CAk report

Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 26 / November 2015

Neue Seminare der Cyber Akademie

ISIS12 und IT-Sicherheit kompakt

IT- Sicherheit kompakt

Am **19. Januar 2016** veranstaltet die Cyber Akademie das neue Seminar ***IT- Sicherheit kompakt*** in Berlin. Das Seminar vermittelt Basiswissen und Handlungsempfehlungen zur Umsetzung des **IT-Sicherheitsgesetzes**. Für viele Verantwortliche stellt sich die Frage, welche konkreten rechtlichen Anforderungen zu erfüllen sind und wie Maßnahmen zur IT-Sicherheit organisiert werden können. Das Seminar greift diese Fragestellung auf und gibt entsprechende Praxishinweise für die Umsetzung der aktuellen Anforderung an die Informationssicherheit in Unternehmen und Behörden. Die Teilnehmer erhalten einen Überblick über die aktuellen Standards zur Einrichtung eines **Informationssicherheitsmanagementsystems (ISMS)** und Kriterien für die richtige Auswahl. Das Seminar richtet sich an Unternehmen, Behörden, Kommunen sowie KRITIS-Betreiber. ***Weitere Informationen und Termine finden Sie hier.***

Informations-Sicherheitsmanagement-System in 12 Schritten

ISIS12 ist das vom Netzwerk Informationssicherheit für den Mittelstand des Bayrischen IT-Sicherheitsclusters entwickelte Verfahren für die Einführung eines Informationssicherheits-Management-Systems in 12 Schritten (**ISIS12**). Am **25. Februar 2015** veranstaltet die Cyber Akademie zu diesem Themenkomplex zum ersten Mal das Seminar ***ISIS12 für Kommunen*** in Berlin.

Häufig fehlen in Unternehmen und Behörden die Ressourcen, um sicherheitsrelevante Aufgaben auch ohne externe Dienstleister zu bewältigen. Auf diese Bedürfnisse ist das Seminar zugeschnitten und außerdem als Vorstufe zur Zertifizierung nach **BSI-Grundschutz** oder **ISO 27001** bestens geeignet. **ISIS12** wird in den Informationssicherheits-Management-Prozess integriert, ist jedoch weniger komplex als der IT-Grundschutz. Darüber hinaus enthält es klar formulierte Anweisungen, beispielsweise zur IT-Dokumentation und zum IT-Service-Management. **ISIS12** betrachtet nur wenige unternehmenskritische Anwendungen und wendet einen gegenüber dem IT-Grundschutz reduzierten **Maßnahmenkatalog** an. Das halbtägige Seminar richtet sich insbesondere an IT-Sicherheitsbeauftragte, CISOs, IT- und Sicherheitsverantwortliche, Führungskräfte und verantwortliche Personen aus dem Bereich Informationssicherheit. ***Weitere Informationen finden Sie hier.***

Weitere Termine:

- 16. Juni 2016, Bonn
- 22. September 2016, Hamburg
- 15. Dezember 2016, München

INHALT

CAk-Seminare 2015

Sensibilisierungskampagnen planen und durchführen
01.–02.12.2015, Nürnberg

Mobile Device Security – Risiken und Schutzmaßnahmen
01.–03.12.2015, München

Das neue IT-Sicherheitsgesetz
08.12.2015, Hannover

IT-Forensik -Spurensuche auf elektronischen Datenträgern
08.–10.12.2015, Stuttgart

Leitfaden zur Überprüfung der Informationssicherheit (IS-Revision)
09.–10.12.2015, Köln

www.cyber-akademie.de

Positionspapier vorgestellt

Fokusgruppe „Digitale Souveränität“ mit konkreten Forderungen

Maßnahmen der Fokusgruppe unter Leitung von Robert Lehner (Fujitsu, 3.v.r.) wurden von Netzpolitikern der Bundestagsfraktionen einhellig begrüßt.

Foto: Fujitsu/mc quadrat

Eine Woche vor Beginn des Nationalen IT-Gipfels in Berlin hat die Fokusgruppe „Digitale Souveränität“ ein Positionspapier vorgestellt. Ihr gehören Fujitsu, die Bundesdruckerei, die Initiative D21, Dataport, der Münchner Kreis, die Software AG sowie TNS Infratest an.

An der Veranstaltung nahmen auch die Bundestagsabgeordneten Hansjörg Durz (CSU), Thomas Jarzombek (CDU), Lars Klingbeil (SPD) sowie Konstantin von Notz (Grüne) an der Veranstaltung teil. Das Positionspapier basiert auf der Annahme, dass die Bürger und die Wirtschaft Verwaltungsdienstleistungen einfach, schnell, ortsunabhängig, wirtschaftlich, vertrauensbasiert und Infrastrukturabhängig nutzen wollen. Das vor diesem Hintergrund verfasste Positionspapier kommt zu mehreren Empfehlungen, um die gewünschte flexible Nutzung zu gewährleisten.

• Für besonders schutzwürdige Daten müsse ein Höchstmaß an Sicherheit gewährleistet werden, ohne dabei Abstriche bei der Bedienbarkeit zu machen.

• Der Bund sollte die Möglichkeiten des ressortübergreifenden Forschungsprogramms der Bundesregierung zur IT-Sicherheit nutzen und ausbauen.

• Politik und Verwaltung in Bund, Ländern und Kommunen sowie die IT-Wirtschaft sollten die Informations- und Aufklärungsarbeit im Bereich "Vertrauen und Sicherheit" vor allem mit Blick auf den Bürger verstärken.

• Politik und Verwaltung in Bund, Ländern und Kommunen sollten gemeinsam mit der IT-Wirtschaft die Relevanz der Themen E-Government und IT-Sicherheit für den Erfolg der IT-Sicherheit stärker betonen und in den Fokus der Öffentlichkeit rücken.

Rupert Lehner, Deutschland- und Europa-Chef von Fujitsu und Federführer der Fokusgruppe Digitale Souveränität, machte sich zudem für intelligente Sicherheitssysteme stark. „Dass die Wohnung besser gesichert ist, als der Gartenschuppen, ist jedem klar. Auch, dass im selben Haus die unterschiedlichen Wohnungen und Geschäfte unterschiedlich gesichert sein können. In der digitalisierten Welt gibt es dieses Verständnis noch nicht“, so Lehner.

Die Vertreter der Politik begrüßten das Positionspapier durchweg. Sie waren sich einig, dass der Bereich IT-Sicherheit zentraler Faktor für den erfolgreichen Ausbau der Digitalisierung ist.

„Durchgehende Ende-zu-Ende-Verschlüsselungen sind hier ein zentraler Baustein. Wo stünden wir heute, zwei Jahre nach den ersten Snowden-Enthüllungen, wenn wir diese Technik in die IT-Großprojekte der letzten Jahre implementiert hätten? Das wäre ein echter Exportschlager“, sagte von Notz.

Trotz der vorhandenen Einigkeit in vielen Punkten, richtete Lehner auch mahnende Worte an die Politik: „Es wird zu viel diskutiert und zu wenig gehandelt“

Lebhafte Diskussion auf dem Podium. Hier: Lars Klingbeil (SPD) (l.) und Dr. Konstantin von Notz (Grüne)

Foto: Fujitsu/mc quadrat

Aus- und Weiterbildungsangebot der Cyber Akademie

Neuer Seminarkalender 2016

Der neue **Seminarkalender der Cyber Akademie** für das Jahr 2016 ist da! Neben dem bereits im Juni gestarteten Seminar **Das neue IT-Sicherheitsgesetz**, welches sich einer positiven Resonanz sowohl bei großen und mittelständischen Unternehmen, KRITIS-Betreibern als auch Behörden erfreut, sind auch einige völlig neu konzipierte Seminare entwickelt und in das Ausbildungsprogramm aufgenommen worden. Hierzu gehören u.a. die Seminare **ISIS12 für Kommunen**, **IT- und Datenschutz als Führungsaufgabe**, **Update IT-Compliance**, **IT-Sicherheit kompakt** 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.

Weitere Informationen sowie den aktuellen Seminarkalender finden Sie hier.

Veranstaltungshinweis

KONGRESS

IT SICHERHEITSTAG NRW

2. DEZEMBER 2015
HUGO JUNKERS HANGAR
MÖNCHENGLADBACH

Am ***2. Dezember 2015*** veranstaltet die IHK des Landes Nordrhein-Westfalen in Mönchengladbach einen Kongress, der zum einen eine Austauschplattform zwischen Wissenschaft, Wirtschaft und Initiativen bietet und zum anderen konkrete Tipps und Hilfestellungen für Unternehmen gibt. Mit Impulsvorträgen, Fachforen und Seminaren geben Experten eine Übersicht zu den aktuellen Fragestellungen und bieten die Möglichkeit zum Fachlichen Austausch. In der begleitenden Ausstellung können individuelle Gespräche mit Lösungsanbietern zur digitalen Sicherheit geführt werden.

Weitere Informationen sowie eine Anmeldemöglichkeit finden Sie hier.

Cloud Computing

Microsoft Cloud-Dienste aus deutschen Rechenzentren

Microsoft wird seine Dienste Azure, Office 365 und Dynamics CRM Online künftig auch aus Rechenzentren in Magdeburg und Frankfurt am Main anbieten. Mit diesem Schritt reagiert Microsoft auf die gestiegene Nachfrage an Cloud-Diensten in und aus Deutschland. Laut BITKOM-Studie „Cloud Monitor 2015“ erwarten 83 Prozent der deutschen Unternehmen, dass ihr Cloud-Anbieter seine Rechenzentren ausschließlich in Deutschland betreibt.

Der Zugang zu den Kundendaten, die in den neuen Rechenzentren gespeichert werden, soll bei einem Datentreuhänder, in diesem Falle die Telekom-Tochter T-Systems, liegen. Ohne Zustimmung des Datentreuhänders oder des Kunden hat Microsoft keinen Zugriff auf Kundendaten.

Die neuen Angebote sollen sich in erster Linie an Organisationen und Unternehmen in datensensiblen Bereichen wie dem öffentlichen, dem Finanz- oder dem Gesundheitssektor richten. Der Datenaustausch zwischen den Rechenzentren findet über ein privates, vom Internet getrenntes Netzwerk statt, womit der Verbleib der Daten in Deutschland gesichert ist. Um den Geschäftsbetrieb und die Wiederherstellung von Daten auch in Katastrophenfällen zu gewährleisten, findet ein kontinuierlicher Datenabgleich zwischen den geographisch getrennten Rechenzentren statt. Microsoft will seinen Kunden transparent darlegen können, wie und wo ihre Daten verarbeitet werden.

Die neuen Cloud-Dienste werden ab der zweiten Jahreshälfte 2016 im Markt ausgerollt. Sie stehen auch Kunden aus anderen europäischen Ländern (EU und EFTA) zur Verfügung. Bereits am Dienstag hatte Microsoft ein eigenes, lokales Cloud-Angebot für Großbritannien angekündigt. Außerdem hat das Unternehmen gerade den Ausbau seiner Rechenzentren in Irland und den Niederlanden abgeschlossen.

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**.

Das aktuelle Urteil: Schmerzensgeld bei heimlichen Bild- und Videoaufzeichnungen

Das Bundesarbeitsgericht (BAG) hat in einem Urteil vom 19.02.2015 (8 AZR 1007/13) deutlich gemacht, dass die Observation eines arbeitsunfähigen Arbeitnehmers durch einen Detektiv für den Arbeitgeber teuer werden kann. Wenn die heimliche Erstellung von Bild- und Videoaufzeichnungen den Beweiswert der Arbeitsunfähigkeitsbescheinigung nicht erschüttert hat, liegt eine schwere Persönlichkeitsrechtsverletzung des Arbeitnehmers vor, die eine Entschädigung nach sich zieht. In den Vorinstanzen hatte das Landesarbeitsgericht dem Arbeitnehmer eine Entschädigung i.H.v. 1.000,00 Euro zugesprochen. Dieses Schmerzensgeld wurde vom BAG nicht beanstandet.

Praxistipp Datenschutz: Was kommt nach dem Safe Harbor-Urteil des EuGH?

Unternehmen und Behörden beschäftigt nach der Entscheidung des Europäischen Gerichtshofes zu Safe Harbor die Frage, wie nun zukünftig mit Datenübermittlungen in die USA umzugehen ist. Dazu hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26.10.2015 ein Positionspapier veröffentlicht (**Link PDF: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/151026 Positionspapier_SafeHarbor.pdf**). Die Aufsichtsbehörden stellen nicht nur eine Datenübermittlung auf Basis von Safe Harbor infrage, sondern sehen auch den Einsatz der EU-Standardvertragsklauseln oder verbindliche Unternehmensregelungen (BCR) kritisch. Unternehmen und Behörden sind aufgerufen, bei einem Datentransfer in die USA die Verfahren datenschutzgerecht zu gestalten. Die Nutzung von US-Cloud-Angeboten ist für Unternehmen und Behörden ab sofort unzulässig, soweit personenbezogene Daten auf US-Servern gehostet werden, beispielsweise der Einsatz von Google-Drive, Apple-iCloud, Dropbox oder WhatsApp. Auch die Cloud-Services von Amazon und Microsoft sind betroffen, soweit US-Unternehmen auf europäische Rechenzentren Zugriff haben und damit die staatlichen Einrichtungen der USA auf europäische Rechenzentren zugreifen können.

Behördliche und betriebliche Datenschutzbeauftragte sollten sich daher unverzüglich einen Überblick verschaffen, inwieweit IT-Dienstleistungen von amerikanischen Unternehmen genutzt werden, die nach der aktuellen Situation unzulässig sind.

Datenschutzaufsicht fordert SSL-Verschlüsselung

Das Bayerische Landesamt für Datenschutzaufsicht fordert nach Presseberichten aktuell Unternehmen zum Einsatz von SSL-Verschlüsselung auf, wenn auf den Webseiten der Unternehmen Kontaktformulare verwendet werden.

Es wird gerügt, dass die personenbezogenen Daten, beispielsweise Name, Telefonnummer oder E-Mail Adresse unverschlüsselt übertragen werden. Gemäß § 9 BDSG ist auch die Übertragung personenbezogener Daten zu schützen. Diese Anforderung ergibt sich aus § 13 Abs. 7 Telemediengesetz. Dort hat der Gesetzgeber seit Juli 2015 ausdrücklich für Internetseiten die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gefordert.

Unternehmen und Behörden müssen daher unverzüglich notwendige Änderungen an den Internetseiten vornehmen, damit jede Datenkommunikation verschlüsselt stattfindet. Auch für die Webseite einer Behörde oder eines Unternehmens muss mindestens eine https- Verschlüsselung installiert sein.

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