CAk update

Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 18 / März 2015

Juni 2015: Cyber Akademie veranstaltet Münchner Cyber Dialog

Zum zweiten Mal findet die Konferenz "Münchner Cyber Dialog" am 9. und 10. Juni statt. Die jährliche Konferenz ist eine Dialogplattform für Politik, Wirtschaft, Wissenschaft und Verwaltung, um die gesamtgesellschaftlichen Chancen und Risiken des Digitalisierungsprozesses zu erörtern. Die Cyber-Akademie will hochwertige, sichere und vertrauenswürdige IT-Infrastrukturen fördern und das Bewusstsein für die Bedeutung der IT-Sicherheit als Grundstein der gesamtwirtschaftlichen Entwicklung in Deutschland erhöhen. Deshalb veranstaltet die Cyber Akademie auch in diesem Jahr den Kongress, der als Katalysator gemeinsamer Anstrengungen zur sicheren Gestaltung des Digitalisierungsprozesses dient.

Repräsentative Umfrage:

Jedes dritte Unternehmen ist das Ziel von digitalen Angriffen

Nahezu jedes dritte (30 Prozent) Unternehmen in Deutschland verzeichnete in den vergangenen zwei Jahren IT-Sicherheitsvorfälle. Das hat eine repräsentative Umfrage im Auftrag des Digitalverbands BITKOM unter 458 Unternehmen ab 20 Mitarbeitern ergeben. Damit lag der Anteil der betroffenen Unternehmen exakt auf dem gleichen Niveau wie bei der entsprechenden Umfrage im Vorjahr. Laut Umfrage sind die IT-Sicherheitsvorfälle bei fast zwei Drittel (65 Prozent) der befragten Unternehmen „vor Ort“ verursacht worden (Vorjahr: 58 Prozent). Dabei handelt es sich zum Beispiel um gezielten Datenklau von aktuellen oder ehemaligen Mitarbeitern oder das Einschleusen mit Schadsoftware infizierter Datenträger. 40 Prozent der Unternehmen verzeichneten Angriffe auf ihre IT-Systeme über das Internet. Im vergangenen Jahr waren es erst 30 Prozent. In Anbetracht der gestiegenen Bedrohungslage bietet die Cyber Akademie im Juni gleich 11 Seminare von Vorbeugung bis zum Ernstfall, von Datenschutz bis Datensicherheit an.

CAk-Seminare 6/2015

Leitfaden zur Überprüfung der Informationssicherheit (IS-Revision)
10.–11.06.2015, Stuttgart

IT-Risikomanagement – Identifikation, Bewertung und Bewältigung von Risiken
15.–16.06.2015, Hannover

IT-Notfallplanung – Vorausschauende Vorbereitung auf den IT-Notfall
17.06.2015, Hannover

IT-Notfallübungen – In der Krise sicher handeln
18.06.2015, Hannover

Datenschutz-Praxis – Verfahrensverzeichnis und Vorabkontrollen
16.06.2015, Stuttgart

Datenschutz-Praxis – Datenschutzaudits vorbereiten und durchführen
17.06.2015, Stuttgart

Datenschutz-Praxis – IT-Grundlagen für Datenschutzbeauftragte
18.06.2015, Stuttgart

IuK-Strategien und -Technologien
16.–18.06.2015, Berlin

Datenschutz-Praxis – Fahrplan für das erste Jahr als Datenschutzbeauftragte(r)
25.06.2015, Frankfurt a.M.

WLAN-Sicherheit
23.– 24.06.2015, Berlin

Mobile Device Security – Risiken und Schutzmaßnahmen
30.06.– 02.07.2015, Berlin

www.cyber-akademie.de

10.–11. Juni 2015 in Stuttgart

Leitfaden zur Überprüfung der Informationssicherheit (IS-Revision)

Foto: Cak/ fotomek, fotolia.com

Zielsetzung

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,
- die Wirksamkeit und Wirtschaftlichkeit von Sicherheitsmaßnahmen zu optimieren,
- entsprechenden IS-Revisions-Verpflichtungen nachzukommen.

Dazu werden die einzelnen IS-Revisions-Arten erläutert und die Methodik von der Planung über die korrekte Durchführung bis hin zur Nachbereitung dargestellt. Das Seminar orientiert sich dabei am Leitfaden zur IS-Revision des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Zielgruppe

IT-Sicherheitsbeauftragte, IT-Leiter und Revisoren in Behörden, Unternehmen und bei entsprechenden IT-Dienstleistungsbetrieben.

Preis

550,– Euro zzgl. MwSt.

Veranstaltungsort

Stuttgart

Gegenstand des Seminars

Die Aktualität und Wirksamkeit von Sicherheitsmaßnahmen zählen vor allem im IT-Umfeld zu den Faktoren mit eng begrenztem Verfallsdatum. Regelmäßige Bestandsaufnahmen im Rahmen von IS-Revisionen helfen deshalb entscheidend bei der Umsetzung und der nachhaltigen Etablierung von Informationssicherheit in einer Behörde und Unternehmung. Folglich sehen auch die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ des IT-Planungsrates, der „Umsetzungsplan KRITIS“ und der „Umsetzungsplan Bund“ derartige Überprüfungen vor.

Referent

Jörn Maier, *Director Information Security Management bei HiSolutions AG ist auf die Auditierung und den Aufbau von Risiko- und IS-Managementsystemen nach ISO 27001 und BSI-Grundschutz spezialisiert. Er ist Certified Information Security Manager, Certified Information Systems Security Professional und BSI-lizensierter Auditteamleiter für Audits auf der Basis von BSI-Grundschutz.*

Mehr Informationen hier

15.–16. Juni 2015 in Hannover

IT-Risikomanagement – Identifikation, Bewertung und Bewältigung von Risiken

Foto: Cak/Orlando Florin Rosu , fotolia.com;

Angesichts der zunehmenden Bandbreite von Gefahren für die IT-Sicherheit ist es von elementarer Bedeutung, die für eine Organisation maßgeblichen Risiken zu identifizieren, mögliche Konsequenzen zu bewerten und Maßnahmen zur Risikominderung zu beschreiben und umzusetzen. Das Seminar gibt eine praktische Anleitung zur Durchführung von IT-Risikoanalysen und zur Definition von risikomindernden Maßnahmen und IT-Risikostrategien

Zielsetzung

Die Seminarteilnehmer erhalten einen umfassenden Überblick über die Anforderungen eines IT-Risikomanagements sowie die unterschiedlichen Ansätze und Methoden. Sie werden in die Lage versetzt:

- Gefährdungen im Rahmen einer Business Impact Analyse zu ermitteln,
- Kosten-Nutzen-Analysen durchzuführen,
- geeignete Maßnahmen im Rahmen einer IT-Risikostrategie zu planen und umzusetzen,
- die Wirksamkeit der Maßnahmen zu prüfen.

Die Teilnehmer lernen, Risikostrategien zu entwickeln und dabei die Balance zwischen Aufwendungen für risikomindernde Maßnahmen und Rest-Risiken zu finden.

Zielgruppe

IT-Sicherheitsbeauftragte,CISOs, IT- und IT-Sicherheitsverantwortliche, Business-Continuity-Manager, Risikomanager, Notfallmanager, Mitarbeiter aus Compliance und Controlling sowie Revision und Prüfungsämtern.

Preis

950,– Euro Endpreis
Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

Veranstaltungsort

Hannover

Referent

Björn Schmelter *ist Managing Consultant und Product Manager bei der HiSolutions AG mit langjähriger Erfahrung im Bereich Risikomanagement. Als Schwerpunkt seiner Tätigkeit begleitet er Unternehmen und Behörden bei der Einführung von Informationssicherheits-, Business Continuity- sowie Compliance Managementsystemen. Björn Schmelter ist u. a. Certified Lead Auditor für Managementsysteme nach ISO27001 und BS 25999, CISA, Enterprise Risk Manager (Univ.) und Mitautor des BSI-Standards 100-4 Notfallmanagement.*

Mehr Informationen hier

17.Juni 2015 in Hannover

Notfallplanung – Vorausschauende Vorbereitung auf den IT-Notfall

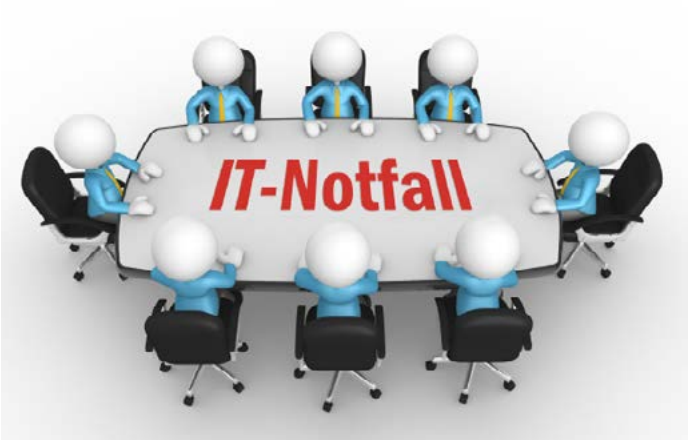

Foto: Cak/ Orlando Florin Rosu, fotolia.com

Zielgruppe

IT-Sicherheitsbeauftragte, CISOs, IT- und IT-Sicherheitsverantwortliche, Business-Continuity-Manager, Notfallmanager

Preis

530,– Euro Endpreis
Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

Veranstaltungsort

Hannover

Gegenstand des Seminars

Trotz bestmöglicher IT-Schutzmaßnahmen besteht immer ein Restrisiko. Für eine vorausschauende IT-Notfallplanung sollten deshalb die Maßnahmen beschrieben werden, die bei Eintreten eines IT-Notfalls einzuleiten sind, um den Schaden zu begrenzen und schnellstmöglich wieder zum Normalbetrieb zurückzukehren.
Die im Seminar vermittelten Best Practices zur Erstellung von IT-Notfallvorsorgekonzepten und -plänen befähigen dazu, im Notfall schnell und gezielt zu reagieren.

Zielsetzung

Die Seminarteilnehmer erhalten einen vertiefenden Einblick in Struktur und Wirkungsweise von Notfallvorsorgekonzepten und die Funktion der IT-spezifischen Anteile.
Die Erstellung, Beurteilung und Umsetzung von IT-Notfallplänen wird in allen Schritten praxisorientiert vermittelt. Dabei wird die Koordination der IT-Notfallplanerstellung mit den Fachbereichen außerhalb der IT und deren unterschiedlichen Anforderungen erläutert.
In praktischen Übungen erörtern die Teilnehmer Notfallvorsorgekonzepte und erlernen die Erstellung von IT-Notfallplänen.

Referent

Stephan Kurth *ist Consultant bei der HiSolutions AG. Der Schwerpunkt seiner Tätigkeit liegt in den Bereichen Business Continuity Management, Krisenmanagement, IT-Notfallmanagement und IT-Risikomanagement. Er hat zahlreiche Unternehmen und Behörden bei der Einführung, Überprüfung und Optimierung von Business Continuity Management-Systemen betreut. Herr Kurth ist Certified ISO 22301 Lead Auditor und ITIL-zertifiziert sowie Mitautor des Umsetzungsrahmenwerks zum Standard BSI 100-4 „Notfallmanagement" (UMRA BSI 100-4).*

Mehr Informationen hier

18. Juni 2015 in Hannover

IT-Notfallübungen – In der Krise sicher handeln

Foto: Cak/ Orlando Florin Rosu, fotolia.com

Zielgruppe

IT-Sicherheitsbeauftragte, CISOs, IT- und IT-Sicherheitsverantwortliche, Notfall- und Krisenmanager, Business-Continuity-Manager

Preis

530,– Euro Endpreis
Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

Veranstaltungsort

Hannover

Gegenstand des Seminars

IT-Notfallpläne greifen nur dann, wenn im Krisenfall alle Beteiligten mit den vorgesehenen Maßnahmen und ihren jeweiligen Aufgaben vertraut sind und das Zusammenspiel vorher trainiert wurde. IT-Notfallübungen sollten deshalb in regelmäßigen Abständen und auf allen Ebenen durchgeführt werden. In einer solchen Übung kann zudem überprüft werden, wie wirkungsvoll die Pläne zur Notfall- bzw. Krisenbewältigung sind.

Zielsetzung

In diesem Seminar werden die Teilnehmer mit den unterschiedlichen Übungsarten und deren Einsatzbereichen vertraut gemacht:

- technische Tests,
- Plan-Review,
- Planbesprechung,
- Stabsübungen,
- Stabsrahmenübungen,
- Kommunikations- und Alarmierungsübung,
- Simulation von Szenarien,
- Ernstfall- oder Vollübung.

In Workshops wenden die Teilnehmer die Methoden und Werkzeuge an und werden befähigt, IT-Notfallübungen in ihrer Institution selbst anzulegen, durchzuführen und auszuwerten.

Referenten

***Stefan Riegel** und **Kai Mettke-Pick** sind Managing Consultants bei der HiSolutions AG. Beide weisen langjährige Erfahrungen in der Beratung zu Krisen,- Notfall- und IT-Notfallmanagement, IT-Risikomanagement sowie Informationssicherheit auf. Ihre Tätigkeitsschwerpunkte liegen zudem im Aufbau von Übungs- und Testprogrammen für Notfall- und Krisenmanagement. Stefan Riegel ist Mitautor des Umsetzungsrahmenwerkes zum BSI-Standard 100-4. Kai Mettke-Pick war viele Jahre als Konzernkoordinator für Business Continuity Management bei einer großen deutschen Bank tätig.*

Mehr Informationen hier

16. Juni 2015 in Stuttgart

Verfahrensverzeichnis und Vorabkontrolle

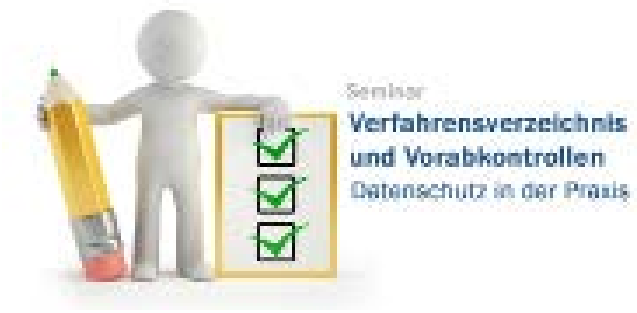

Foto: Cak /Art3D_fotolia.com

Gegenstand des Seminars

Viele Prozesse in Behörden und Unternehmen nutzen Verfahren zur automatischen Datenverarbeitung. Diese müssen in so genannten Verfahrensverzeichnissen dokumentiert werden, sobald personenbezogene Daten betroffen sind. Führt man sich vor Augen, dass unter automatischer Datenverarbeitung jegliche Prozesse zum Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen von Daten unter Einsatz von Datenverarbeitungsanlagen verstanden werden (dies schließt z. B. auch die Videoüberwachung ein!), dann werden Komplexität und Umfang deutlich.

Zudem verlangt der Gesetzgeber, dass hinsichtlich personenbezogener Daten besondere Risiken für die Rechte und Freiheiten der Betroffenen ausgeschlossen sein müssen! Im Zweifelsfall sind durch den Datenschutzbeauftragten Vorabkontrollen durchzuführen, welche die Unbedenklichkeit des jeweiligen Verfahrens ergeben bzw. entsprechende Schutzmaßnahmen definieren.

Zielsetzung

Die Teilnehmer werden befähigt, eigenständig Verfahrensverzeichnisse zu erstellen bzw. die Erstellung durch entsprechende Stellen zu koordinieren sowie Vorabkontrollen zu planen und durchzuführen. Folgende Inhalte werden dazu vermittelt:

- Grundlagen
- Meldepflichten
- Funktion und Arten von Verfahrensverzeichnissen
- Gesetzliche Anforderungen an Verfahrensverzeichnisse und Vorabkontrollen
- Folgen fehlender oder mangelhafter Verfahrensverzeichnisse beziehungsweise Vorabkontrollen
- Vorgehensweise bei der Erstellung und Pflege von Verfahrensverzeichnissen bzw. Durchführung von Vorabkontrollen

Das Seminar geht explizit sowohl auf das Bundesdatenschutzgesetz (BDSG) als auch auf die Landesdatenschutzgesetze (LDSG) der jeweiligen Teilnehmer ein (bei Bedarf auch KDO, DSG-EKD).

Zielgruppe

Datenschutzbeauftragte und -sachbearbeiter, zur Erstellung bzw. Prüfung von Verfahrensverzeichnissen verpflichtete Stellen sowie sonstige verantwortliche Personen aus dem Bereich Datenschutz

Preis

530,- Euro Endpreis

Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

Veranstaltungsort

Stuttgart

Referent

Michael Steiner, *Dipl.-Wirtschaftsjurist (FH) ist bei PERSICON legal GmbH als Consultant für Datenschutz und IT-Recht tätig und berät Behörden und mittelständische Unternehmen zu Fragen des betrieblichen Datenschutzes. Er verfügt zudem über die Qualifikationen Datenschutzbeauftragter (TÜV) und Datenschutzauditor (TÜV).*

Mehr Informationen hier

17. Juni 2015 in Stuttgart

Datenschutzaudits vorbereiten und durchführen

Foto: Cak/fotomek_fotolia .com

Gegenstand des Seminars

Nichts ist beständiger als der Wandel. Schon scheinbar kleine Veränderungen innerhalb einer Institution können erhebliche Auswirkungen auf die Wirksamkeit von implementierten Datenschutzmaßnahmen haben.

Dem gegenüber kann die Nichteinhaltung datenschutzrechtlicher Bestimmungen schnell zu hohen Strafen und einem massiven Imageverlust führen.

Nur eine ständige Überprüfung und Verbesserung der Datenschutzkonzepte und der organisationsinternen Prozesse im Bereich des Datenschutzes gewährleistet die Einhaltung datenschutzrelevanter Anforderungen und Regelungen in der Organisation und vermindert so nachhaltig das Risiko datenschutzrechtlicher Verstöße.

Eine Verpflichtung zur Prüfung besteht insbesondere für diejenigen Verfahren und Prozesse, welche bei externen Dienstleistern im Rahmen einer Auftragsdatenverarbeitung ausgelagert sind.

Integraler Baustein eines jeden Datenschutzmanagements sollte deshalb die regelmäßige Auditierung der eigenen Organisation und der ausgelagerten Verfahren und Prozesse auf die Einhaltung der datenschutzrechtlichen Bestimmungen sein.

Zielsetzung

Die Teilnehmer erhalten in diesem Seminar eine Anleitung mit Tipps aus der Praxis, um Datenschutzaudits innerhalb der eigenen Organisation und bei externen Dienstleistern kompetent selbst durchzuführen bzw. die Überprüfung durch externe Auditoren effizient vorzubereiten.

Das Seminar geht dazu auf die rechtlichen Grundlagen ein und vermittelt praxisnah Planung und Ablauf von Audits sowie die Dokumentation von Auditergebnissen.

Mit dem gewonnenen Know-how können die Teilnehmer in Ihrer Organisation maßgeblich dazu beitragen, dass datenschutzrechtliche Verpflichtungen eingehalten werden und das Risiko von Datenschutzverstößen nachhaltig reduziert wird

Zielgruppe

Führungskräfte, Datenschutzbeauftragte und verantwortliche Personen aus den Bereichen Datenschutz und Revision. Grundlagenkenntnisse zum Datenschutz werden vorausgesetzt

Preis

530,- Euro Endpreis

Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

Veranstaltungsort

Stuttgart

Referenten

Michael Steiner, *Dipl.-Wirtschaftsjurist (FH) ist bei PERSICON legal GmbH als Consultant für Datenschutz und IT-Recht tätig und berät Behörden und mittelständische Unternehmen zu Fragen des betrieblichen Datenschutzes. Er verfügt zudem über die Qualifikationen Datenschutzbeauftragter (TÜV) und Datenschutzauditor (TÜV).*

Oliver Goldstein *ist Volljurist und als Consultant im Bereich Compliance bei PERSICON legal GmbH tätig. Er studierte Rechtswissenschaften an der Freien Universität Berlin. Nach erfolgreichem Abschluss seines Zweiten Staatsexamens arbeitete er mehrere Jahre als Richter am Amtsgericht in der ordentlichen Gerichtsbarkeit des Landes Berlin. Dabei spezialisierte er sich auf den Bereich des Zivil- und Wirtschaftsrechts. So entwickelte er ein fundiertes Fachwissen vom Vertragsrecht über das IT-Recht bis zu den Aspekten des Europarechts.*

Mehr Informationen hier

18. Juni 2015 inStuttgart

IT Grundlagen für Datenschutzbeauftragte

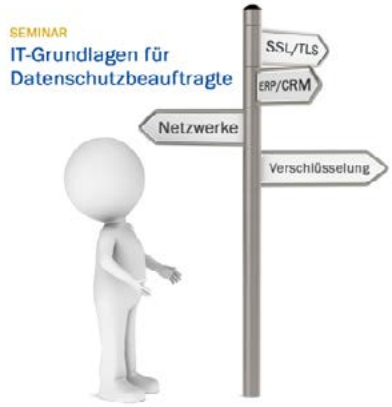

Foto: Cak/c_jojje11_fotolia.com

Zielgruppe

Betriebliche und behördliche Datenschutzbeauftragte sowie sonstige verantwortliche Personen aus dem Bereich Datenschutz.

Preis

490,- Euro zzgl. MwSt.

Veranstaltungsort

Stuttgart

Gegenstand des Seminars

Personenbezogene Daten werden mittlerweile zum Großteil elektronisch verarbeitet. Datenschutzbeauftragten fällt die Aufgabe zu, Verfahren der automatisierten Datenverarbeitung unter Datenschutzaspekten zu bewerten, diese in Verfahrensverzeichnissen zu führen, die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme zu überwachen sowie technische und organisatorische Schutzmaßnahmen vorzuschlagen und zu prüfen.

Zielsetzung

Das Seminar vermittelt die für Datenschutzbeauftragte erforderlichen IT-Grundlagen.
Unter Anwendung von praktischen Beispielen erwerben die Teilnehmer einen fachlich fundierten Überblick über die wichtigsten IT-Begriffe sowie deren Funktion und Anwendung in der Praxis. Das erlernte Wissen unterstützt die Teilnehmer wesentlich darin,

- technische Konzepte, Maßnahmen und Verfahren aus Datenschutzsicht hinsichtlich Zulässigkeit und Angemessenheit zu bewerten
- die eigenen Aufgaben in effizienter Koordination mit IT-Bereich und IT-Sicherheitsbeauftragten zu erfüllen.

Referent

Knud Brandis, *MBA, Vorstandsmitglied der PERSICON AG, ITIL Expert (APMG), Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Certified Information System Security Professional (CISSP), lizenzierter BSI-Grundschutzauditor, zertifizierter BSI-IS-Revisor, Mitautor der BSI-Grundschutzkataloge, Lehrbeauftragter an der Fachhochhochschule Brandenburg und der Dualen Hochschule Baden-Württemberg.*

Mehr Informationen hier

16.–18. Juni 2015 in Berlin

IuK-Strategien und -Technologien

Foto: © Nmedia, fotolia.com

Zielgruppe

IT-, IuK- und IT-Sicherheitsverantwortliche, CIOs, IT-Leiter, IuK-Architekten und -Administratoren

Preis

990,– Euro zzgl. MwSt.

Veranstaltungsort

InterCityHotel Berlin Hauptbahnhof
Katharina-Paulus-Str.5, 10557 Berlin

Gegenstand des Seminars

Voraussetzung für eine zielgerichtete, effiziente Nutzung von Informations-und Kommunikations- (IuK) Technologien in Behörden und Unternehmen ist die Beschreibung einer individuellen IuK-Strategie. Diese sollte die aktuellen und zukünftigen IuK-Anforderungen der Institution umfassend aufführen, Maßnahmen zur Anpassung der bestehenden Infrastruktur beschreiben und entsprechende Kostenund Sicherheitsaspekte adressieren.

Zielsetzung

Das Seminar vermittelt die technischen und konzeptionellen Grundlagen zur Strategiedefinition bzw. -aktualisierung. Dabei setzt es sich mit grundsätzlichen und aktuellen Fragestellungen auseinander, wie z. B. Nutzung von Open Source-Soft- und Hardware, Bring Your Own Device, Social Media, Virtualisierung und Cloud-Computing.

Die Teilnehmer werden dazu befähigt,

- die Einsatzmöglichkeiten neuer Technologien zu erkennen,
- die möglichen sicherheitsrelevanten Auswirkungen von IuK-Entwicklungenfür den eigenen Bereich adäquat zu beurteilen,
- den Anpassungsbedarf bestehender Strukturen zu identifizieren,
- die damit verbundenen Aufwendungen abzuschätzen,
- fachkundig strategische Technologieentscheidungen zu treffen und IuK-Strategien zu entwerfen.

Referent

Herbert Miosga, *Fachberater für IuK-Strategien und Kommunikationssysteme in der öffentlichen Verwaltung, verfügt über mehr als 35 Jahre IuK-Erfahrung.*
Seine aktuellen Tätigkeitsfelder sind End-to-End-Architekturen und -Management, IuK-Sicherheitsmanagement, TCP/IP-Konvergenz und IPv6. Darüber hinaus gehören schichtenorientiertes Service-Management für Internet- und Cloud-basierte IuK-Strukturen zu seinem Kompetenzportfolio. Herr Miosga hat an zahlreichen nationalen und internationalen Architektur- und Netzprojekten maßgeblich mitgewirkt.

Mehr Informationen hier

25. Juni 2015 in Frankfurt a.M.

Datenschutz-Praxis – Fahrplan für das erste Jahr als Datenschutzbeauftragte(r)

Foto: Cak/Reimer – pixelvario, fotolia.com

Gegenstand des Seminars

Hilfe, jetzt bin ich Datenschutzbeauftragte(r)! Dies ist ein Gedanke, den viele Datenschutzbeauftragte nach der Beauftragung beschleicht. Rechtliche und technische Grundkenntnisse rund um den Datenschutz sind das eine, die praktische Umsetzung in der Behörde ist der zweite Schritt, der dann folgen muss. Oftmals hat man aus zeitlichen oder Ressourcengründen nur einen Anlauf, um es richtig zu machen.

Hier erleben viele Datenschutzbeauftragte Mühen und zum Teil Überforderungen, da ihnen die Erfahrung fehlt, die umfangreichen Aufgaben in einem durchdachten Handlungsplan zu strukturieren und effizient umzusetzen.

Zielsetzung

Das Seminar vermittelt anschaulich die wesentlichen Handlungen, welche ein Datenschutzbeauftragter im ersten Jahr seiner Aktivität durchführen sollte, um eine wirksame Datenschutzorganisation zu etablieren.

Zu den Inhalten gehören u. a. Verfahrensdokumentation, Richtlinienerstellung, Datenschutzhandbuch, Steuerung von Dienstleistern, Awareness-Maßnahmen, Anfragenbearbeitung und Audits. Die Teilnehmer werden befähigt, einen eigenen „Fahrplan" für das erste Jahr mit Prioritätensetzung auszuarbeiten.

Das Seminar geht sowohl auf das Bundesdatenschutzgesetz (BDSG) als auch auf die Landesdatenschutzgesetze (LDSG) der jeweiligen Teilnehmer ein.

Zielgruppe

Betriebliche und behördliche Datenschutzbeauftragte und -sachbearbeiter bzw. -koordinatoren, welche möglichst über datenschutzrechtliches Grundwissen verfügen.

Preis

530,– Euro Endpreis

Das Seminar ist als Schul- und Bildungsleistung nach § 4, Nr. 21, Buchstabe a, Doppelbuchstabe bb des Umsatzsteuergesetzes von der Umsatzsteuer befreit.

Veranstaltungsort

Frankfurt a.M.

Referent

Thomas Feil, *Fachanwalt für IT-Recht und Arbeitsrecht, ist seit 1994 Rechtsanwalt und berät Behörden in datenschutzrechtlichen Fragen. Er ist TÜV-zertifizierter Datenschutzbeauftragter und verfügt über jahrelange Erfahrung in der Durchführung von Seminaren und Workshops zum Thema Datenschutz.*

Mehr Informationen hier

23.–24. Juni 2015 in Berlin

WLAN-Sicherheit

Foto: Cak/ mipan, fotolia.com

Zielgruppe

IT-Sicherheitsbeauftragte, IT- und IT-Sicherheitsverantwortliche, IT-Administratoren, Datenschutzbeauftragte, Sicherheitsbehörden, Anwender mobiler Endgeräte.

Netzwerk-Grundkenntnisse sollten vorhanden sein

Preis

790,– Euro zzgl. MwSt.

Veranstaltungsort

InterCityHotel Berlin Hauptbahnhof
Katharina-Paulus-Straße 5, 10557 Berlin

Gegenstand des Seminars

Drahtlose Netzwerke tragen dem Mobilitätstrend Rechnung und sind spätestens mit dem Erfolg von Smartphones und Tablets Standard geworden, bringen aber auch Sicherheitsprobleme mit sich: Beim WLAN-Einsatz in einer Organisation können die internen Strukturen nach außen sichtbar und angreifbar werden. Übertragene Daten können von Dritten empfangen, aufgezeichnet und manipuliert werden. Zudem gehen die Anwender mobiler Geräte bei der Nutzung öffentlicher WLANs entsprechende Risiken ein und gefährden Daten und Prozesse der eigenen Organisation.

Zielsetzung

In diesem Seminar erfahren die Teilnehmer, wie man

- sichere drahtlose Netzwerke aufbaut und
- WLAN-Clients so betreibt, dass die Risiken bei WLAN-Verwendung minimiert werden.

Neben der Betrachtung der WLAN-Technologie und den Möglichkeiten zur sicheren Umsetzung wie Authentisierung und Verschlüsselung wird auch auf entsprechende Bedrohungen durch Angreifer eingegangen. Dazu werden die Angriffsmöglichkeiten exemplarisch demonstriert.

Referenten

Tobias Elsner, *IT Security Resulter der @-yet GmbH führt IT-Sicherheitsüberprüfungen bei Behörden und Unternehmen durch. Er verfügt über langjährige Erfahrung als IT-Berater in den Bereichen IT-Infrastruktur, IT-Security und Servervirtualisierung und besitzt die Qualifikation EC Council Certified Ethical Hacker.*

Nils Hemmann, *IT Security Resulter der @-yet GmbH führt IT-Sicherheitsüberprüfungen bei Behörden und Unternehmen durch. Er verfügt über mehr als 15 Jahre allgemeine Erfahrung in der IT, davon mindestens sechs Jahre als Berater und Projektleiter im Bereich der IT-Security.*

Mehr Informationen hier

30. Juni – 2. Juli 2015, Berlin

Mobile Device Security – Risiken und Schutzmaßnahmen

Foto: Cak/Texelart , fotolia.com; Illustration: Behörden Spiegel-Gruppe

Smartphones, Tablets und Notebooks bieten hohe Mobilität und Flexibilität, bringen aber auch besondere Sicherheitsrisiken für Behörden und Unternehmen mit sich – vor allem dann, wenn „Bring Your Own Device (BYOD)“ oder „Private Use Of Company Equipment“ ins Spiel kommen. Insbesondere Smartphones sind für Angreifer interessant, da auf diesen eine Vielzahl von Daten bei häufig sehr unzureichendem Schutzniveau zu finden sind.

Zielsetzung

Das Seminar gibt einen Einblick in die typischen Bedrohungen für mobile Endgeräte (unsichere Apps, gezielte Angriffe, Rooten / Jailbreak, usw.), Authentisierung, Password-Sicherheit, Verschlüsselung, Mobile Device Management und die (Un-)Sicherheit der Übertragungswege. Dabei werden auch die verschiedenen Plattformen (iOS, Android, Blackberry, Windows) verglichen. Die Angriffs- und Schutzmöglichkeiten werden anschaulich in praktischer Form demonstriert.
Die Teilnehmer erkennen, ob und unter welchen Voraussetzungen BYOD in der eigenen Institution ratsam und praktikabel ist und wie mobile Endgeräte verwaltet werden können.

Zielgruppe

IT-Sicherheitsbeauftragte, CIOs, IT-Leiter, IT-Administratoren, IuK-Verantwortliche, IT-Dienstleister, Ermittler in Strafverfolgungsbehörden, Datenschutzbeauftragte

Preis

1.250,– Euro zzgl. MwSt.

Veranstaltungsort

InterCityHotel Berlin Hauptbahnhof
Katharina-Paulus-Straße 5, 10557 Berlin

Referent

Tobias Elsner, *IT Security Resulter der @-yet GmbH führt IT-Sicherheitsüberprüfungen bei Behörden und Unternehmen durch. Er verfügt über langjährige Erfahrung als IT-Berater in den Bereichen IT-Infrastruktur, IT-Security und Servervirtualisierung und besitzt die Qualifikation EC Council Certified Ethical Hacker.*

Mehr Informationen 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:** Sven Schuberth; **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