

Anmeldung:

Am besten gleich faxen/mailen

Termine / Veranstaltungsort:

Donnerstag, 4. Dezember 2008, ARS Seminarzentrum,
Schallautzerstraße 2-4 (Ecke Uraniastraße), 1010 Wien

Mittwoch, 14. Oktober 2009, ARS Seminarzentrum,
Schallautzerstraße 2-4 (Ecke Uraniastraße), 1010 Wien

jeweils von 9.00 bis 17.00 Uhr

Gebühr:

Je € 450,- inkl. Seminarunterlagen, Begrüßungskaffee,
Erfrischungsgetränken, Mittagessen und exkl. 20 % USt.
Anmeldungen werden in der Reihenfolge des Eintreffens und
nach Maßgabe freier Plätze berücksichtigt.
Wir ersuchen Sie, nach Erhalt der Rechnung die Teilnahme-
gebühr bis zum Seminartermin zu überweisen.

Ermäßigungen:

| | |
|------------------------------------|--|
| 10 % (per TN) | ab 3 TN eines Unternehmens |
| 30 % (per TN) | ab 10 TN eines Unternehmens |
| 20 % | für RAA, WT-BerufsanwärtlerInnen, NO-KandidatInnen |
| Ermäßigungen sind nicht addierbar! | |

Storno:

Bitte haben Sie Verständnis, dass bei Stornierungen ab 14 Tage vor Seminarbeginn 50 % des Seminarbetrages, bei Stornierungen oder Nichterscheinen am Veranstaltungstag die volle Gebühr in Rechnung gestellt wird. Bei jeder Stornierung beträgt die Bearbeitungsgebühr € 40,- exkl. USt. Bei einer Umbuchung auf einen Folgetermin bleibt die ursprüngliche Rechnung inkl. der Fälligkeit gültig. Zusätzlich wird eine Gebühr von € 20,- exkl. USt. (ausgenommen am Seminartag: 15 % Aufschlag) in Rechnung gestellt. Stornierungen können ausschließlich schriftlich entgegengenommen werden! Selbstverständlich können Sie jedoch gerne eine **Ersatzperson** nominieren. Die Veranstalter behalten sich vor, das Seminar aus wichtigen Gründen zu verschieben sowie Programmänderungen vorzunehmen.

Anmeldung / Information:

Fax: (01) 713 80 24 DW 14
Tel.: (01) 713 80 24 DW 17
E-Mail: office@ars.at, http://www.ars.at

Projektorganisation: Katharina Ludwin
Inhalt / Konzeption: Ute Walch

Adresskorrektur: (01) 713 80 24 DW 40

DVR-Nr.: 0927571

CYBERCRIME

Organisierte Kriminalität im Netz

Technische Möglichkeiten & rechtliche Verantwortlichkeit

RA Dr. Clemens Thiele,
LL.M. Tax (GGU)
EUROLAWYER®



DI Dr. Christian Reiser
ERSTE Group Bank AG



Do., 4. Dezember 2008, Wien
Mi., 14. Oktober 2009, Wien
jeweils von 9.00 bis 17.00 Uhr

Mag. Leopold Löschl
Leiter Computer- und
Netzwerkriminalität,
Bundeskriminalamt



WWW.ARS.AT

Fax: (01) 713 80 24 DW 14
E-Mail: office@ars.at
ARS, Schallautzerstraße 2-4, 1010 Wien

Ja, ich melde mich an für das Seminar „Cybercrime“ mit RA Dr. Thiele, LL.M., DI Dr. Reiser und Mag. Löschl Termin: _____

Ja, ich bestelle per Nachnahme die Seminarunterlagen zu 40 % des Seminarbeitrages, da ich an der Teilnahme verhindert bin.

Seminarunterlagen können nicht retourniert werden!
... und bin einverstanden, dass meine Daten elektronisch gespeichert werden und ich per Fax oder E-Mail über weitere Veranstaltungen informiert werde.
Als Gerichtsstand wird Wien vereinbart.

1. TeilnehmerIn Vor- und Nachname / Titel

Aufgabenbereich / Abteilung

KonzipientIn

Tel.

BerufsanwärtlerIn

Fax

E-Mail

2. TeilnehmerIn Vor- und Nachname / Titel

Tel.

Fax

E-Mail

Firma

Branche

Beschäftigte: bis 100 100-200 über 200, bitte Zahl: _____

Straße, Postfach

PLZ, Ort

Datum

Unterschrift

Wer muss informiert sein:

- Jeder (kann betroffen sein), ob Bankkunde, Online-Besteller oder www-Surfer
- EDV-Beauftragte
- LeiterInnen von Rechtsabteilungen
- Personalverantwortliche aller Branchen
- RechtsanwältInnen/StrafverteidigerInnen

Ihr Nutzen:

Das Web 2.0 bestimmt zum Großteil unseren Alltag. Es gibt aber auch die dunkle Seite des Internets, die mittlerweile Massenkriminalität wie Spamming, Hacking, Spoofing oder Phishing hervorgebracht hat.

- Wie schütze ich mich vor Cyberkriminalität?
- Was ist zu tun, wenn etwas passiert ist?
- Stimmt es, dass der Cyberspace ein „rechtsfreier Raum“ ist?

Cybercrimes sind weiter auf dem Vormarsch. Die Zahl der Cyber-Verbrechen in der EU ist im Laufe des letzten Jahres dramatisch angestiegen und wächst weiter – auch in Österreich. Auch die Konsumentenschutzorganisationen (VKI und AK) verzeichneten im ersten Halbjahr 2007 mit mehr als 10.000 Betrugsfällen eine deutliche Zunahme von Delikten. Vor allem Delikte wie Kreditkartenmissbrauch und Viren-/Website-Attacks führen die Beschwerdeliste an. Ein Großteil der Manipulationen richtete sich den Angaben zufolge gegen Online-Auktionsseiten, auf denen besonders gern betrogen wird. Dabei nimmt auch die Zahl von innerbetrieblicher Sabotage und der Missbrauch von IT-Einrichtungen in Unternehmen immer mehr zu. Cybercrime ist längst keine Randerscheinung mehr, die nur große Rechenzentren oder die Bank-IT betrifft. Zunehmende Professionalität und ein hohes Maß an Organisationsstruktur erhöht das Gefahrenpotenzial, erschwert effiziente Bekämpfungsstrategien und fordert umso mehr eine umfassende Bewusstseinsbildung, denn – es kann jeden treffen.

Seminarinhalte:

■ Der Cybercrime-Report 2006

- Phänomen Cybercrime – Vom Einzeltäter zur organisierten Kriminalität
- Computer- und Netzwerkkriminalität in Österreich
- Modi operandi, inkl. Beispiele
- Prävention und Arbeitsweisen der Ermittlungsbehörden
- Internationale Projekte (Europol, Interpol, Sonstige)

■ Erscheinungsformen der Internet-Kriminalität

- Hacking
- Cracking
- Phishing
- Spoofing
- Viren, Trojaner & Co

■ Rechtsgrundlagen des Internet-Strafrechts

- Cyber-Crime-Convention (CCC)
- Rahmenbeschluss der EU über Angriffe auf Informationssysteme
- Österreichisches Kernstrafrecht (insbes. §§ 118a ff StGB)
- Österreichisches Nebenstrafrecht (Urheber-, Marken-, Datenschutz)
- Zugangskontrolle (ZuKG)
- Strafbare Suchtmittelpropaganda im Internet

■ Mitarbeiterüberwachung – technisch wirksam & rechtlich sicher?

- Auswertung von Logfiles
- Arbeitsrechtliche Grenzen
- Datenschutz und Videoüberwachung

Seminarinhalte:

■ Strafprozessuale Besonderheiten der Internet-Kriminalität

- Auskunftspflicht der Provider
- Überwachung von Telekommunikation

■ Identitätsschutz im Internet und seinen Diensten

- Elektronische Signatur
- Verschlüsselung

■ Der praktische Tipp

- Wie setzt man sich als Opfer von Cybercrimes zur Wehr?

Referenzen:

RA Dr. Clemens Thiele, LL.M. Tax (GGU)

Gründer der Rechtsanwaltskanzlei EUROLAWYER® in Salzburg. Verfasser zahlreicher Publikationen und Fachbücher, jüngst der Kommentierung der Cybercrime-Delikte im Salzburger Kommentar zum StGB (5. Abschnitt – Verletzung der Privatsphäre und bestimmter Berufsgeheimnisse). Eurolawyer® berät und vertritt spezialisiert in allen Rechtsbereichen des E-Commerce, insbesondere im Internetrecht. Der Tätigkeitsbereich liegt daher überwiegend im gewerblichen Rechtsschutz (Domain-, Marken- und Wettbewerbsrecht), im Urheberrecht sowie im IT-, Presse- und Medienrecht.

DI Dr. Christian Reiser

Experte für Informationssicherheit bei der Erste Group Bank AG, nachdem er als selbstständiger Berater die verschiedensten Firmen aus fast allen Branchen in Bezug auf Schutz ihrer virtuellen Werte unterstützt hat. Dabei setzte er neben Standards wie ISO 27001 und Cobit auch den Standard des gesunden Menschenverstandes ein. Unter seinen zahlreichen Veröffentlichungen ist auch ein Buch über die elektronische Unterschrift zu finden, das er gemeinsam mit drei Juristen geschrieben hat – für ihn als Techniker eine besondere Herausforderung.

Mag. Leopold Löschl

Jurist und EDV-Trainer, als ausgebildeter Polizist ehemals dem Generalinspektorat der Sicherheitswache dem Aufgabenbereich EDV-Organisation und Datenschutz dienstzugehörig. Später Wechsel in das Bundeskriminalamt, wo er 2003 die Funktion des Referatsleiters für Betrugs- und Fälschungsdelikte übernahm. Mit 1.8.2006 wurde ihm die Leitung des Büros für Computer- und Netzwerkkriminalität im Bundeskriminalamt übertragen.