CAk report
Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 35 August 2016

Neues Seminar der Cyber Akademie

Leitfaden zur Überprüfung der Informationssicherheit

Praxisnahe Anleitung zur Vorbereitung und Durchführung von IS-Revisionen

Nahezu alle Geschäftsprozesse von Behörden und Unternehmen werden durch IT-Verfahren unterstützt, Informationen werden digital verarbeitet und über IT-Netze übermittelt. Somit sind Wirtschaft, Verwaltung und auch Bürgerinnen und Bürger auf das einwandfreie und sichere Funktionieren der eingesetzten Informationstechnik angewiesen. Behörden und Unternehmen Sicherheitsmaßnahmen treffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, Anwendungen und Systemen zu gewährleisten und einen Schutz gegen Angriffe zu bieten. Alleinig regelmäßige Überprüfungen der etablierten Sicherheitsmaßnahmen – IS-Revisionen – liefern hierzu verlässliche Aussagen über die wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit von Sicherheitsmaßnahmen.
IS-Revisionen sind somit ein wesentliches Informations- und Steuerungsinstrument für die Verantwortlichen in Behörden und Unternehmen. Bundesbehörden sind zudem gemäß „Um-setzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (UP Bund) verpflichtet, mindestens alle drei Jahre eine umfassende IS-Revision durchzuführen.

Das Seminar vermittelt den Teilnehmern die Fähigkeiten, um

- den zu erwartenden Aufwand und Nutzen bei der Implementierung von IS-Revisionen in ihrer Institution zu bewerten,
- IS-Revisionen in Ihrer Institution selbst vorzubereiten und durchzuführen,
- entsprechenden IS-Revisions-Verpflichtungen (z. B. UP Bund) nachzukommen.

Die Teilnehmer können mit den erworbenen Seminarerkenntnissen wesentlich dazu beitragen, die Informationssicherheit in einer Institution zu erhalten und zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Wirtschaftlichkeit der Sicherheitsmaßnahmen und -prozesse zu optimieren.

Dazu werden im Seminar die Grundlagen der IS-Revision praxisnah erläutert:

- Es wird auf die einzelnen IS-Revisions-Arten wie Kurz-, Querschnitts- und Partialrevision eingegangen und deren Unterscheidungsmerkmale erläutert.
- Darüber hinaus wird die Methodik zur Durchführung einer IS-Revision von der Planung über die korrekte Durchführung bis hin zur Nachbereitung vermittelt.
- Das Seminar orientiert sich dabei am Leitfaden zur IS-Revision des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Das Seminar findet am **14. September in Berlin** statt. Weitere Informationen zu den Seminarinhalten finden Sie unter ↗ http://www.cyber-akademie.de/suche.jsp?suche=IS-Revision

INHALT

CAk-SEMINARE 2016

- Best Practices IT-Audit (06.09.)
- Informationssicherheit nach BSI-Grundschutz und ISO 27001 im Praxisvergleich (08.09.)
- Das neue IT-Sicherheitsgesetz (13.09.)
- Leitfaden zur Überprüfung der Informationssicherheit (14.09.)
- IT-Forensik – Spurensuche auf elektronischen Datenträgern (14.09.–16.09.)
- IT-Risiko- und IT-Notfallmanagement-Woche (19.09.–22.09.)
- Bertiebsrat und Datenschutz (20.09.)

www.cyber-akademie.de

Public IT-Security 2016

Cyber Akademie auf der PITS in Berlin

Unter dem Titel "IT-Sicherheit in der Tiefe" findet am 13./14. September 2016 der IT-Sicherheitskongress für den Public Sector im Hotel Adlon in Berlin statt. Zahlreiche IT- und IT-Sicherheitsverantwortliche aus Bund, Ländern und Kommunen werden dabei über die aktuelle IT-Sicherheitslage sowie technische, organisatorische und regulatorische Herausforderungen diskutieren.
Die Cyber Akademie wird auch in diesem Jahr mit einem Stand auf dem Leitkongress für IT-Sicherheit in der öffentlichen Verwaltung vertreten sein.

Wir würden uns freuen, Sie am Stand der Cyber Akademie begrüßen zu können und Ihnen die Leistungen der Cyber Akademie vorzustellen.

Weitere Informationen zum Kongress finden Sie unter
↗ www.public-it-security.de.

Lagebild Cybercrime des Bundeskriminalamtes 2015

Sicherheitsbehörden mit großem Nachholbedarf bei IT-Experten

Die Polizei braucht nach Einschätzung der Gewerkschaft der Polizei (GdP) gut ausgebildete IT-Experten. Zwar stelle das Internet als Kriminalitätsraum und Tatbegehungsmittel die Ermittler per-manent vor große und neue Herausforderungen, doch die eigentliche Schwierigkeit bestehe für die Polizei darin, Fachkräfte für diese Aufgabe bei den Sicherheitsbehörden zu gewinnen, sagte der GdP-Bundesvorsitzende und Programmbeirat der Cyber Akademie Oliver Malchow anlässlich des vom Bundeskriminalamt (BKA) veröffentlichten Bundeslagebildes „Cybercrime 2015“.

„Nach den Anschlägen und Gewalttaten der letzten Woche wird intensiv über die Abgründe des sogenannten Darknet diskutiert. Dieses mehr oder weniger geheime Netz ist für die Polizei kein Neuland. Erfolgreiche Ermittlungen beispielsweise im Bereich der Kinderpornografie haben das deutlich gezeigt. Da aber das Internet einen immer stärkeren Part in unserem Leben einnimmt, muss die Polizei auch dort, die immens wichtige Präventions- aber auch Ermittlungsarbeit leisten können“, sagte Malchow. Wenn er aber aus den Kollegenkreisen höre, dass derzeit die Polizei in den meisten Bundesländern für Informatiker nicht attraktiv sei, lasse das aufhorchen.

Zudem sei es ein Problem, so Malchow, dass qualifizierte Hochschulabgänger sich häufig zunächst im Öffentlichen Dienst Berufserfahrungen holen, um dann erheblich lukrativere Angebote aus der Wirtschaft anzunehmen. Die Länder und der Bund hätten durchaus schon einiges unternommen, um Spezialisten auf lange Sicht zu binden oder anzulocken. Die Wirklichkeit zeige aber, dass dies noch nicht ausreiche.

GdP-Chef Malchow appellierte an die verantwortlichen Politiker in Bund und Ländern, in dieser durch brutale Terrorakte und

Foto: CAk/Dach

entsetzliche Gewalttaten geprägten Zeit über den Tag hinaus zu denken und eine zukunftssichere Polizei zu stellen. „Es reicht nicht aus, jetzt unter dem Eindruck der Ereignisse zu versprechen, Tausende von Polizistinnen und Polizisten einzustellen zu wollen. Die Tätigkeit bei der Polizei muss auch für Experten attraktiver werden. Das hat auch mit der entsprechenden Vergütung zu tun“, betonte er.

Die GdP ist Gesellschafter der Cyber Akademie. GdP-Mitglieder, die sich im Rahmen der Cyber Akademie-Lehrgänge aus- und fortbilden möchten, können Sonderkonditionen in Anspruch nehmen.

U.a. folgende Seminare richten sich vor allem an Mitarbeiter von Polizei- und Sicherheitsbehörden:

↗ Mobile Device Security
↗ IT-Forensik – Spurensuche auf elektronischen Datenträgern
↗ Grundlagen der Kryptologie
↗ IuK-Notfallmanagement für die Polizei nach BSI 100-4

Awareness-Kampagnen planen und durchführen

Cyber Akademie schult Mitarbeiter kommunaler Landesverbände

Der Hacker-Angriff auf den Bundestag im Frühjahr 2015 wurde durch einen infizierten E-Mail-Anhang ausgelöst. Um Unternehmen und Behörden besser zu schützen, sollten sie ihre Mitarbeiter regelmäßig zum Thema Informationssicherheit sensibilisieren. Die Cyber Akademie führt jedoch nicht nur Awareness-Schulungen für Mitarbeiter von Behörden und Unternehmen an, sie bildet auch Multiplikatoren aus, die Sensibilisierungskampagnen in der eigenen Organisation planen und durchführen und mit relativ geringem Aufwand das Sicherheitsniveau deutlich erhöhen können.

Ende Juli führte die Cyber Akademie im schleswig-holsteinischen Bad Segeberg eine entsprechende Schulung für Mitarbeiter kommunaler Landesverbände durch. Tobias Henke berichtet von der Veranstaltung.

Für den Leiter des Seminars, Dr. Werner Degenhardt, Akademischer Direktor und CIO der Fakultät für Psychologie und Pädagogik der Ludwig-Maximilians-Universität München, ist die Frage, wie die IT die jeweilige Behördenleitung erreicht, von zentraler Bedeutung. Aussagen wie „Es funktioniert doch“, „Wofür braucht ihr das Geld?“ würden laut Degenhardt oftmals fallen, wenn sich die Leitung einer Behörde mit der IT-Abteilung unterhalte. Seminarteilnehmer Micha Mark Knierim sieht dies ähnlich. „Den Entscheidern muss der Nutzen verdeutlicht werden.“

Bis auf wenige Ausnahmen waren die Schulungsteilnehmer Mitarbeiterinnen und Mitarbeiter aus schleswig-holsteinischen Kommunalverwaltungen, die im Bereich Informationssicherheit beschäftigt sind und sich an einem landesweiten Projekt der kommunalen Landesverbände in Schleswig-Holstein beteiligen. Im Rahmen des Projektes werden die Empfehlung eines landesweiten kommunalen

Dr. Werner Degenhardt, Akademischer Direktor und CIO der Fakultät für Psychologie und Pädagogik der Ludwig-Maximilians-Universität München

Foto: CAk/privat

Mindestsicherheitsstandards und zahlreiche Hilfestellungen zu dessen Umsetzung erarbeitet. Die Entwicklung des Standards erfolgt in Anlehnung an das Modell ISIS 12 des bayerischen Sicherheitsclusters, das sich besonders an den Bedürfnissen von kleinen und mittleren Behörden orientiert, ergänzt um spezielle Anforderungen des schleswig-holsteinischen Unabhängigen Landeszentrums für Datenschutz und des Landesrechnungshofs.

Grundlagen zur Sensibilisierung von Mitarbeitern

Zunächst standen theoretische Grundlagen der Mitarbeitersensibilisierung im Vordergrund. Die Mehrzahl der Cyber-Vorfälle in der vergangenen Zeit, wie z. B. der Angriff auf den Deutschen Bundestag oder auf das Lukas-Krankenhaus in Neuss, wurden durch infizierte Mailanhänge ausgelöst. Die gefährlichsten Attacken werden in aller Regel mittels Social Engineering vorbereitet, d. h. die Täter suchen gezielt den Kontakt zu einzelnen Mitarbeitern und versuchen in vermeintlich belanglosen Gesprächen sicherheitsrelevante Dinge zu erfahren. Ein entscheidender Aspekt für das Gelingen einer Awareness-Kampagne ist die Einbindung der Leitungsebene. „Wie überzeuge ich die Behördenleitung?“, fragte der Projektleiter Frank Weidemann und brachte damit eine der zentralen Fragen auf den Punkt. Degenhardt sagte, dass es ratsam sei, die Entscheider nicht direkt anzusprechen, sondern dies zum Beispiel über die engsten Mitarbeiter der Behördenleitung zu tun.

Leitfaden für die Planung von Kampagnen und best practice Beispiele

Um herauszufinden, worauf eine Sensibilisierungskampagne konkret abzielen sollte, ist eine konkrete Bedarfsermittlung notwendig, welche zum Beispiel durch anonymisierte Umfragen erfolgen kann. Nach einer Risikoabschätzung, die das Verhältnis von Investitionen in die Kampagne mit ihren Maßnahmen im Vergleich zu möglichen Schäden durch Sicherheitsvorfälle untersucht, erfolgt eine Zielgruppenbestimmung für die Kampagne. Auf dieser Grundlage wird ein strukturierter Kampagnenplan mit Maßnahmen erstellt. Der letzte Schritt vor dem Start der Kampagne ist die Definierung von Zielen. Diese müssen eindeutig beschrieben und messbar sein. Um möglichst viele Teilnehmer einer Sensibilisierungskampagne zu erreichen, gibt es verschiedene Möglichkeiten. „Können die Maßnahmen auch privat genutzt werden?“, fragte Seminarteilnehmerin Anja Frank und machte auf einen Aspekt aufmerksam, der für die Eigenmotivation entscheidend sein kann. Eine pauschale Antwort auf diese Frage ist nicht möglich, da sich die private Nutzung von der IT der Mitarbeiter oft deutlich unterscheidet. Allerdings waren sich die Seminarteilnehmer einig, dass die Akzeptanz einer Maßnahme größer ist, wenn das Gelernte auch bei der Nutzung der privaten IT verwendet werden kann.

Als ein best practice Beispiel wurde den Seminarteilnehmern zunächst eine Awareness-Kampagne der Deutschen Telekom zum Thema Social Engineering gezeigt.

Hierbei wurde ein Mitarbeiter in einem Supermarkt in ein scheinbar belangloses Gespräch verwickelt, aus dem sein Gegenüber Rückschlüsse über seine Arbeit zog. In der anschließenden Diskussion waren sich die Teilnehmer des Seminars darin einig, dass ein Film ein gutes Mittel sei, um für IT-Sicherheit zu sensibilisieren. „Das Medium Film sind die Mitarbeiter vom heimischen Fernseher gewohnt“, so Knierim. Die Kampagne der Telekom erreichte insgesamt 40 Prozent der Mitarbeiter. Dies ist eine sehr gute Quote. Die Mitarbeiter zu verpflichten, macht laut Degenhardt keinen Sinn, da die Wahrscheinlichkeit groß sei, dass dann keine wirkliche Sensibilisierung stattfinde.

Messen des Erfolges

Teilnehmer Jan-Hendrik Pagel schilderte ein aus seiner Sicht problematisches Verhalten. „Manchmal ruft mich ein Mitarbeiter und sagt, er habe eine Fehlermeldung auf seinem Bildschirm gehabt. Wenn ich ihn dann frage, was es war, kommt als Antwort ‚Weiß ich nicht, hab ich weggeklickt‘“. An diese Aussage anknüpfend diskutierten die IT-Verantwortlichen abschließend die Frage, wann eine Kampagne für mehr IT-Sicherheit als Erfolg zu bewerten sei. Während Teilnehmer Friedrich Jürgensen sagte, es sei schon sehr viel erreicht, wenn die IT öfter angerufen werde, wünschte sich Teilnehmerin Angela Köhnke-Treptow, dass die Mitarbeiter nach einer guten Kampagne in der Lage seien, selbstständig zu entscheiden, ob sie beispielsweise Mails löschen sollen oder nicht.

Das nächste Seminar „Sensibilisierungskampagnen planen und durchführen“ findet am 28./29. November 2016 in München statt. Das Seminar kann auch als Inhouse-Veranstaltung gebucht werden.

Zur Mitarbeitersensibilisierung bietet die Cyber Akademie zudem das Praxisseminar „Security Awareness“ sowie „Live-Hacking als Security-Event“ für große Teilnehmergruppen an.

Für weitere Informationen senden Sie bitte eine Email an
↗ info@cyber-akademie.de

Schutz Kritischer Infrastrukturen

UP-KRITIS veröffentlicht Anforderungskatalog

Im Juli hat der UP-KRITIS einen Anforderungskatalog vorgelegt, welcher Betreibern Kritischer Infrastrukturen in Verhandlungen mit Lieferanten, Herstellern und Dienstleistern unterstützen soll. Ziel der „Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen“ ist es laut UP-KRITIS, die Informationssicherheit und Verfügbarkeit der kritischen Dienstleistungen gewährleisten zu können.

Während die KRITIS-Betreiber anhand des Katalogs Sicherheitsanforderungen mit Herstellern, Lieferanten und Dienstleistern vereinbaren sollten, sollen sich letztere an den Empfehlungen orientieren können, auf welche Anforderungen sie sich einzustellen haben, wenn sie Kritis-Betreibern Leistungen anbieten möchten.

Der vollständige Anforderungskatalog steht Ihnen hier zum Download bereit: ↗ http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Anforderungen_an_Lieferanten.pdf

Der Deutsche Bundestag hat im Sommer 2015 das IT-Sicherheitsgesetz verabschiedet. In dem Gesetz sind u.a. die Sektoren Energie, Finanzen, Gesundheit, IT- und Telekommunikation, Transport und Logistik sowie Ernährung als Kritische Infrastrukturen definiert.

Hinsichtlich der Anforderungen durch die europäische (NIS-Richtlinie) und nationale Regulierung (IT-Sicherheitsgesetz) bietet die Cyber Akademie u.a. folgende Leistungen für IT-Anwender, Dienstleister und Aufsichtsbehörden an:

Foto: CAk/© jro_grafik, fotolia.com

↗ Das IT-Sicherheitsgesetz – Inklusive Update Rechtsverordnung und NIS-Richtlinie (Informationsseminar)

↗ Umsetzung des IT-Sicherheitsgesetzes in der Praxis – Was ist zu beachten? (Consulting)

↗ Einführung von Informationssicherheits-Management-Systemen und ISMS Tools (Best Practice Schulungen)

↗ Best-Practice IT-Audit

↗ Ausbildung zum LEAD-Auditor

Cyber Akademie unterstützt WhiteIT Projekt

„Ankommen – So geht Deutschland“

Die Cyber Akademie unterstützt ein Projekt des Bündnisses White IT, welches unter der Schirmherrschaft der niedersächsischen Landtagsabgeordneten und Landesbeauftragten für Migration und Teilhabe Doris Schröder-Köpf (SPD) Flüchtlingskinder und ihre Familien über Kinderrechte in Deutschland aufklären und für mögliche Gefahren im öffentlichen Raum sensibilisieren will. Dazu gehören etwa die Ansprache und das Fotografieren durch Fremde und auch Verhaltenshinweise zur Prävention von Gewalt und ungewünschte körperliche Berührungen. In der Berliner Bundespressekonferenz wurde das Projekt Anfang August der Öffentlichkeit vorgestellt.

Stellten Anfang August das Kinderbuch „Ankommen – so geht das“ vor (v. l. n. r.): Rainer Becker, Vorsitzender der Deutschen Kinderhilfe; Thi Thai Hang Nguyen, Generalsekretärin des Diplomatic Councel; Doris Schröder-Köpf, Niedersächsische Landesbeauftragte für Migration und Teilhabe; R. Uwe Proll, Moderator und Chefredakteur Behörden Spiegel; Boris Pistorius, Niedersächsischer Minister für Inneres und Sport; Dr. Ralf Selbach, Vorstandsvorsitzende des Deutschen Roten Kreuzes Landesverband Niedersachsen. Foto: CAk/Einhaus

Niedersachsens Innenminister Boris Pistorius, ebenfalls Schirmherr des Buches, betonte: „Wir haben großes Vertrauen in Hilfsorganisationen und Polizei, es ist aber auch unsere Aufgabe, die Kinder selbst zu stärken, damit sie lernen, dass niemanden ihnen wehtun darf und dass sie ‚Nein!‘ sagen können“, erklärte. Es gehe auch darum, dass solche Straftaten künftig öfter zur Anzeige gebracht werden, um in die Statistik einzufließen und damit das Problembewusstsein in der Öffentlichkeit zu schärfen. Das vom Innenministerium unterstützte Bündnis „White IT“ konzentriert sich eigentlich auf den Umgang mit digitalen Medien und Inhalten. Gleichwohl sei ein Buch haptisch deutlich kindesnäher, erklärte Pistorius, den Nutzen werde es vor allem durch eine flächendeckende Verteilung geben.

In der Erstauflage sind bislang 15.000 Exemplare gedruckt, die bereits in den Einrichtungen des Deutschen Roten Kreuzes verteilt werden, zuerst in Niedersachsen, danach auch bundesweit. Das Bündnis White IT geht davon aus, dass bei entsprechender Nachfrage insgesamt 100.000 Exemplare durch die Deutsche Kinderhilfe und das Deutsche Rote Kreuz ausgegeben werden können.

White IT

Das interdisziplinäre Bündnis WhiteIT besteht aus über 70 Bündnispartnern aus Industrie und Handel, Strafverfolgungsbehörden, Gewerkschaften, Vereinen, Opferschutzverbänden, Wissenschaft und öffentlicher Hand. Ziel ist es, nachhaltige und wirkungsvolle Strategien zur Bekämpfung sexueller Gewalt gegen Kinder und deren Darstellung im Internet zu entwickeln und gemeinsam umzusetzen. Das Bündnis wurde im Jahr 2009 auf Initiative des niedersächsischen Innenministeriums gegründet. Die Geschäftsstelle WhiteIT wird weiterhin von dort aus geführt. WhiteIT setzt sich für die Verhinderung sexualisierter Gewalt gegen Kinder und deren digitale Abbildung ein.

Weitere Informationen zu der Aktion und dem Bündnis WhiteIT finden Sie auch unter ↗ www.whiteit.com .

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, 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