



IIR Praxislehrgang

# IT-Security

## 3 Tage-Intensivseminar

- 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



### Ihre Experten:

- RA Dr. Axel Anderl, LL.M., DORDA Rechtsanwälte GmbH
- Ing. Franz Hoheiser-Pförtner, MSc, CISSP, FHP Security
- Ing. Thomas Mandl, Cyber Defense Consulting Experts e.U.
- Mag. Krzysztof Müller CISA, CISSP, NTTSecurity
- Dr. Ernst Piller, Smart ID
- Mag. Nino Tlapak, LL.M., DORDA Rechtsanwälte GmbH

Seit mehr als 10 Jahren über  
200 zufriedene Teilnehmer!



4. – 6. Juli 2017, Wien  
[www.iir.at/IT-Security](http://www.iir.at/IT-Security)

Kooperationspartner:

VERLAG  
ÖSTERREICH

### 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
- Die organisierte Kriminalität und ihre Business Modelle
- Aktuelle Statistiken zu den Bedrohungsbildern
- Wo liegen die größten Gefahren für Ihr Unternehmen?
  - Bot Netzwerken, Designer Malware und Spionage-Trojaner
- Warum der Incident Response Prozess immer wichtiger wird!

#### FALLBEISPIEL

#### Live Hacking Demonstration – Methoden kennen und Abwehrmaßnahmen optimieren

**FALLBEISPIEL**

- Sehen Sie live, wie Hacker in Ihr System eindringen können, welche Methoden verwendet werden und wie Sie Schwachstellen aufspüren
- 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

#### 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**

#### 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

- Bedrohungsbilder durch soziale Netze (direkt und indirekt)
- Die Konsequenzen für das Unternehmen (technisch und organisatorisch)
- Blockade von Social Media Plattformen statt Richtlinien?
- Wie können Social Media Aktivitäten sinnvoll in eine IT Organisationsrichtlinie integriert werden?
- Social Media Security – Awareness schaffen: Zugänge sperren vs. Bewusstsein schaffen
- Hackerangriffe durch soziale Netze: Schutzmechanismen und Scanmethoden

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

09:00 – 12:30 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
- Vor- und Nachteile dieser Technologien

*Dr. Ernst Piller, Geschäftsführer, Smart ID*

13:30 – 17:00 Uhr

#### 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 und Strafrechtliche Haftung
- 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

**DSGVO**

- Wie funktioniert Datenschutz – Ein Widerspruch in der Praxis
- Welche Rechte/Pflichten bringt die EU-Datenschutz-Grundverordnung
- Auslese und Archivieren von Daten der eigenen Mitarbeiter und Geschäftspartner
- Datenschutz vs. Kontrolle und Überwachung der Mitarbeiter
- Die neue Rolle des Datenschutzbeauftragten im Unternehmen
- Sonderfall Hackerangriff: Wie verhalte ich mich richtig?

## Stichwort Identitymanagement

- Benutzerdaten durch IDM organisieren und verwalten
- Welche Compliance-Vorgaben sind zu erfüllen
- Grenzen in der Umsetzung: Worauf muss geachtet werden?

## Computerkriminalität und Strafrecht

- Welche strafrechtlichen Normen gibt es?
- Worauf habe ich im Unternehmen zu achten?
- Fallbeispiele

## Vertragsregelung gegenüber Security-Outsourcing-Partnern

- Kann ich meine Haftung durch Outsourcing übertragen
- Besondere Verpflichtungen des Auftraggebers bei Outsourcing-Verträgen
- Handhabung von Leistungsstörungen bei Outsourcing-Verträgen

*RA Dr. Axel Anderl, LL.M., Partner, DORDA Rechtsanwälte GmbH  
Mag. Nino Tlapak, LL.M., Rechtsanwaltsanwarter, DORDA  
Rechtsanwälte GmbH*

## 3. Seminartag

09:00 – 17:00 Uhr | 6. Juli 2017

09:00 – 14:00 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
- Messung und Evaluierung von Security Awareness im Unternehmen auf organisatorischer und technischer Ebene
- Mobile Security und Sicherheitsbewusstsein – So schaffen Sie die Verknüpfung

#### 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

**PRAXISBEISPIEL**

#### Der Weg zur sicheren IT – Erfolgreiches IT Risk Management

- Von der Gefährdung zum Risiko – Welche Instrumente zur Durchführung der Schwachstellenanalyse stehen Ihnen zur Verfügung
- Welche Instrumente zur Durchführung der Schwachstellenanalyse stehen Ihnen zur Verfügung
- IT-Risikovermeidung – Effiziente Methoden der Risikominimierung
- Das IT-Sicherheitsteam – Personen und organisatorische Einbettung
- Risk Management Controlling

## Business Continuity Planning und Incident Response

- Nehmen Sie eine Bedrohungsanalyse vor und stufen Sie die Gefährdungen ein
- Das Bilden von Computer Emergency Response Teams
- Wie Sie durch intelligente Backup- und Restore-Strategien die Fortsetzung des Betriebs nach Datenverlust gewährleisten

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

14:30 – 17:00 Uhr

### Aktuelle Standards und Normen

#### Standardisierte Informationssicherheit

- Die wichtigsten Standards im Überblick
  - ISO 27000 Reihe
  - BSI Grundschutzhandbuch
  - ISO 9000
- ITIL, COBIT
- 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. Umstellungskosten

**PRAXISBEISPIEL**

*Mag. Krzysztof Müller CISA, CISSP, NTTSecurity*

*Eine inhaltliche Schwerpunktsetzung im Rahmen dieses Trainingsprogramms kann in Abstimmung zwischen den TeilnehmerInnen und den Trainern erfolgen.*

**JA**, ich bestätige meine Teilnahme am IIR Praxislehrgang:  
„IT-Security“ (21181) von 4. – 6. Juli 2017

## 1. TeilnehmerIn

Nachname \_\_\_\_\_ Vorname \_\_\_\_\_  
Position \_\_\_\_\_ Abteilung \_\_\_\_\_  
E-Mail \_\_\_\_\_ Tel./Fax\* \_\_\_\_\_

## 2. TeilnehmerIn

Nachname \_\_\_\_\_ Vorname \_\_\_\_\_  
Position \_\_\_\_\_ Abteilung \_\_\_\_\_  
E-Mail \_\_\_\_\_ Tel./Fax\* \_\_\_\_\_

## 3. 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  TeilnehmerIn 3

Firma \_\_\_\_\_  
Straße \_\_\_\_\_  
PLZ/Ort \_\_\_\_\_  
Branche \_\_\_\_\_

## 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	<b>31. März 2017</b>	<b>€ 2.195,-</b>
Bei Anmeldung bis	<b>9. Juni 2017</b>	<b>€ 2.295,-</b>
Bei Anmeldung bis	<b>4. Juli 2017</b>	<b>€ 2.395,-</b>

## Nutzen Sie unser attraktives Rabattsystem:

	bei 2 Anmeldungen erhält ein Teilnehmer	<b>10 % Rabatt</b>
	bei 3 Anmeldungen erhält ein Teilnehmer	<b>20 % Rabatt</b>
	bei 4 Anmeldungen erhält ein Teilnehmer	<b>30 % Rabatt</b>

Diese Gruppenrabatte sind nicht mit anderen Rabatten kombinierbar.

## Veranstaltungsort

**MID Town Businesscenter**  
Rennweg/Ungarg. 64-66/Stg.3 /1. Stock, 1030 Wien

## IIR Qualitätsgarantie

Ihre Zufriedenheit ist uns wichtig: Stellen Sie am ersten Veranstaltungstag bis 12:00 Uhr mittags fest, dass die gebuchte Veranstaltung nicht Ihren Erwartungen entspricht, so können Sie Ihre Teilnahme abbrechen und erhalten von IIR den vollen Betrag rückerstattet, oder Sie besuchen stattdessen eine andere gleichwertige Veranstaltung.

## Service und Kontakt



**Magdalena Ludl**, Senior Customer Service Manager  
Tel. +43 (0)1 891 59 – 0 | Fax +43 (0)1 891 59 – 200  
E-Mail: anmeldung@iir.at

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.