IIR

KONFERENZEN
SEMINARE
Wissen, das bewegt

Inkl. neuer Aspekte der EU-Datenschutz-Grundverordnung & des Privacy Shields

IIR Praxislehrgang

IT-Security

Ihre Schwerpunkte:

- **Risikoanalyse in der IT** – Gefahren erkennen und Präventionsstrategien entwickeln
- **Firewalls, Penetration Tests und Verschlüsselungsmethoden** – Vorgehensweisen und Werkzeuge
- **Mobile Security, Internet Tracking & Co** – Aktuelle und kommende Herausforderungen
- **Log Management und SIEM** – So funktionieren Aufzeichnung und Auswertung
- Rechtliche Rahmenbedingungen und IT Standards – **Compliance, Outsourcing und Haftungsfragen**

INTENSIV & KOMPAKT MIT ZERTIFIKAT

3 Tages-Intensivseminar mit Zertifikat

29. November – 1. Dezember 2016, Wien

www.iir.at/IT-Security

1. Tag | 29. November 2016 — 09:00 – 17:00 Uhr

IT-Risiken kennen und verstehen – Die Bedrohungsbilder im Wandel

Aktuelle Bedrohungsszenarien für Ihre IT-Security erleben und verstehen

- Übersicht der IT-Risiken mit aktuellen technischen und organisatorischen Bedrohungsbildern
  - Welche neuen Angriffsszenarien gibt es, wie haben sie sich in letzter Zeit verändert?
  - Ableitung von Gegenmaßnahmen für Ihre IT
- Die Organisierte Kriminalität und ihre Business Modelle
  - Aktuelle Daten und Fakten
  - Infos zu Cyber Crime Organisationen
- Live Demonstration topaktueller Angriffsmethoden
- Aktuelle Statistiken zu den Bedrohungsbildern
- Wo liegen die größten Gefahren für Ihr Unternehmen
  - Erklärung von Bot Netzwerken und die massive Gefahr, die von ihnen ausgeht
  - Designer Malware und Spionage-Trojaner
  - Politisch motivierte Angriffe
- Warum der Incident Response Prozess immer wichtiger wird!
- Zukunftsausblick

FALLBEISPIEL
Live Hacking Demonstration – Methoden kennen und Abwehrmaßnahmen optimieren

- Sehen Sie live, wie Hacker in Ihr System eindringen können, welche Methoden verwendet werden und wie Sie Schwachstellen aufspüren. Erleben Sie diese Demonstration, sehen Sie und verstehen Sie die Bedrohungen.
- Rootkits, Google Hacking, Infektionen durch Drive By Downloads, Man in the Middle Angriffe auf SSL Verschlüsselte Kommunikation, SQL Injection, etc.

Prävention und Analyse von Attacken
Ethical Hacking & Penetration Testing

- Warum Penetration Testing?
- Testen Sie durch gezielte Hackerangriffe die Wirksamkeit Ihrer Security und messen Sie den Erfolg Ihrer bisherigen Maßnahmen
- Erkennen Sie Schwachstellen und leiten Sie Gegenmaßnahmen ein
- Analysieren der Angriffspunkte für die weitere Vorgehensweise

Technische Methoden & Tools für Ihre IT-Sicherheit

SIEM und Log-Analyse

- Der Mehrwert von Log-Analyse Tools zur Erkennung von Anomalien im Netzwerk
- Einsatzbereiche und Anforderungen an die Log-Analyse und Auswertung durch SIEM Tools
- Welche Log-Daten sind grundsätzlich erforderlich um sinnvolle Ergebnisse bei sicherheitsrelevanten Ereignissen zu bekommen?
- Der Mehrwert von Log-Analyse Lösungen
- Praktische Beispiele

WAF – Web Application Firewalls

- Grundsätzliche Funktionsweise und Unterschiede zu IPS Systemen
- Wie können Web Application Firewalls die Sicherheit Ihrer Web Systeme verbessern
- Einsatzbereiche von WAFs
- Vor- und Nachteile

PRAXISBEISPIEL
Live Demonstrationen von modernen Angriffsszenarien

- Welche der vorgestellten Sicherheitslösungen könnte hier helfen?
- Vorgehensweise bei der Implementierung

Secure Mobile Computing
Mobile Security – Die neuen Herausforderungen

- Die Bedeutung von Mobile Security in der heutigen Zeit
- Mobile Geräte unterwegs (Laptops, Smartphones, Blackberries, PDAs) – Wie Sie die steigenden Security-Anforderungen in den Griff bekommen
- Security bei flexiblen Datenträgern (CD-ROMs, USB-Sticks und Festplatten)

Die kommerzielle Nutzung von Social Media: Ein Risiko

- Die Risiken bei der Nutzung
- Bedrohungsbilder durch soziale Netze (direkt und indirekt)
- Die Konsequenzen für das Unternehmen (technisch und organisatorisch)
- Blockade von Social Media Plattformen statt Richtlinien? Social Media Security: Awareness schaffen
- Zugänge sperren vs. Bewusstsein schaffen
- Mitarbeitern die verantwortungsvolle Nutzung beibringen aber wie?
- IT Organisationsrichtlinien und Awareness abstimmen Hackerangriffe durch soziale Netze
- Die Angriffsmöglichkeiten
- Die Bedrohungsbilder
- Technologie: Schutzmechanismen und Scanmethoden
- Beispiele aus der Praxis
  IT Organisationsrichtlinien
- Wie können Social Media Aktivitäten sinnvoll in eine IT Organisationsrichtlinie integriert werden?
- Beispiel aus der Praxis

Trainer:
Ing. Thomas Mandl, *Sr. Security Consultant, Owner, Cyber Defense Consulting Experts e.U.*

**Das Seminar bietet eine große Themenvielfalt. Die genaue Schwerpunktsetzung erfolgt vor Ort und orientiert sich an den Bedürfnissen der anwesenden Teilnehmer.*

2. Tag | 30. November 2016 — 09:00 – 17:00 Uhr

Stichwort Kryptografie
- Die bekanntesten Verschlüsselungsmethoden (AES, RSA, Elliptische Kurven u.a.)
- Definition und Zielsetzung von Public Key Infrastrukturen (PKI)
- Komponenten und Funktionsweise einer PKI
  - Warum ist Kryptographie so wichtig?
  - Schlüsselmanagement

Authentisierung – Tools und Einsatzmöglichkeiten
- Lernen Sie verschiedene Möglichkeiten der Authentisierung kennen
  - Passwort/Passwortalgorithmen
  - Digitale Signatur
  - Biometrie
  - Chipkarten / Hardware Token
  - etc.
- Erfahren Sie die Vor- und Nachteile dieser Technologien

Trainer:
Dr. Ernst Piller, *Geschäftsführer, Smart ID*

Der rechtliche Rahmen – Rechtsvorgaben kennen und sicher erfüllen

Die aktuelle Haftungssituation – Haftungsrechtliche IT-Risiken kennen
- Wer haftet wann – Wo werden die Unternehmensleitung und/oder die Mitarbeiter in die Pflicht genommen
- Zivilrechtliche Haftung/Strafrechtliche Haftung
- Wie kann man prüfen, ob man selbst haftet
- Persönliche Haftungsrisiken kennen und vermeiden
- Kann man IT-Haftungsrisiken versichern – Welche Möglichkeiten gibt es

IT-Sicherheit unter Compliance und IT-Governance Aspekten
- Compliance als internationaler Rechtsstandard
- Anforderungen an die IT-Sicherheit – Vertraulichkeit, Verfügbarkeit und Integrität von Systemen und internen Daten sicherstellen
- Einflüsse aktueller nationaler und internationaler gesetzlicher und technischer Vorgaben
- Elektronische Kommunikation und Rechtsrisiken
- Die Pflicht zur elektronischen Dokumentation

IT-Security und Datenschutz
- Wie funktioniert Datenschutz – Ein Widerspruch in der Praxis
- Welche Rechte/Pflichten gibt es?
- Auslese und Archivieren von Daten der eigenen Mitarbeiter und Geschäftspartner
- Datenschutz vs. Kontrolle und Überwachung der Mitarbeiter
- Die Rolle des Datenschutzbeauftragten im Unternehmen

Stichwort Identitymanagement
- Wie Sie Benutzerdaten durch IDM organisieren und verwalten
- Welche Compliance-Vorgaben sind zu erfüllen
- Wo liegen die Grenzen in der Umsetzung, worauf muss geachtet werden

Computerkriminalität und Strafrecht
- Welche strafrechtlichen Normen gibt es
- Wie werden diese angewendet
- Worauf habe ich im Unternehmen zu achten
- Fallbeispiele

Sonderfall Hackerangriff
- Wie verhalte ich mich richtig
- Welche Rechte/Pflichten treffen mich als Vorstand/IT-Leiter
- Wie kann ich gegen den Täter vorgehen
- Welche Gesetze habe ich einzuhalten

Vertragsregelung gegenüber Security-Outsourcing-Partnern
- Kann ich meine Haftung durch Outsourcing übertragen
- Worauf ist bei Outsourcing zu achten
  - Besondere Verpflichtungen des Auftraggebers bei Outsourcing-Verträgen
  - Handhabung von Leistungsstörungen bei Outsourcing- Verträgen

Trainer:
RA Dr. Axel Anderl, LL.M., *Partner, DORDA BRUGGER JORDIS Rechtsanwälte GmbH*

Mag. Nino Tlapak, LL.M., *Rechtsanwaltsanwärter, DORDA BRUGGER JORDIS Rechtsanwälte GmbH*

3. Tag | 1. Dezember 2016 — 09:00 – 17:00 Uhr

IT-Securitymanagement im Unternehmen

IT-Security Management – Schritt für Schritt Umsetzung im eigenen Unternehmen
- Von der Vision zu realistischen IT-Sicherheitszielen
- Die nachhaltige Integration der Security in das Unternehmensmanagement
- Warum Sie den IT-Security-Prozess als Kerngeschäft definieren sollten
- Wie Sie ein Sicherheitskonzept erarbeiten und eine Security-Policy erstellen
- Zielgerichtete Umsetzung und Kommunikation der Security-Policy
- Erkennen Sie, wie neue Formen der Geschäftsprozesse die IT-Security beeinflussen
- Security-Controlling

Security Awareness – Wie es Ihnen gelingt Sicherheitsbewusstsein zu schaffen
- Mitarbeiter verstehen – Psychologische Aspekte im Zusammenhang mit IT-Security
- Wie weit hat sich das Securitybewusstsein bisher durchgesetzt
- Messung und Evaluierung von Security Awareness im Unternehmen auf organisatorischer und technischer Ebene
- Wie Sie Ihre Mitarbeiter erfolgreich ins Securitykonzept integrieren
- Mobile Security und Sicherheitsbewusstsein – So schaffen Sie die Verknüpfung
- Data Loss Protection/Prevention – Der Umgang mit sensiblen Unternehmensdaten

PRAXISBEISPIEL
Awareness-Kampagnen – Instrumente zur Sensibilisierung der Mitarbeiter

- Umsetzung und Evaluierung einer unternehmensweiten Security Awareness-Kampagne
- Prüfung und Verpflichtung der Mitarbeiter
- Wirksamkeit und weitere Vorgehensweise im Kampf für mehr Security Awareness

Der Weg zur sicheren IT – Erfolgreiches IT Risk Management

- Von der Gefährdung zum Risiko – Bewerten Sie Ihr IT-Sicherheitsniveau
- Welche Instrumente zur Durchführung der Schwachstellenanalyse stehen Ihnen zur Verfügung
- IT-Risikovermeidung – Effiziente Methoden der Risikominimierung
- Das IT-Sicherheitsteam – Personen und organisatorische Einbettung
- Die Rolle des IT-Sicherheitsverantwortlichen
- Risk Management Controlling

Business Continuity Planning und Incident Response

- Nehmen Sie eine Bedrohungsanalyse vor und stufen Sie die Gefährdungen ein
- Erarbeiten Sie einen Notfallplan, um Vorfälle zu managen
- Das Bilden von Computer Emergency Response Teams
- Wie Sie durch intelligente Backup- und Restore-Strategien die Fortsetzung des Betriebs nach Datenverlust gewährleisten

Trainer:
Ing. Franz Hoheiser-Pförtner, MSc, *Certified Information Systems Security Professional (CISSP), FHP Security*

Aktuelle Standards und Normen Standardisierte Informationssicherheit

- Die wichtigsten Standards im Überblick
  - ISO 27000 Reihe
  - BSI Grundschutzhandbuch
  - Andere IT-Standards
- ITIL, COBIT
- ISO 9000
- Gegenüberstellung hinsichtlich Eignung, Aufwand und Zertifizierbarkeit
- Welcher Standard sich für wen eignet und die Anforderungen am besten abdeckt
- Erfüllung von Compliance-Anforderungen mit Hilfe von Informationssicherheit – Normen, Standards und Werkzeuge

PRAXISBEISPIEL
Einführung des Information Security Management Systems (ISMS) nach ISO 27001

- Ziele und Vorgaben des Sicherheitsmanagementsystems
- Organisatorische Forderungen vs. Technische Lösungen
- Die Verknüpfung von Organisation, Technik und Management
- Nutzen vs. Umstellungskosen

Trainer:
Mag. Krzysztof Müller, CISA, CISSP,
selbständiger Sicherheitsexperte

Anmeldung

Tel. +43 (0)1 891 59 – 0 | Fax +43 (0)1 891 59 – 200 | anmeldung@iir.at | www.iir.at

T0481_www

☐ **JA,** ich bestätige meine Teilnahme am IIR Praxislehrgang:
„IT-Security" (21001) von 29. November – 1. Dezember 2016 in Wien

1. TeilnehmerIn

Nachname _____ Vorname _____

Position _____ Abteilung _____

E-Mail _____ Tel./Fax* _____

2. TeilnehmerIn

Nachname _____ Vorname _____

Position _____ Abteilung _____

E-Mail _____ Tel./Fax* _____

Ja, ich möchte Informationen aus dem Themenbereich **„IT/Telekom"** per E-Mail erhalten. ☐ TeilnehmerIn 1 ☐ TeilnehmerIn 2

Firma _____ Branche _____

Straße _____ PLZ/Ort _____

Ansprechperson bei Rückfragen zu Ihrer Anmeldung:

Nachname _____ Vorname _____

Position _____ Abteilung _____

E-Mail _____ Tel./Fax* _____

Wer ist in Ihrem Unternehmen für die Genehmigung Ihrer Teilnahme zuständig?

Nachname _____ Vorname _____

Position _____ Abteilung _____

E-Mail _____ Tel./Fax* _____

Datum/Unterschrift

*Bitte geben Sie Tel./Fax nur bekannt, wenn Sie an weiteren Informationen über unsere Produkte interessiert sind.

Teilnahmegebühr (exkl. 20% USt.)

Einschließlich Dokumentation, Mittagessen und Getränken pro Person:

Bei Anmeldung bis	**19. August 2016**	**€ 2.195,–**
Bei Anmeldung bis	**4. November 2016**	**€ 2.295,–**
Bei Anmeldung bis	**29. November 2016**	**€ 2.395,–**

Nutzen Sie unser attraktives Rabattsystem:

👤👤	bei 2 Anmeldungen erhält ein Teilnehmer	**10 %** Rabatt
👤👤👤	bei 3 Anmeldungen erhält ein Teilnehmer	**20 %** Rabatt
👤👤👤👤	bei 4 Anmeldungen erhält ein Teilnehmer	**30 %** Rabatt

Diese Gruppenrabatte sind nicht mit anderen Rabatten kombinierbar.

Veranstaltungsort

Die Veranstaltung findet in Wien statt.
Der genaue Veranstaltungsort wird noch bekannt gegeben.

Sie erhalten nach Eingang der Anmeldung Ihre Anmeldebestätigung und Ihre Rechnung. Bitte begleichen Sie den Rechnungsbetrag vor dem Veranstaltungstermin. Einlass kann nur gewährt werden, wenn die Zahlung bei IIR eingegangen ist. Etwaige Programmänderungen aus dringendem Anlass behält sich der Veranstalter vor.

Rücktritt: Bitte haben Sie Verständnis dafür, dass wir Ihnen bei einem Rücktritt von Ihrer Anmeldung innerhalb von zwei Wochen vor der Veranstaltung die volle Tagungsgebühr verrechnen müssen. Eine Umbuchung auf eine andere Veranstaltung oder die Entsendung eines Vertreters ist jedoch möglich. Bitte berücksichtigen Sie bei Ihrer Planung: IIR behält sich bis zu zwei Wochen vor Veranstaltungsbeginn die Absage vor.

Im Sinne einer leichteren Lesbarkeit sind manche der verwendeten Begriffe in einer geschlechtsspezifischen Formulierung angeführt. Selbstverständlich wenden wir uns gleichermaßen an Damen und Herren.