CAk report

Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 19 / April 2015

Fortbildungswochen Juni 2015

IT-Risiko und IT-Nofallmanagement

Vom **15. bis 18. Juni 2015** findet in **Hannover** eine IT-Sicherheits-Woche statt! Mit der Dynamik der technischen Weiterentwicklungen, wächst auch das Spektrum an möglichen Risiken. Aufgabe eines ***IT-Risikomanagements*** ist es deshalb, die für eine Organisation maßgeblichen Risiken zu identifizieren, mögliche Konsequenzen zu bewerten, und Maßnahmen zu Risikominderung zu definieren und umzusetzen. Trotzdem bleiben Restrisiken bestehen und nur darauf zu hoffen, dass diese nie eintreten, wäre zumindest fahrlässig: Kommt es zum IT-Notfall, dann sind in kürzester Zeit Maßnahmen zu treffen, um Schäden zu begrenzen und zum Normalbetrieb zurückzukehren. Die ***IT-Notfallplanung*** beschreibt dazu entsprechende Prozesse, Maßnahmen und Verantwortlichkeiten bei Risikoeintritt. Notfallpläne, welche in der Schublade liegen und nie getestet wurden, zeigen ihre Wirksamkeit aber erst im Ereignisfall. ***IT-Notfallübungen*** bewirken hier über das Testen hinaus, dass alle Beteiligten mit den jeweiligen Abläufen vertraut gemacht werden und das Zusammenspiel praxisnah trainiert wird.

Die Seminare sind modular konzipiert, so dass auch die Teilnahme an einzelnen Seminaren möglich ist. ***Weitere Informationen finden Sie hier.***

Datenschutz-Praxiswoche

In der *Datenschutz-Praxiswoche* der Cyber Akademie, die vom **16. bis 18. Juni in Stuttgart** stattfindet, werden die Themen Verfahrensverzeichnis, Vorabkontrollen, Datenschutzaudits und IT-Grundlagen behandelt. Ziel ist es, dass die Teilnehmer in ihrer Organisation maßgeblich dazu beitragen, dass datenschutzrechtliche Verpflichtungen eingehalten werden und das Risiko von Datenschutzverstößen nachhaltig reduziert wird. Dabei wird sowohl auf das Bundesdatenschutzgesetz als auch auf das Landesdatenschutzgesetz der jeweiligen Teilnehmer eingegangen (bei Bedarf auch KDO, DSG-EKD!). Für Neueinsteiger empfehlen wir das Seminar ***Fahrplan für das erste Jahr als Datenschutzbeauftragte(r)***, dass einen einführenden Überblick über die ersten 12 Monate als Datenschutzbeauftragter gibt.

Weitere Termine:

- Verfahrensverzeichnis und Vorabkontrolle : 16.06.2015, Stuttgart
- Datenschutzaudits vorbereiten und durchführen: 17.06.2015, Stuttgart
- IT-Grundlagen für Datenschutzbeauftragte: 18.06.2015, Stuttgart

INHALT

CAk-Seminare 2015

IT-Forensik - Spurensuche auf elektronischen Datenträgern
05. – 07.05.2015, Frankfurt a.M.

Hacking-Methoden in der Praxis: Vorgehen des Angreifers und Schutzmaßnahmen
11. – 12.05.2015, Berlin

IuK-Strategien und Technologien
16. – 18.06.2015, Berlin

WLAN-Sicherheit - Drahtlos sicher in der Organisation und unterwegs
23. – 24.06.2015, Berlin

www.cyber-akademie.de

2. Akademie-Gespräch auf der CeBIT 2015:

Was bedeutet das IT-Sicherheitsgesetz für die Bundesländer?

Die Herausforderungen durch das IT-Sicherheitsgesetz waren Gegenstand des zweiten Akademie-Gesprächs der Cyber-Akademie auf der CeBIT. Das IT-Sicherheitsgesetz des Bundes wirft auch Fragen für Länder und Kommunen auf. Viele Betreiber Kritischer Infrastrukturen liegen in kommunaler Hand, auch wenn die Verwaltungen in Bund, Land und Kommune selbst keine Betreiber Kritischer Infrastrukturen nach dem Gesetz sein sollen.

Mit dem IT-Sicherheitsgesetz beträten Bund und Länder Neuland und der Weg sei bei der Abgrenzung der verschiedenen Regelungsbereiche voneinander nicht vorgezeichnet sagte Axel Köhler, CISO von Niedersachsen. Vor allem sei zu klären, welche Kriterien für die Beurteilung als Kritischer Infrastruktur praktisch anzuwenden seien und welche Infrastrukturen zu den kritischen gehören sollen. Auch sei eine Prognose, wie hoch das Meldevorkommen sein werde, nicht leicht.

Von den geschätzten 400 Betreibern von kommunalen Rechenzentren in Deutschland seien nur etwa 10% derzeit in der Lage, hohen den hohen Sicherheitsanforderungen des IT-Sicherheitsgesetzes derzeit gerecht zu werden und bei vielen

(v.l.n.r.) Axel Köhler, Thomas Feil, Florian Lindemann, Uwe Proll, Sven Schubert, Andreas Reichel, Reinhold Harnisch während des Akademie-Gesprächs

Foto: CAk/Giessen

Kommunen sei finanziell und personell der Mehraufwand nicht aufzubringen, sagte Reinhold Harnisch, Geschäftsführer des Kommunalen Rechenzentrums Minden-Ravensberg/Lippe (krz). „Kommunen sollten diese Aufgaben mit anderen Kommunen teilen aber auch Kompetenzen in der Zusammenarbeit mit den Ländern bündeln“, so Andreas Reichel, Vorstand Technik bei Dataport. Auch die Länder hätten große Probleme die Mittel für die Umsetzung des IT-Sicherheitsgesetzes aufzubringen, bestätigte Frank Müller, Informationssicherheitsbeauftragter von Mecklenburg Vorpommern. Außerdem würden bisherige Kommunikationsstrukturen zwischen Ländern und Betreibern durch das Gesetz aufgebrochen und alle Meldungen müssten an das Bundesamt für Informationssicherheit (BSI).

Einhellig wurde auf dem Akademie-Gespräch die Meinung vertreten, dass der Ernstfall eines Systemausfalls geübt werden müsse. Gemeinsam mit allen Beteiligten, horizontal und vertikal, privatwirtschaftlich und öffentlich, müsste die Zusammenarbeit intensiviert werden. Dieser hybride Ansatz kann den Herausforderungen eines Ernstfalls, der nicht auf Zuständigkeiten Rücksicht nimmt, vielleicht noch am ehesten begegnen.

CeBIT 2015:

Die Cyber Akademie auf der CeBIT

Auf der diesjährigen CeBIT in Hannover präsentierte sich auch die Cyber Akademie. Am Gemeinschaftsstand Niedersachsen im Public Sector Parc in Halle 7, informierten sich während der fünftägigen Messe Experten sowie Besucher aus dem privaten Sektor über Praxis-Workshops rund um die Informationssicherheit und Zertifikatslehrgänge zum Datenschutz- und IT-Sicherheitsbeauftragten.

Durch die Neuausrichtung der CeBIT auf die Geschäftswelt konnten im Vergleich zum Vorjahr nochmals mehr Kundenkontakte verbucht werden. Besonderes Interesse

Sebastian Lahr, CAk (Bildmitte) im Kundengespräch während der CeBIT 2015

Foto: CAk/Giessen

kam auch von Seiten der Sicherheitsorgane, die sich vor allem mit dem Thema IT-Forensik immer stärker auseinandersetzen müssen. Am 17.03.2015 fand zudem die Programmbeiratssitzung der Cyber Akademie statt. Neben der Weiterentwicklung der CAk und der Erörterung neuer Schwerpunktthemen, wurde auch die neue Leitung vorgestellt, welche zum 1. Februar dieses Jahres Florian Lindemann übernommen hat.

Cyber-Attacke auf TV5 Monde:

Frankreich im Visier von Cyber-Dschihadisten

In der Nacht vom 8. auf den 9. April wurde der französische Nachrichtensender TV5 Monde zum Ziel eines massiven und professionell vorbereiteten Hackerangriffes. Während die Sicherheitsbehörden von einer terroristischen Attacke ausgehen, sind die Folgen des Cyber-Angriffs noch nicht absehbar.

Gespannt schaut die Welt wieder nach Frankreich. Nach dem blutigen Terroranschlag auf das Satire-Magazin „Charlie-Hebdo“ scheint das Land nun Ziel einer cyber-terroristischen Attacke geworden zu sein. Bereits seit Januar 2015 war eine vermehrte Anzahl von Cyber-Angriffen auf öffentliche Einrichtungen – besonders auf Rathäuser – registriert worden.

Der öffentlichkeitswirksame Angriff, zu dem sich die islamistische Gruppe „Cyber-Kalifat“ bekannte, begann am 8. April gegen 21 Uhr und legte den Sender TV5 Monde lahm. Gleichzeitig wurden die Netzauftritte gekapert und Propagandamaterial des IS verbreitet. Zudem sei nach Aussage des IT-Direktors des Senders, Pierre Verines, die angerichtete Zerstörung an der IT-Infrastruktur „phänomenal, massiv und beeindruckend“. Gegenwärtig versucht der Sender mit IT-Experten der staatlichen IT-Sicherheitsagentur ANSSI (Agence nationale de sécurité des systèmes d’information) den Angriff zu analysieren und die Schäden zu beziffern.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) befürchtet, dass der Angriff in Frankreich auch in Deutschland Nachahmer finden könnte. Mit Blick auf den Angriff auf TV5 Monde erklärte BSI Vizepräsident Andreas Könen im ARD-Morgenmagazin, dass die Medienbranche ebenfalls als Bestandteil Kritischer Infrastruktur betrachtet werden müssten.

Die Bundesregierung arbeitet aktuell an einem Gesetzesentwurf, um die Sicherheit informationstechnischer Systeme zu erhöhen. Kernelemente des Gesetzes sind u.a. die Einführung von Meldepflichten bei IT-Sicherheitsvorfällen, die Festlegung von Mindeststandards an die IT-Sicherheit von Kritischen Infrastrukturen sowie die Stärkung des BSI als zentrale Lage- und Warnstelle. Am 20. April befasst sich der Deutsche Bundestag in einer öffentlichen Anhörung mit dem Entwurf des IT-Sicherheitsgesetzes.

Fragen zum vorliegenden Gesetzentwurf können Sie auch gerne an uns richten. Unser Experte für IT-Recht, Herr Thomas Feil, wird in unserem Video-Blog jede Woche Fragen beantworten ***(siehe Seite 4)***.

Mit dem Vorgehen von Cyber-Kriminellen sowie der Anwendung adäquater Schutzmaßnahmen befasst sich das Seminar der Cyber Akademie ***Hacking Methoden in der Praxis***, welches am 11. und 12. Mai 2015 in Berlin durchgeführt wird. ***Weitere Informationen finden Sie hier.***

↗ Veranstaltungshinweis

FORUM Informationssicherheit für die Öffentlichkeit bei Infrastrukturausfällen

Unser Partner das Kompetenzzentrum für ***Kritische Infrastruktur (KKI)*** veranstaltet am 30.04.2015 ein Forum zum Thema „Informationssicherheit für die Öffentlichkeit bei Infrastrukturausfällen“ in Berlin. Weitere Informationen sowie das aktuelle Programm finden Sie ***hier.***

Cyber-Attacken auf Mobile Devices

Mit ihrer Verbreitung werden Smartphones auch zunehmend für Angreifer attraktiv. Auf dem Partnertag der ***Allianz für Cyber-Sicherheit (ACS)***, die beim Bundesamt für Sicherheit in der Informationstechnik angesiedelt ist, sprach neulich Jan Kok von Nokia Solutions and Networks GmbH & Co. KG darüber, dass trotz Sicherheitsmaßnahmen wie Firewalls auf mobilen Geräten nur 45% der Angriffe erkannt und abgewehrt werden. Das Mobile Security Labor von Nokia in Berlin konnte beobachten, dass in Europa nur ein Prozent der Mobilfunkgeräte betroffen sind, während es in Asien sieben Prozent sind. Auch in der Sommer- und Reisezeit steige die Zahl der Infektionen. Vermutet wird, dass im Ausland genutzte Mobilfunkgeräte Infizierungen mitrbingen bzw. deren Nummern und IP-Adressen in den ausländischen Netzen hinterlassen wurden. Kok empfiehlt daher statt eines Client-Approaches, also einer auf den Einzelkunden und sein Einzelgerät orientierten Sicherheitsstrategie und der Frage wie schädliche die Malware ist, lieber auf ein Monitoring mit Blick auf die Unregelmäßigkeiten zu setzen. Er nennt dies Network-Based-Approach. Es sei sinnvoller, geziehlt Investitionen dann zu tätigen, wenn unregelmäßige Verkehre identifiziert werden könnten, statt sich generell zu schützen. Zu diesem Thema bieten wir Ende Juni das Seminar ***Mobile Device Security – Risiken und Schutzmaßnahmen*** an.

Video-Blog

CAk nachgefragt…

Thomas Feil, Fachanwalt für IT-Recht, Datenschutzbeauftragter TÜV

Feil, Thomas
ist seit 1994 Rechtsanwalt. Er ist Fachanwalt für IT-Recht und Arbeitsrecht. Weitere Spezialisierungen sind das Datenschutzrecht, Urheberrecht, Wettbewerbsrecht und das Markenrecht. Thomas Feil beantwortet ab sofort regelmäßig Ihre Fragen rund um das Thema IT-Sicherheitsgesetz. Sie haben auch eine Frage zum IT-Sicherheitsgesetz? ***Dann stellen sie Ihre Frage hier!***

IMPRESSUM
Herausgeber: Cyber Akademie GmbH, Geschäftsführer: R. Uwe Proll; **Presserechtlich Verantwortlicher:** R. Uwe Proll
Geschäftsstelle: Friedrich-Ebert-Alle 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 (Berlin)
Programmbeirat: Dr. Bernd Benser, Chief Business Officer GridLab GmbH; Dr. Gerd Landsberg, Geschäftsführendes Präsidialmitglied des Deutschen Städte- und Gemeindebundes (DStGB); Troels Oerting, Assistant Director Europol, Head of 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; Andreas Schuster, Landesbezirksvorsitzender Brandenburg der Gewerkschaft der Polizei (GdP); Dieter Schürmann, Landeskriminaldirektor im Ministerium für Inneres und Kommunales NRW