



Seminarort

CCG-Zentrum, Technologiepark Argelsrieder Feld 11,
D-82234 Weßling-Oberpfaffenhofen

Eine Lageskizze sowie Hinweise für die Anreise und Übernachtung schicken wir Ihnen mit der Bestätigung der Anmeldung zu.

Gebühr

EUR 1.369,-

Die CCG ist als gemeinnützig anerkannt und von der USt befreit.

Mitglieder der CCG erhalten 10% Rabatt, Studenten bei Vorlage des Studentenausweises 75%. Bei Anmeldung mehrerer Mitarbeiter einer Firma / Dienststelle zum gleichen Seminar erhält jeder Teilnehmer 10%.

Die Rabatte sind nicht miteinander kombinierbar.

Bitte zahlen Sie bargeldlos nach Erhalt der Rechnung.

Anmeldungen

Bitte möglichst bis 14 Tage vor Seminarbeginn an:

Carl-Cranz-Gesellschaft e.V., Postfach 11 12, D-82230 Weßling
Tel. +49 (0) 8153 / 88 11 98 -12, Fax -19, E-Mail: anmelden@ccg-ev.de
Internet: www.ccg-ev.de

Die Anmeldungen werden schriftlich bestätigt.

Weitere Informationen zum Inhalt

Dr. Gerhard Weck
Infodas GmbH
Rhonestr. 2, D-50765 Köln
Tel. +49 (0) 221 / 70912-52, Fax -55
E-Mail: G.Weck@infodas.de

Stornierung

Bei Stornierung mündlich oder schriftlich bestätigter Anmeldungen wird eine Bearbeitungsgebühr von EUR 25,- berechnet. Bei Stornierungen, die später als 7 Tage vor Seminarbeginn eingehen, werden 25% der Gebühr, bei Nichterscheinen die volle Gebühr in Rechnung gestellt. Die Vertretung eines angemeldeten Teilnehmers ist möglich.

Ausfall von Seminaren oder Dozenten

Die CCG behält sich vor, bei zu geringer Teilnehmerzahl oder aus anderen triftigen Gründen ein Seminar bis 10 Tage vor Beginn abzusagen. Sie behält sich weiter vor, entgegen der Ankündigung im Programm auch kurzfristig einen Dozenten und evtl. auch dessen Thema zu ersetzen. Ein Schadensersatzanspruch bleibt ausgeschlossen.

Teilnehmer

Verantwortliche für Datenverarbeitung und Kommunikation ebenso wie Entwickler und Anwender von Datenverarbeitungs- und Kommunikationssystemen aller Art, Systembetreuer, Datenschutz- und IT-Sicherheitsbeauftragte aus Industrie und Behörden, Sicherheitsberater, Nutzer und Betreiber von IT-Systemen aller Art.

Seminarinhalte

Die Komplexität und Allgegenwärtigkeit heutiger Informationsverarbeitung schafft neue Probleme, Schwachstellen, Gefahren und Risiken. Weltweite Netze wie das Internet haben Datenverarbeitung zu einem flächendeckenden Werkzeug gemacht, dessen neue Möglichkeiten überall benutzt, dessen Risiken aber noch zu wenig bekannt sind, noch weniger beherrscht werden.

Informationsverarbeitung beschwört darüber hinaus neue Gefahren für die Betroffenen herauf. Diese Bedrohungen so klein wie möglich zu halten, muss Ziel schon der Konzeption und erst recht der Implementierung und des Betriebs aller IT-Systeme sein.

Will man den Gefahren durch und für die Informationsverarbeitung wirksam begegnen, so muss man einerseits die Struktur und die Hintergründe dieser Gefahren verstehen und andererseits benötigt man eine umfassend anwendbare Methodik, die die notwendigen Maßnahmen zum Schutz materieller und immaterieller Werte an die Hand gibt.

Die Teilnehmer erfahren, welche Risiken heute mit dem Betrieb von IT-Systemen und Netzen verbunden sind. Sie erhalten eine Übersicht über die technischen und organisatorischen Hilfsmittel sowie die anzuwendenden Standards – schon vorhandene und noch zu entwickelnde – mit denen Informationsverarbeitung künftig so weit irgend möglich ordnungsmäßig sicher und beherrschbar gestaltet werden kann.

Vortragende

F. Reiländer	Dipl.-Inform.	Infodas GmbH, Köln
G. Weck	Dr.	

Unterlagen

Jeder Teilnehmer erhält die Vortragsunterlagen.
Die Kosten dafür sind in der Gebühr enthalten.

Seminar IN 6.12

Informationssicherheitsmanagement

18. – 20. Oktober 2011
Oberpfaffenhofen bei München

Wissenschaftliche Leitung

Dr. Gerhard Weck
Infodas GmbH, Köln

Seminarprogramm

Dienstag, 18.10.2011
10.15 – 16.30 Uhr

- | | |
|--------------------------|---|
| 10.15 – 10.30 | Begrüßung, Organisation, Einführung |
| 10.30 – 12.00
G. Weck | Einleitung: Besonderheiten der Sicherheit in der Informationstechnik (IT-Sicherheit)
Fünf Thesen zur IT-Sicherheit • Grundlegende Veränderungen in der Informationstechnik durch Computer: Darstellung der Zeichen – Digitalisierung – Interpretation und Information – das Kontextproblem • Informationsverarbeitende Systeme (Systeme der Informationstechnik) |
| 13.00 – 14.30
G. Weck | Modell der IT-Sicherheit
Security and Safety: unklare und widersprüchliche Begriffe – die Beziehung Mensch↔Maschine als Besonderheit • ein verbessertes semantisches Modell der IT-Sicherheit – Verlässlichkeit und Beherrschbarkeit als Grundlagen • Duale Sicherheit – semantische Dimensionen (Ziele) der IT-Sicherheit – Grundfunktionen – Mechanismen • IT-Sicherheit und Grundrechte der Verfassung |
| 15.00 – 15.45
G. Weck | Bedrohungen und Schwachstellen
Statistiken zur IT-Sicherheit • Fallbeispiele für Gefährdungen und Risiken • Arten von IT-Sicherheitsvorfällen • Studien zur IT-Sicherheit • staatliche Ermittlungen • kriminelle Ziele • Zusammenarbeit zwischen Hackern und organisierter Kriminalität |
| 15.45 – 16.30
G. Weck | Schadensszenarien
Höhere Gewalt (physische Schäden, Ausfall der Infrastruktur, Streik, Schäden im Umfeld) • Organisatorische Mängel (fehlende oder unzureichende Regelungen, ungeeignete Rechtevergabe, unkontrollierter Einsatz von IT-Systemen) • Menschliche Fehlhandlungen (mangelnde Sorgfalt, unsachgemäße Behandlung, Unwissenheit) |
| ab ca. 17.30 | Social Event
Führung durch die Münchener Altstadt (optional) |

Mittwoch, 19.10.2011
08.30 – 16.30 Uhr

- | | |
|-------------------------------|--|
| 08.30 – 10.00
G. Weck | Technische Schäden und bewusste Angriffe
Fehler in Hard- und Software • Qualität und Komplexität der Systeme • Pufferüberlauf und seine Folgen • Diebstahl, Spionage und Sabotage • Typische Angriffsabläufe in Rechnernetzen (Footprinting, Scanning, Eindringen, Übernahme der Kontrolle, Verwischen der Spuren) |
| 10.30 – 12.00
G. Weck | Kriminelle Angriffe auf die IT-Sicherheit
Wirtschaftsspionage • Neugier, spielerische Herausforderung • Verbreitung von Viren und Würmern • Virenbaukästen und Zero-Day-Exploits • Denial of Service • Bot-Netze • Verteilung von Spam • Targeted Attacks / Wegwerf-Trojaner • Phishing und Farming |
| 13.00 – 14.30
F. Reiländer | Informationssicherheitsmanagement
Aufbau und Aufgaben des Sicherheitsmanagements • Die Rolle des IT-Sicherheitsbeauftragten • IT-Sicherheitsprozess, -ziele und -strategien • Organisation und Verantwortlichkeiten • Standards zur IT-Sicherheit (ISO/IEC 2700x, BSI-Standards/IT-Grundschutz, ZDv 54/100, etc.) |
| 15.00 – 16.30
F. Reiländer | Sicherheitsdokumentation
Die Bedeutung der Security Policy • Ziele und Inhalte eines IT-Sicherheitskonzeptes • Verpflichtung von IT-Benutzern, System- und Aufgabenverantwortlichen zur Umsetzung des IT-Sicherheitskonzeptes • System- und anwendungsspezifische IT-Sicherheitsrichtlinien |

Donnerstag, 20.10.2011
08.30 – 16.30 Uhr

- | | |
|-------------------------------|--|
| 08.30 – 10.00
F. Reiländer | Methodik und Elemente zur Erstellung von Sicherheitskonzepten
IT-Strukturanalyse • Schutzbedarfsanalyse • Bedrohungsanalyse und Bewertung der Risiken • Maßnahmenplanung • Maßnahmenkatalog zur Beseitigung inakzeptabler Risiken • Wirtschaftlichkeitsanalyse • Der Umgang mit dem Restrisiko |
| 10.30 – 12.00
F. Reiländer | Risikoanalyse
Klassische Risikoanalyse und ihre Grenzen • Problematik der Festlegung von Schadenshöhe und –wahrscheinlichkeit • Wirkungsnetzanalyse • Der BSI-Standard 100-3 • Technische Schwachstellenanalyse • Kombinierte Verfahren |
| 13.00 – 14.30
F. Reiländer | Anwendung von Standards und Werkzeugen
Aufbau von IT-Sicherheitskonzepten nach IT-Grundschutz • Der BSI-Standard 100-4 v • ISO 27001 • Militärische IT-Sicherheitskonzepte gemäß ZDv 54/100 • Datenbankgestützte Werkzeuge (GSTOOL, SAVe®) |
| 15.00 – 16.30
F. Reiländer | Schulung und Sensibilisierung
Adressatenkreise • Planung von Schulungsinhalten • Sicherheitsregeln für Mitarbeiter • Aufzeigen typischer Fehler von Anwendungen • Verhalten bei Sicherheitsvorfällen • Notfallvorsorge/Notfallplanung • Spezielle Sensibilisierungsmaßnahmen |

Voraussetzungen

DV-Kenntnisse, Erfahrung und Kenntnisse im Umgang mit PCs oder Arbeitsplatzsystemen erwünscht

Weitere Seminare zum Themenbereich

- „Systems Engineering in IT-Projekten“, 14.–18.11.2011 (Code IN 3.01)
- „Sicherheit in Netzen – Probleme und Lösungen“, 22.–24.11.2011 (Code IN 6.13)