+++ Management Circle Intensiv-Seminar +++

In drei Tagen zum IT-Security-Experten

Intensiv-Seminar mit qualifiziertem Teilnahme-zertifikat

Der zertifizierte IT-Sicherheitsbeauftragte

So wehren Sie Betriebsausfall, Datenverlust und Spähangriffe ab

Die Eckpfeiler für eine sichere IT-Organisation:

- **IT-Sicherheitsgesetz und EU-Datenschutzverordnung:** Der neueste Stand der Gesetzgebung
- **IT-Sicherheitsziele und -strategie:** Formulierung zielgruppenorientierter Security Guidelines
- **Datensicherung, Kryptografie und Forensik:** Wesentliche Methoden und Instrumente
- **Physische IT-Sicherheit:** Organisatorische Maßnahmen bei Einbruch und Stromausfall
- **Umgang mit großen Datenmengen:** Big Data Policies und Qualitätskontrollen
- **Sicher in der Cloud und im Mobile Business:** Einbindung, Verfügbarkeit und Notfallversorgung

Aktuelle Rechtsprechung: Persönliche Haftungsrisiken des IT-Sicherheitsbeauftragten

Special

Exklusive Praxisberichte:

- ✔ **Integriertes IT-Sicherheitsmanagement bei der Open Grid Europe GmbH**
- ✔ **Prozessbasierte Datenschutzkontrolle bei der Merck KGaA**

Ihre Experten:

Andreas Kirk
Open Grid Europe GmbH

Jörn Maier
HiSolutions AG

Norbert Moeren
Merck KGaA

Dr. Tobias Sedlmeier
Dr. Sedlmeier & Dr. Dihsmaier Rechtsanwälte

Ihr Exklusiv-Termin:
16. bis 18. Juni 2014 in Köln

Hoher Lernerfolg durch begrenzte Teilnehmerzahl!

MANAGEMENTCIRCLE®
BILDUNG FÜR DIE BESTEN

Melden Sie sich jetzt an! Ihre Telefon-Hotline: + 49 (0) 61 96/47 22-700

Setzen Sie gesetzliche Anforderungen sicher um und minimieren Sie Haftungsrisiken

Ihr Seminarleiter:

Jörn Maier, Director Information Security Management, **HiSolutions AG,** Berlin

Der IT-Sicherheitsbeauftragte: Warum IT-Sicherheit im Unternehmen immer wichtiger wird

- Der Spagat zwischen neuen Technologien und erhöhten Sicherheitsanforderungen
- Wachsende Bedrohungen durch Wirtschaftsspionage und Datensicherheit
- Stetiger Wandel im technischen Umfeld
- Wechselnde Rahmenbedingungen: Wesentliche nationale und internationale IT-Standards
  - ISO 27001
  - Prüfungsstandard der Wirtschaftsprüfer IDW PS 330
  - ITIL
  - COBIT 5
- Ausblick: Anforderungen aus dem geplanten IT-Sicherheitsgesetz und der EU-Datenschutz-Grundverordnung

Die Aufgaben des IT-Sicherheitsbeauftragten im Überblick

- Festlegung der IT-Sicherheitsziele und -strategie
  - Ausrichtung an den Unternehmenszielen
- Erstellung einer IT-Sicherheitsleitlinie
- Formulierung von zielgruppenorientierten Sicherheitsrichtlinien
- Etablierung eines Identitätsmanagements
- Integration der wesentlichen Betroffenen in den Sicherheitsprozess
- Effiziente Planung des Ressourceneinsatzes für IT-Sicherheit
- Reporting an die Geschäftsführung, den Vorstand und weitere Organe
- Weiterentwicklung der IT-Sicherheitsmaßnahmen
- Methoden und Instrumente
  - Datensicherung und -archivierung
  - Kryptografische Verfahren (Verschlüsselungs- und Signaturverfahren)
  - Schutz vor Schadsoftware (z. B. Viren)

Erstellung von Sicherheitskonzepten: Der Grundpfeiler Ihres Sicherheitsmanagements

- Die Basis: Der IT-Grundschutz nach dem BSI
  - Struktur und Inhalte der Grundschutzkataloge
  - Daraus resultierende Anforderungen an ein IT-Sicherheitskonzept
- Grundlagen: Informationsverbund, Strukturanalyse und Schutzbedarfsfeststellung
- Modellierung nach dem IT-Grundschutzkatalog: Abbildung realer Systeme durch die Bausteine des IT-Grundschutzbaukastens
- Soll-Ist-Vergleich mittels Basis-Sicherheitscheck – So entsteht Ihr IT-Sicherheitskonzept
- Detaillierte Risikoanalyse – Wenn Grundschutz nicht ausreicht
- Technische Unterstützung bei der Erstellung von IT-Sicherheitskonzepten

Aufbau eines Informationssicherheits-managementsystems

- Formulierung von IT-Sicherheitsleitlinien
- Kritische Faktoren für ein erfolgreiches IT-Sicherheitsmanagement
- Rollenverteilung in einer Sicherheitsorganisation
- Aufgaben des IT-Sicherheitsmanagements
- Modelle für unterschiedliche Organisationsformen und Unternehmensgrößen
- Integration des IT-Sicherheitsmanagements in die Unternehmensstrukturen

AUCH ALS INHOUSE TRAINING

Zu diesen und allen anderen Themen bieten wir auch **firmeninterne Schulungen** an. Ich berate Sie gerne, rufen Sie mich an.

Stefanie Bruch
Tel.: 0 61 96/47 22-739
E-Mail: stefanie.bruch@managementcircle.de
www.managementcircle.de/inhouse

MANAGEMENT CIRCLE INHOUSE
BILDUNG FÜR DIE BESTEN

Get-Together

Ausklang des ersten Seminartages in informeller Runde. **Management Circle** lädt Sie zu einem kommunikativen Umtrunk ein. Entspannen Sie sich in angenehmer Atmosphäre und vertiefen Sie Ihre Gespräche mit Referenten und Teilnehmern.

So etablieren Sie eine rechtssichere und zuverlässige IT-Sicherheitsorganisation

Ihr Seminarleiter:

Jörn Maier

Physische IT-Sicherheitsmaßnahmen: Gewährleistung des Geschäftsbetriebs

- Anforderungen an physische, technische, organisatorische und personelle Maßnahmen
- Bedeutung der IT-Sicherheitsvorkehrungen für den Geschäftsbetrieb
- Analyse der Standorte der IT-Komponenten/IT-Betriebsräume: Zentrales Rechenzentrum, Netzwerk-Verteilerräume, dezentraler Serverraum etc.
- Wesentliche IT-Sicherheitsvorkehrungen für
  – Überspannung, Energie- und Klimaausfall
  – Wassereinbruch und Feuer
  – Einbruch und Sabotage
- Aufdeckung und Alarmierung der Störungen in den IT-Sicherheitsvorkehrungen

IT-Risikomanagement: Gefahr erkannt – Gefahr gebannt?

- Aufgaben des IT-Risikomanagements
  – Der Mensch als Risikofaktor
  – Beherrschbarkeit der Systeme
  – Vorkehrungen gegen externe Risiken
- Ansätze für ein Frühwarnsystem
  – Definition einer Risikostrategie
  – Methoden zur Risikoidentifikation, -analyse, -bewertung und -bewältigung
- IT-Notfallplanung: Was tun, wenn's brennt?
- IT-Compliance und IT-Revision

Seminarzeiten

Am ersten Seminartag: Empfang mit Kaffee und Tee, Ausgabe der Seminarunterlagen ab 8.45 Uhr

	Beginn des Seminars	Business Lunch	Ende des Seminars
1. Seminartag	9.30 Uhr	13.00 Uhr	ca. 18.00 Uhr
2. Seminartag	9.00 Uhr	12.30 Uhr	ca. 18.00 Uhr
3. Seminartag	9.00 Uhr	12.30 Uhr	ca. 17.00 Uhr

An allen Tagen ist jeweils am Vor- und Nachmittag eine Kaffee- und Teepause in Absprache mit den Referenten und Teilnehmern vorgesehen.

Ein Erfahrungsbericht: Integriertes IT-Sicherheitsmanagement bei der Open Grid Europe GmbH

Praxisbericht

- Vorgehen zum Aufbau und zur Implementierung der Informationssicherheit
- Eingliederung der Informationssicherheit in die Organisation
- Zusammenarbeit mit Fachbereichen, Datenschutzbeauftragten und Betriebsrat
- Ausgestaltung des IT-Risikomanagements und der IT-Risikoanalyse
- Muster für Richtlinien und Regelwerke zur Informationssicherheit
- Beispiele für die Ausgestaltung eines Internen Kontrollsystems
- Interne und externe Audits: Beispiele für Überwachungsmaßnahmen
- Prävention – Wie kann entsprechend vorgesorgt werden?

Andreas Kirk
Leiter Compliance/Internal Control,
Open Grid Europe GmbH,
Essen

Sicher in die Cloud: Datenschutz und technische Sicherheit beim Cloud Computing

- Organisationsformen und Modelle des Cloud Computing im Überblick
- Virtualisierung und Mandantentrennung
- Notfallvorsorge und Verfügbarkeit: Bei Ausfällen richtig reagieren
- Vorfälle schnell und rechtssicher aufklären: Forensik
- Insolvenz oder Fusion des Dienstleisters

Big Data: Sicherer Umgang mit großen Datenmengen

- Datenquellen: Customer Analytics und Social Media
- Big Data und Datenschutz
- Wer darf welche Daten und Informationen wie und zu welchen Zwecken aus- und verwerten?
- Was darf wie gespeichert werden?
- Regelmäßige Tests zur Weiterentwicklung
- Qualitätskontrollen korrekt durchführen
- Big Data Policies und Richtlinien

So setzen Sie aktuelle IT-Trends um und mindern Haftungsrisiken

Ihr Seminarleiter:

Jörn Maier

Persönliche Haftung des IT-Sicherheitsbeauftragten – So schützen Sie sich und Ihr Unternehmen

Special

- Gesetzliche Anforderungen: IT-Sicherheitsgesetz, BDSG-Novelle, SOX, Basel II/III
- Typische Haftungsrisiken im Unternehmen
  - Strafrechtliche Haftungsrisiken
  - Zivilrechtliche Haftungsrisiken
- Aufzeigen der möglichen Haftungsszenarien für IT-Sicherheitsbeauftragte
  - Unzureichendes Sicherheits- und Notfallkonzept
  - Urheberrechtsverstöße durch Unternehmen und Mitarbeiter
  - Verlust sensibler Daten
  - Aktuelle Bedrohungen durch Cloud Computing, Mobile Devices, Social Media etc.
- Mögliche rechtliche Konsequenzen bei Pflichtverletzungen
  - Schadenersatz-, Unterlassungs- und Löschungsansprüche
  - Aufsichtsbehördliche Maßnahmen
  - Verlust des Versicherungsschutzes
- Vorbeugungsmaßnahmen, z. B. organisatorische Pflichten, Haftungsklauseln in Verträgen

Dr. Tobias Sedlmeier
Fachanwalt für IT-Recht,
Dr. Sedlmeier & Dr. Dihsmaier Rechtsanwälte,
Heidelberg

Aktuelle Bedrohungsszenarien bei Nutzung sozialer Netzwerke

- Risiken bei der Nutzung von Facebook, XING und Twitter
  - Ausspähung durch individualisierte kurzlebige Trojaner
  - Abfluss von Daten per E-Mail und Instant Messaging
  - Facebook-Apps als Malware Gateway
  - Cross Site Scripting, Cross Site Request Forging, Session Hijacking
- Aufbau von Bot-Netzen und deren Vermarktung
- Vorgaben zum Umgang mit Social Media – was geht, was geht nicht
- Wesentliche Punkte von Social Media Guidelines

Mobile Devices und BYOD: Mobile Endgeräte sicher einbinden

- Mobile Devices im Überblick: Aktuelle Entwicklungen und Trends
- Typische Einsatzgebiete und -möglichkeiten im Unternehmen
- Neue Möglichkeiten vs. neue Herausforderungen für Unternehmen
  - Zentrales „OTA" (Over the Air) Mobile Device Management
  - Trennung privater und betrieblicher Nutzung durch Management Agents
  - Verschlüsselung der sensiblen Unternehmensdaten
  - Sichere Verteilung und Nutzung von Apps im Unternehmen
- Mobile Devices und Arbeitnehmerüberwachung
  - Personaldaten- und Auftragsdatenverarbeitung: Kontrollmöglichkeiten des Arbeitgebers
  - Betriebliche Mitbestimmung bei Verhaltens- und Leistungskontrolle

Praxisbericht

Integriert statt On-Top – Prozessbasierte Datenschutzkontrolle

- Motivation: Die Datenschutzanforderungen effizient umsetzen
- Übersicht über die erforderlichen Datenschutzprozesse
- Darstellung der Prozesse und Erweiterungen für internationale Datentransfers
- Technische Implementierung und Ausrollen der Prozesse
- Nutzung der Datenschutzprozesse für andere IT-Compliance Kontrollen, einschließlich des Informationsschutzes
- Zusatznutzen: Datenschutz wird messbar

Norbert Moeren
Group Data Privacy Officer,
Merck KGaA,
Darmstadt

Zum Seminarinhalt

Der IT-Sicherheitsbeauftragte – wichtiger denn je

Die IT ist mittlerweile aus dem Tagesgeschäft nicht mehr wegzudenken – nahezu jeder Arbeitsschritt ist mit einer Software hinterlegt oder wird technisch gesteuert, von der externen oder internen Kommunikation ganz zu schweigen. Dies bedeutet gleichzeitig aber auch ein erhöhtes Risiko für Ihr Unternehmen: Datenabfluss, Stromausfall oder ein Hacker-Angriff können im schlimmsten Fall zur Betriebsstörung und zu schweren Reputationsschäden führen.

Jetzt sind Sie als IT-Sicherheitsbeauftragter gefragt: Sie fungieren als Berater in allen Projekten mit IT-Bezug und unterstützen die Geschäftsleitung bei allen strategischen Entscheidungen, die die Informationssicherheit betreffen. Aber auch operativ wird vieles von Ihnen gefordert: Mit der Einführung und Weiterentwicklung eines IT-Sicherheitsmanagementsystems und der entsprechenden Sicherheitsmaßnahmen tragen Sie maßgeblich zur Wettbewerbsfähigkeit und zum Fortbestand des Unternehmens bei!

Die Eckpfeiler für eine sichere IT-Organistion

- Sie hören, welche **Anforderungen aus** den **Standards und Gesetzen** rund um **IT-Sicherheitsgesetz, BDSG** und **EU-Datenschutzverordnung** entstehen.
- Sie informieren sich über **straf- und zivilrechtliche Haftungsrisiken,** die Ihnen **bei Datenverlust** oder mangelnden Sicherheitsvorkehrungen drohen.
- Sie erfahren, wie Sie eine schlüssige **IT-Sicherheitsstrategie festlegen.**
- Sie erhalten einen Leitfaden für die **Formulierung eines IT-Sicherheitskonzepts** und die **Festsetzung von Sicherheitsleitlinien.**
- Sie hören, welche **physischen Sicherheitsvorkehrungen** Sie **gegen Stromausfälle, Wasserschäden und Einbrüche** treffen müssen.
- Sie erfahren, wie Ihnen ein effizientes **IT-Risikomanagement** dabei hilft, **Bedrohungen** im Vorfeld zu **identifizieren und frühzeitig vorzubeugen.**
- Schließlich informieren Sie sich über **erhöhte Gefahrpotenziale durch** neue Trends rund um **Big Data, Cloud Computing** und **Bring Your Own Device** und wie Sie diesen begegnen.

Sie haben noch Fragen? Gerne!

Rufen Sie mich an oder schreiben Sie mir eine E-Mail.

Martha Peplowski
Projektmanagerin
Tel.: 0 61 96/47 22-698
E-Mail: martha.peplowski@managementcircle.de

Ihr Expertenteam

Andreas Kirk, Diplom-Wirtschaftsinformatiker, CISA, CISM, ist verantwortlich für das Internal Control und Datenschutzbeauftragter bei der **Open Grid Europe GmbH.** Zuvor verantwortete er die Informationssicherheit sowie die IT-Revision bei der E.ON Ruhrgas AG. Andreas Kirk verfügt über vieljährige Erfahrungen insbesondere bei der Einführung komplexer Standardsoftware, der Prozessoptimierung und bei der Beurteilung bzw. beim Aufbau von Kontroll- und Überwachungssystemen. Seit 1993 ist er auch als externer Referent und in verschiedenen Arbeitskreisen (DSAG, SAP) tätig.

Jörn Maier ist Director Information Security Management bei der **HiSolutions AG** in Berlin und arbeitet seit 2001 im Umfeld der Informationssicherheit. In dieser Zeit war er als Sicherheitsberater für die Unisys Deutschland GmbH und die HiSolutions AG bzw. als Leiter IT-Sicherheit und Behördenauskünfte für die Kabel Baden-Württemberg GmbH & Co KG tätig. Er ist zertifizierter Datenschützer, CISM, CISSP und seit 2003 vom BSI lizensierter Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz. Seine fachlichen Schwerpunkte liegen u.a. im Aufbau und der Auditierung von Informationssicherheitsmanagementsystemen, im Aufbau von Risikomanagementsystemen sowie im Datenschutz. Er studierte in Ulm und Aberdeen Informatik und diplomierte mit dem Thema „Schutzmechanismen für Webserver gegen Denial of Service Angriffe". Er veröffentlicht regelmäßig in Fachzeitschriften zu Sicherheitsthemen und hält Vorträge im Bereich Informationssicherheit.

Norbert Moeren leitet das Group Data Protection Office der **Merck KGaA.** In dieser Funktion ist er als Datenschutzbeauftragter der Merck KGaA und deren deutschen Tochtergesellschaften bestellt. Seit 2001 ist er bei Merck in verschiedenen Funktionen für die Themenfelder der IT Governance, IT Audit, IT Risikomanagement, IT Sicherheit und IT Compliance verantwortlich. Hierzu gehörten u. a. auch die erfolgreiche Zertifizierung des Kontrollsystems nach den Standards der ISO 9001, ISO 20000 und ISO 27001. Norbert Moeren studierte an der RWTH Aachen Maschinenbau in der Fachrichtung Produktionstechnik. Darauf aufbauende Erfahrungen im Öffentlichen Dienst und in der Industrie sowie Qualifizierungen als Certified Risk Manager (CRISC), Certified Information Systems Security Professional (CISSP), ISO 27001 Lead Auditor und zertifizierter Datenschutzbeauftragter bilden die fachliche Grundlage für die heutige Tätigkeit.

Dr. Tobias Sedlmeier ist Rechtsanwalt und Fachanwalt für IT-Recht und praktiziert in der **Kanzlei Dr. Sedlmeier & Dr. Dihsmaier** in Heidelberg. Er ist spezialisiert auf die rechtliche Beratung im Umfeld von IT, Technologie, Medien und Kreativwirtschaft und betreut dabei sowohl die Anbieter- als auch die Kundenseite. Seine Beratungsfelder sind u. a. IT-Recht, IT-Compliance, Datenschutz, Urheberrecht, Markenrecht, Wettbewerbs- und Kartellrecht, Arbeitsrecht und Wirtschaftsstrafrecht. Dr. Tobias Sedlmeier ist zudem Lehrbeauftragter für Datenschutzrecht an der Universität Würzburg und Ausbilder von angehenden Fachanwälten für IT-Recht. Vor der Gründung seiner eigenen Kanzlei war er u. a. als Rechtsanwalt bei Hengeler Mueller und Freshfields Bruckhaus Deringer sowie als Staatsanwalt tätig.

Wen Sie auf diesem Seminar treffen

Diese Veranstaltung richtet sich an **IT-Sicherheitsbeauftragte, IT-Security Officer, IT-Security Manager, CISOs, CIOs, Leiter IT, Leiter IT-Strategie, Rechenzentrumsleiter, IT-Projektleiter** und **IT-Architekten.** Angesprochen sind auch **Fach- und Führungskräfte** aus den Bereichen **IT, IT-/EDV-Sicherheit, IT-Controlling, IT-Risikomanagement, IT-Revision, betriebliche Sicherheit** und **IT-Organisation.** Herzlich eingeladen sind zudem **Compliance Officer, betriebliche Datenschutzbeauftragte** sowie **interessierte Beratungsunternehmen.**

Termin und Veranstaltungsort

16. bis 18. Juni 2014 in Köln
Hotel Mondial am Dom Cologne
Kurt-Hackenberg-Platz 1
50667 Köln
Tel.: 0221/2063-570
Fax: 0221/2063-527
E-Mail: h1306@accor.com

Zimmerreservierung
Für unsere Seminarteilnehmer steht im Tagungshotel ein begrenztes Zimmerkontingent zum Vorzugspreis zur Verfügung. Nehmen Sie die **Reservierung bitte rechtzeitig selbst direkt im Hotel** unter Berufung auf Management Circle vor.

Mit der Deutschen Bahn ab € 99,– zur Veranstaltung. Infos unter:
www.managementcircle.de/bahn DB BAHN

Über Management Circle

Als anerkannter Bildungspartner und Marktführer im deutschsprachigen Raum vermittelt Management Circle *WissensWerte* an Fach- und Führungskräfte. Mit seinen 200 Mitarbeitern und jährlich etwa 3000 Veranstaltungen sorgt das Unternehmen für berufliche Weiterbildung auf höchstem Niveau. Weitere Infos zur *Bildung für die Besten* erhalten Sie unter **www.managementcircle.de**

Anmeldebedingungen

Nach Eingang Ihrer Anmeldung erhalten Sie eine Anmeldebestätigung und eine Rechnung. Die Teilnahmegebühr für das dreitägige Seminar beträgt inkl. Business Lunch, Erfrischungsgetränken, Get-Together und der Dokumentation € 2.595,–. Sollten mehr als zwei Vertreter desselben Unternehmens an der Veranstaltung teilnehmen, bieten wir **ab dem dritten Teilnehmer 10% Preisnachlass.** Bis zu zwei Wochen vor Veranstaltungstermin können Sie kostenlos stornieren. Danach oder bei Nichterscheinen des Teilnehmers berechnen wir die gesamte Teilnahmegebühr. Die Stornierung bedarf der Schriftform. Selbstverständlich ist eine Vertretung des angemeldeten Teilnehmers möglich. Alle genannten Preise verstehen sich zzgl. der gesetzlichen MwSt.

Der zertifizierte IT-Sicherheitsbeauftragte

WS

Ich/Wir nehme(n) teil am:

❑ **16. bis 18. Juni 2014 in Köln** 06-77875

– 10 %

1 Name/Vorname

Position/Abteilung

2 Name/Vorname

Position/Abteilung

3 Name/Vorname

Position/Abteilung

Firma

Straße/Postfach

PLZ/Ort

Telefon/Fax

@ E-Mail

Datum Unterschrift

Ansprechpartner/in im Sekretariat:

Anmeldebestätigung bitte an: Abteilung

Rechnung bitte an: Abteilung

Mitarbeiter: ❍ BIS 100 ❍ 100–200 ❍ 200–500 ❍ 500–1000 ❍ ÜBER 1000

Datenschutzhinweis
Die Management Circle AG und ihre Dienstleister (z.B. Lettershops) verwenden die bei Ihrer Anmeldung erhobenen Angaben für die Durchführung unserer Leistungen und um Ihnen Angebote zur Weiterbildung auch von unseren Partnerunternehmen aus der Management Circle Gruppe per Post zukommen zu lassen. Unsere Kunden informieren wir außerdem telefonisch und per E-Mail über unsere interessanten Weiterbildungsangebote, die den vorher von Ihnen genutzten ähnlich sind. Sie können der Verwendung Ihrer Daten für Werbezwecke selbstverständlich jederzeit gegenüber Management Circle AG, Postfach 56 29, 65731 Eschborn, unter datenschutz@managementcircle.de oder telefonisch unter 06196/4722-500 widersprechen oder eine erteilte Einwilligung widerrufen.

Anmeldung/Kundenservice

Telefon:	**+49 (0) 61 96/47 22-700**
Fax:	**+49 (0) 61 96/47 22-999**
E-Mail:	**anmeldung@managementcircle.de**
Internet:	**www.managementcircle.de/06-77875**
Postanschrift:	**Management Circle AG Postfach 56 29, 65731 Eschborn/Ts.**
Telefonzentrale:	**+49 (0) 61 96/47 22-0**

KP/SM+BZU/K