

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 Kommunikations-
systemen aller Art, Systembetreuer, Datenschutz- und IT-Sicherheitsbe-
auftragte aus Industrie und Behörden, Sicherheitsberater, Nutzer und
Betreiber von IT-Systemen aller Art.

Seminarinhalte

Netze schaffen neue Möglichkeiten der Informationsverarbeitung, schaffen
aber auch 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.

Kryptographie spielt für die Sicherheit von Netzen eine entscheidende
Rolle, nicht nur für die traditionelle Geheimhaltung, sondern - zunehmend
wichtiger - auch für die Authentisierung von Personen, Geräten und Pro-
grammen ebenso wie für die Gewährleistung der Unversehrtheit (Integri-
tät) von Daten und Programmen. Kryptographie ist die informations-
technische Voraussetzung für die Rechtsverbindlichkeit eines „Electronic
Commerce“.

Informationsverarbeitung in Netzen beschwört darüber hinaus neue Ge-
fahren für die Betroffenen herauf. Diese Bedrohungen so klein wie möglich
zu halten, muss Ziel schon der Konzeption und erst recht der Implementie-
rung und des Betriebs vernetzter Systeme sein. Auch hier ist die Krypto-
graphie Kern einer mehrseitigen Sicherheit.

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

Voraussetzungen

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

Unterlagen

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

Seminar IN 6.13

Sicherheit in Netzen – Probleme und Lösungen

22. – 24. November 2011
Oberpfaffenhofen bei München

Wissenschaftliche Leitung

Dr. Gerhard Weck
Infodas GmbH, Köln

Seminarprogramm

Dienstag, 22.11.2011
09.00 – 17.30 Uhr

09.00 – 09.15	Begrüßung, Organisation, Einführung
09.15 – 10.00 G. Weck	Modell der IT-Sicherheit Was ist „sichere Informationsverarbeitung“? • Grundkonzept für die Sicherheit in IT-Systemen • Duale Sicherheit • Komponenten der Verlässlichkeit / der Beherrschbarkeit
10.30 – 12.00 G. Weck	Angriffe und Schäden Sicherheitslücken und ihre Folgen • Sicherheitsvorfälle • Win32-Viren und -Würmer / Verwundbarkeiten • Struktur der Hacker Community • Workflow und Geldflüsse • Schwachstellen • Softwarezuverlässigkeit • Pufferüberlaufprobleme
13.00 – 14.30 G. Weck	Netzwerk-Protokolle Nutzen und Zweck von Protokollen • Bestandteile von Protokollen • Das OSI 7-Schichten-Modell der ISO • Der Protokollstack von TCP/IP • Protokolle und Dienste • Struktur des Internets
15.00 – 15.45 G. Weck	Physische Netzbedrohungen Gefährdung der Leitungen • Einfluss der Netztopologie • Zuverlässigkeit der Übertragungsstrecken
15.45 – 16.30 G. Weck	Angriffsmöglichkeiten Angriffsbäume • Vorbereitung und Planung von Angriffen • Footprinting – die Wahl des Angriffsziels • Scanning – erste Informationen • Auswertung und Angriffsplanung
16.45 – 17.30 G. Weck	Angriffstechniken Abhören • Verfälschung • Maskerade • Unterlaufen von Zugriffsberechtigungen • Datenüberflutung • Denial-of-Service Angriffe • Bot-Netze • Mail-Bomben • Spam • Phishing • Angriffe auf Web-Server

Mittwoch, 23.11.2011
08.30 – 16.30 Uhr

08.30 – 10.00 B. Weiss	Die Kryptographie: Basis von Sicherheitstechniken und -systemen Private-Key-Verfahren • Public-Key-Verfahren • hybride Verschlüsselungstechnik • Hashfunktionen • Zertifikate • Chipkarten • Sicherheitsmodule • TPM • Identitätsmanagement • Standards der Kryptographie
10.30 – 12.00 B. Weiss	Schutz der elektronischen Dokumente Elektronische Unterzeichnung (Signatur) von Dokumenten • Verschlüsselung eines Dokuments • Analyse eines vertrauenswürdigen Dokuments • Entschlüsselung eines Dokuments • Verifikation von Signaturen • Zeitstempel • Rechtliche Anforderungen an die elektronische Unterschrift
13.00 – 14.30 B. Weiss	Sicherheitsarchitekturen Aufbau von Identitätsmanagementsystemen (Public-Key-Infrastrukturen) • Bridge-CA • Verifikationsmodelle • Signatur von Massendaten • Langzeitarchivierung von signierten Dokumenten • Anwendungen der digitalen Signatur in der Praxis • Web-Services Security • OCSP Responder
15.00 – 16.30 B. Weiss	Security Gateway Konzepte Virtuelle Poststelle: Die virtuelle Poststelle als pragmatische Lösung für vertrauenswürdige E-Mails • De-Mail: Plattform zum sicheren Austausch rechtsgültiger elektronischer Dokumente • Virtual Workstation
ab ca. 17.30	Social Event Führung durch die Münchener Altstadt (optional)

Weitere Seminare zum Themenbereich

- „Informationssicherheitsmanagement“, 18.–20.10.2011 (Code IN 6.12)
- Deutsche und europäische Citizen Cards – Technologie, Sicherheit, Anwendungen“, 11.–13.10.2011 (Code IN 6.18)
- „Systems Engineering in IT-Projekten“, 14.–18.11.2011 (Code IN 3.01)

Donnerstag, 24.11.2011
08.30 – 16.30 Uhr

08.30 – 10.00 S. Köpsell	Sicherheit in verteilten Systemen und durch verteilte Systeme Mehrseitige Sicherheit: Better safe than sorry Systematik von Schutzzielen • Angreifermodelle • Zugangs- und Zugriffskontrolle • Sicherheitsanker • Prinzip der mehrseitigen Sicherheit • Verteilung zum Schutz der Verfügbarkeit
10.30 – 12.00 S. Köpsell	Mehrseitig sichere Verfahren multilaterale Verfahren für Vertraulichkeit der Kommunikationsumstände und Verfügbarkeit • Möglichkeiten, Aufwand und Grenzen dieser Verfahren • Datenschutzfreundliches Identitätsmanagement
13.00 – 14.30 S. Köpsell	Multimedia-Sicherheit Schutzziele • Mechanismen der Multimedia-Sicherheit • Anforderungen an die Verfahren • digitale Bilder • Ziele und Prinzipien der Digitalen Bildforensik
15.00 – 16.30 E. Franz	Steganographie Aufbau eines steganographischen Systems • Sicherheit steganographischer Systeme • steganographische Verfahren für digitale Bilder • Steganalyse – Angriffe auf steganographische Verfahren

Vortragende

Elke Franz S. Köpsell	Dr. Dr.	TU Dresden
G. Weck	Dr.	Infodas GmbH, Köln
B. Weiss	Dipl.-Ing.	Secunet Security Networks AG, Siegen