung zu folgenden Themen im Zentrum:

- **Industrie 4.0 und Internet of Things**
- **Digitalisierung und Sicherheit im Gesundheitswesen**
- **IT-Sicherheit in der Wertschöpfungskette**
- **Schutz Kritischer Infrastrukturen und Cyber-Defence**
- **IT-Sicherheit in Mittelstand und Kommunen**

Darüber hinaus werden Formen der Kooperation zwischen Staat und Unternehmen zur Erhöhung des IT-Sicherheitsniveaus auf nationaler und internationaler Ebene sowie die regulatorischen Rahmenbedingungen für eine sichere Digitalisierung diskutiert.

Weitere Informationen, das Programm und eine Anmeldemöglichkeit finden Sie unter: www.muenchner-cyber-dialog.de.

Referenten des Cyber Dialogs sind u.a.:

Dr. Michael Wilhelm, *CIO des Freistaates Sachsen und Staatssekretär im Sächsischen Staatsministerium des Innern*

Arne Schönbohm, *Präsident des Bundesamts für Sicherheit in der Informationstechnik*

Dr. Hans-Joachim Popp, *CIO Deutsches Zentrum für Luft- und Raumfahrt e.V.*

Dr. Rolf Werner, *Vorsitzender der Geschäftsführung, Head of Central Europe, Fujitsu Technology Solutions GmbH*

Personaloffensive bei der Bundeswehr

Projekt Digitale Kräfte gestartet

(BS) Auf der Suche nach IT-Talenten stehen die Streitkräfte in Konkurrenz mit zahlreichen Arbeitgebern aus der Wirtschaft. Im Rahmen des "Wettbewerbs um die besten Köpfe aus dem IT-Bereich" hat die Bundeswehr Mitte März das Projekt Digitale Kräfte als Teil der Arbeitgeberkampagne "Mach, was wirklich zählt" gestartet.

Die Bundeswehr ist mit rund 21.000 militärischen und zivilen IT-Dienstposten bereits heute einer der größten IT-Arbeitgeber Deutschlands. Der Bedarf an Fachkräften aus dem Bereich der Informationstechnik ist weiterhin hoch und wird künftig noch steigen.

Moderne Waffensysteme sind heutzutage durch komplexe Netzstrukturen verbunden, in Gefechtsständen und Feldlagern sind hunderte Kilometer Kabel verlegt. Die Angehörigen der Bundeswehr verschicken rund 1,1 Millionen E-Mails pro Tag.

Foto: BS/Bundeswehr

Die neue Kampagne stellt Berufsbilder vor, welche die große Vielfalt an IT-Aufgaben in der Bundeswehr veranschaulichen sollen – vom IT-Soldaten über den Administrator bis hin zu Forschung und Entwicklung. Unter "IT-Soldaten" versteht man diejenigen, welche in einem Feldlager, bei einer Übung oder im Auslandseinsatz für die Kommunikation sorgen.

Auf allen Ebenen werden IT-Fachkräfte gesucht – besonders IT-Administratoren. Hier ermöglicht die Bundeswehr sowohl militärische als auch zivile Karrierechancen. Allein in diesem Jahr bietet sie rund 700 offene Stellen an.

IT-Sicherheit im Mittelstand

Studie zur Verschlüsselung bei KMU

(CAk) Das Bundeswirtschaftsministerium (BMWI) hat aktuell eine Studie zum Thema “Einsatz von elektronischer Verschlüsselung – Hemmnisse in der Wirtschaft” öffentlich ausgeschrieben.

Im Rahmen der Studie soll untersucht werden, welche Hemmnisse dem Einsatz von wirksamen Verschlüsselungsmechanismen entgegenstehen. Hierbei sollen insbesondere kleine und mittlere Unternehmen (KMU) betrachtet werden, da deren Nachholbedarf bzgl. IT-Sicherheitslösungen oftmals besonders hoch ist. Die Untersuchung soll daher auch das Spannungsfeld zwischen dem Vorhandensein technischer Lösungen und der Sensibilität für das Thema Datensicherheit einerseits und der kaum verbreiteten Anwendung von Verschlüsselung andererseits differenziert bei Unternehmen mit und ohne Anwendungserfahrung beleuchten. Außerdem sollen die rechtlichen Vorgaben für den Einsatz von Verschlüsselung branchenspezifisch zusammengestellt werden. Aus den Ergebnissen sollen anschließend gegebenenfalls gezielte Fördermaßnahmen zur Erhöhung des IT-Sicherheitsniveaus der KMU in Deutschland ableitbar sein.

Die Studie soll u.a. die Anwendungsbereiche bestimmen, in denen Verschlüsselungslösungen bei KMU unterschiedlicher Größe und aus unterschiedlichen Branchen zum Einsatz kommen, die rele-vanten Arten von Verschlüsselungslösungen identifizieren und eine entsprechende Übersicht erstellen. Im Zuge der Studie sollen zudem 100 ausgewählte KMU zur Nutzung von Verschlüsselungslösungen befragt werden. Hierbei sollen insbesondere auch die Gründe für die Nichtnutzung sowie bestehende Mängel bei der Nutzerfreundlichkeit im Fokus stehen. Darüber hinaus sollen durch die Befragung Hemmnisse, u. a. Auswirkungen auf den Arbeitsprozess, identifiziert werden.

Zudem soll die Anwenderfreundlichkeit vorhandener Verschlüsselungsangebote aus Nutzersicht und potenziell vorhandene rechtliche und organisatorische Anforderungen für deren Einsatz evaluiert werden. Hieraus sollen schließlich konkrete Orientierungshilfen für KMU für den Einsatz von Verschlüsse-lungslösungen erstellt werden.

Zum Thema Verschlüsselung bietet die Cyber Akademie am 10 und 11. Mai den Kurs Grundlagen der Kryptologie an.

Praxistipps der Cyber Akademie

Neues aus IT- und Datenschutzrecht

Vor dem Hintergrund der rechtlichen Anforderungen an die IT-Sicherheit und den Datenschutz, finden Sie an dieser Stelle aktuelle Informartionen, rechtliche Entwicklungen und Entscheidungen aus dem Bereich IT- und Datenschutz. 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.

↗ Wegfall der Landesdatenschutzgesetze und neue Bußgeldvorschriften für Behörden

Die EU-Datenschutzgrundverordnung (DS-GVO) ändert auch das Datenschutzrecht der Bundesländer. Ab Inkrafttreten im Frühjahr 2018 werden das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze (LDSG) hinfällig. Die bisherigen LDSGs sind nicht mehr anzuwenden und alle behördlichen Datenschutzbeauftragten in den Ländern und Kommunen müssen sich auf die neuen gesetzlichen Regelungen einstellen und diese umsetzen. Die Bußgeldregelungen der DS-GVO heben sich massiv von den für Behörden bisher geltenden Bußgeldregelungen der LDSGs ab. In vielen LDSGs war bisher von Bußgeldern bis zu maximal 50.000,00 Euro die Rede. Nach Artikel 83 Abs. 4 DS-GVO werden zukünftig Bußgelder von bis zu 10 Millionen Euro vorgesehen. Artikel 83 Abs. 5 sieht sogar für einige Datenschutzverstöße Bußgelder von bis zu 20 Millionen Euro vor. Die Bußgelder können Behörden treffen, wenn gegen Datenschutzbestimmungen der DS-GVO verstoßen wird. Deutlich fordert die DS-GVO in Artikel 83 Abs. 1, dass die Bußgelder wirksam und abschreckend sein sollen!

Einige Regelungen der DS-GVO können durch innerstaatliche Regelungen ergänzt und konkretisiert werden.

Video-Blog

CAk News in 100 Sekunden . . .

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 , Angela Götze, Rebecca Hesse (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, Landesbezirksvorsitzender der Gewerkschaft der Polizei (GdP) in Hessen ; Dieter Schürmann, Landeskriminaldirektor im Ministerium für Inneres und Kommunales NRW