

Ja, ich melde mich an für das Seminar „Der IT-Notfallplan in der Praxis“

Termin _____

Ja, ich bestelle per Nachnahme die Seminarunterlage 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/ E-Mail über weitere Veranstaltungen informiert werde. Als Gerichtsstand wird Wien vereinbart.

1. TEILNEHMER/IN KonzipientIn BerufsanwärterIn

Name / Vorname / Titel _____

Aufgabenbereich / Abteilung _____

Tel. _____ Fax _____

E-Mail _____

2. TEILNEHMER/IN KonzipientIn BerufsanwärterIn

Name / Vorname / Titel _____

Aufgabenbereich / Abteilung _____

Tel. _____ Fax _____

E-Mail _____

FIRMA Beschäftigte bis 100 100-200 über 200

Branche _____

Firma _____

Straße, Postfach _____

PLZ, Ort _____

Datum _____ Unterschrift _____

HP

TERMINE / VERANSTALTUNGORT

Termine 23. September 2010
ARS Seminarzentrum, Schallautzerstraße 2-4, 1010 Wien

07. April 2011
ARS Seminarzentrum, Schallautzerstraße 2-4, 1010 Wien

Uhrzeit jeweils von 9.00-17.00 Uhr

Gebühr je € 450,-

inkl. Seminarunterlage, 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 Teilnahmegebühr bis zum Seminartermin zu überweisen.

PREISSTAFFELUNG

€ 450,- für die/den **1. TeilnehmerIn** eines Unternehmens

€ 410,- für die/den **2. TeilnehmerIn** eines Unternehmens

€ 380,- ab der/dem **3. TeilnehmerIn** eines Unternehmens




20 % für RA-KonzipientInnen, WT-BerufsanwärterInnen, NO-KandidatInnen

Ermäßigungen sind nicht addierbar!

STORNO

Bitte haben Sie Verständnis, dass bei Stornierungen ab 14 Tage vor Seminarbeginn 50 % des Seminarbeitrages, bei Stornierungen oder Nichterscheinen am Veranstaltungstag die volle Gebühr in Rechnung gestellt wird. Bei jeder Stornierung beträgt die Bearbeitungsgebühr € 40,-. 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 Seminare aus wichtigen Gründen zu verschieben sowie Programmänderungen vorzunehmen.

ANMELDUNG

 (01) 713 80 24-14  (01) 713 80 24-17  office@ars.at

INFORMATION

Projektorganisation: Katharina Ludwin
Inhalt / Konzeption: Elisabeth Binder



Der IT-Notfallplan in der Praxis



Bedrohungsbilder erkennen & abwehren



23. September 2010, Wien
07. April 2011, Wien
jeweils von 9.00-17.00 Uhr



ARS
AKADEMIE
FÜR RECHT,
STEUERN &
WIRTSCHAFT

Von den Besten lernen.

Gesamtprogramm auf www.ars.at

DVR Nr.: 0927571



IHR NUTZEN

IT-Sicherheit wird oft als unliebsames Thema gesehen, das man gerne vor sich herschiebt. Es entstehen dabei Kosten, es erfordert laufende Kontrolle, Verbesserungen und vor allem Schulungen der eigenen IT-Mannschaft, da die Bedrohungsbilder mannigfaltig sind und sich häufig ändern.

Der Win32/Conficker-Computerwurm, der seit Oktober 2008 weltweit wütet und auch in Österreich sehr prominente Opfer gefunden hat, demonstriert in einer sehr deutlichen Sprache, wie wichtig ein funktionierender Notfallplan geworden ist. Ein lebbarer und funktionierender IT-Notfallplan hilft Ihnen beim Disaster Recovery (Wiederherstellung) Ihrer IT-Infrastruktur.

Dieses Seminar soll das entsprechende Bewusstsein vermitteln, welche Bedrohungsbilder derzeit aktuell sind, wie sich der Win32/Conficker-Wurm so rasant ausbreiten konnte und wie ein IT-Notfallplan beschaffen sein müsste, um einen effizienten Disaster-Recovery-Prozess zu ermöglichen. Anhand von praktischen Beispielen und Live-Demonstrationen wird die Grundstruktur eines Notfallplanes erstellt, der Ihnen bei einem Anti-Virus-Befall helfen wird.

REFERENT



Ing. Thomas Mandl

Ing. Thomas Mandl IT-Security Consulting; vorher CTO bei IKARUS Security Software, zuvor 8 Jahre Senior System Administrator und Leiter Rechenzentrum eines US-High-Tech-Microchip-Konzerns (Standort Wien); Inhaber von europäischen Softwarepatenten im Bereich Soft- und Hardware Security; Spezialgebiete: UNIX/Linux und Windows OS Hardening, forensische Analysen von Hacker- und Virenattacken, Firewalls und Intrusion Detection Systeme, Penetration Tests und Security Audits; Vortragstätigkeit (u. a. an der Donau-Universität Krems, FH Technikum Wien, TU Wien) zum Thema IT- und Information Security.

SEMINARINHALTE

■ Bedrohungsbilder im Wandel (Kurzübersicht)

- Wie sieht es derzeit wirklich aus? Welche Angriffsszenarien gibt es, womit ist zu rechnen, was ist wahrscheinlich?
- Arbeitsweise der organisierten Kriminalität im Cyber Space
- Drive-by-Infektionen
- Aktuelle Statistiken zu den Themen Vulnerabilities, Betriebssystemsicherheit, Browser-Sicherheit, Angriffsmethoden und Auswirkungen
- Angriffsziel 3rd Party Software (Adobe PDF Reader, Apple Quicktime, etc.)
- Live-Demonstration von Angriffen auf Clientsysteme durch 3rd Party Software
- Rootkits (am Beispiel von Mebroot) - wie sie arbeiten, was sie können und warum sie so gefährlich sind
- Relevanz für den Notfallplan

■ Conficker und Malware 2.0

- Conficker-Detailinformationen und praktische Erfahrungsberichte
- Was wir daraus lernen können (Praxisbeispiele)
- Wo gab es einen Notfallplan und wieso hat der geholfen?
- Was ist bei Disaster Recovery nach Malwarebefall zu beachten?
- Wie stelle ich sicher, dass keine unerwünschte Malware zurückbleibt?
- Welche Prozesse und Techniken sind erforderlich, um eine restlose Wiederherstellung der IT zu gewährleisten?

■ Der IT-Notfallplan

- Definition und Ziele eines Notfallplans
- Vergleiche zu Notfallplänen in anderen Sparten (Flugindustrie, Gesundheitswesen, Betriebssicherheit,...)

- Aufbau eines IT-Notfallplans für das Disaster Recovery durch Virusbefall
- Definition von Rollen und Kontaktlisten
- Alarmierungsplan
- Notbetriebsverfahren und Wiederherstellungsverfahren
- Weitere im Notfall hilfreiche Dokumente
- Welche Systeme sollten in einen Notfallplan aufgenommen werden?
- Inventarisierung und Priorisieren von Systemen
- Welche Abhängigkeiten bestehen zwischen den Systemen?
- Koordination von Gegenmaßnahmen
- Training und Umsetzung eines Notfallplans
- Integration des Notfallplanes in Ihre IT-Prozesse
- Kommunikation bei verteilten Standorten
- Weiterführende Maßnahmen nach einem Disaster Recovery
- Fallbeispiele

WER MUSS INFORMIERT SEIN

- ✓ CIOs und Verantwortliche für Unternehmenskommunikation
- ✓ IT-Sicherheitsbeauftragte
- ✓ Technische LeiterInnen und MitarbeiterInnen von EDV-Abteilungen
- ✓ SystemadministratorInnen
- ✓ NetzwerkadministratorInnen
- ✓ IT- und EDV-BeraterInnen
- ✓ IT-ProjektleiterInnen