

Workshop:

IT-Sicherheit im Firmennetzwerk

- Hackingangriffe & Schutzmaßnahmen

Zielgruppe	<ul style="list-style-type: none">• IT-Fachkräfte• IT-Manager / IT-Leiter / CTOs• IT-Sicherheitsbeauftragte• IT-Revisoren
Beschreibung	<p>Der Workshop ist aufgeteilt in Theorie und Praxismodule, so dass die Teilnehmer aus den eigenen Erfahrungen lernen, wie Hacking Attacks durchgeführt werden und welche Auswirkungen diese auf die eigenen Netzwerke haben können. Aufbauend auf dieses Wissen werden dann ökonomisch sinnvolle und rechtlich notwendige Schutzmaßnahmen erarbeitet.</p> <p>Der Praxis-Workshop wird von erfahrenen IT-Security Auditoren gehalten, die Ihre Erfahrungen aufgrund von IT-Security Audits und Penetration Tests und durch IT-Sicherheitsforschung gesammelt haben.</p>
Termine	Montag, den 01.07.2010 und Dienstag, den 02.07.2010 Montag, den 22.11.2010 und Dienstag, den 23.11.2010
Seminarort	Ramada Hotel Exterstraße 2 67433 Neustadt an der Weinstraße http://www.ramada.de/hotels/hotels_index.php?hotel_code=15728
Workshop-Zeiten	10:00 Uhr bis 18:00 Uhr
Dauer	2 Tage
Preis	950,- € zzgl. der gesetzlichen Mehrwertsteuer
	<p>Im Seminarpreis sind folgende Leistungen enthalten:</p> <ul style="list-style-type: none">• Nutzung eines vorinstallierten und konfigurierten Notebooks für die Seminardauer• Pausenverpflegung inkl. Mittagessen

Voraussetzungen	Netzwerkkenntnisse Windows Betriebssystemkenntnisse
Workshopziel	Die Seminarteilnehmer sollen typische Angriffe und Gefahren für die Informationssicherheit des eigenen Unternehmens fachlich verstehen und aufbauend auf das Wissen über aktuelle und zukünftige Hacking-Techniken werden ökonomisch sinnvolle Verteidigungsmaßnahmenansätze und Techniken vorgestellt.

Inhalte

Modul 1 - "Digitale Kriminalität"

- Tendenzen und Trends in der "Digitalen Kriminalität"
- Globalisierung der "Digitalen Kriminalität"
- digitale Straftaten heute und morgen

Modul 2: Angriffs- und Hackingtechniken im internen Firmennetzwerk

- Information Gathering
 - Sniffing
 - Scanning
 - i. Portscanning
 - ii. Service Scanning
 - iii. Vuln-Scanning
- Netzwerkmanipulationen
 - ARP-Poisening
 - ICMP-Redirecting
- Angriffe auf Kennwörter
 - Kerberos
 - LM/NTLM-Hashes
 - POP3 / SMTP
 - RDP-Authentifizierung
- Remote Exploits

Modul 3: Angriffs- und Hackingtechniken gegen Internetplattformen

- Known and Unknown Vulnerabilities Testing
 - BufferOverflow
 - SQL-Injection
 - XSS
 - Directory Indexing
 - Information Leakage
 - Path Traversal
- Authentication Hacking
 - Auth. Bypass
 - BruteForcing / Dictionary Attacks
 - Privilege Escalation
 - ID-Theft / ID-Spoofing
 - Manipulation Session-ID
 - Manipulation Cookie
 - ...

Modul 4: Angriffs- und Hackingtechniken gegen Firmennetze aus dem Internet

- Client-Side Attacks
 - Social Malware
 - Drive-By Downloads
- RAS-Angriffe
 - VPN
 - RDP
 - usw.

Modul 5: Angriffe auf Funkkomponenten

- Handy, iPhone, Blackberry & Co.
 - GSM
 - Bluetooth
 - Handy-Trojaner
- DECT-Telefonie
- WLAN

Modul 6: Schadsoftware (Viren, Trojaner, Bot-Clients)

Aktuelle Viren und Trojaner sind teilweise in der Lage ohne das Antivirenprogramme dies bemerken sich auf PCs und Servern zu installieren. Nach einer erfolgreichen Installation tarnen sich diese Programme.

- Virens Scanner
 - Arbeitsweise von aktuellen Virens Scanner
 - Virenkits oder der Virus im Eigenbau
 - Warum Virens Scanner keinen effektiven Schutz bieten können
- Würmer
 - Vorstellen von aktuellen Wurmern
 - Analyse der Verbreitungsmechanismen
 - Automatisierte Erkennung von Wurmern
 - Honeypots
- Trojaner
 - Identitätsdiebstahl
 - kommerzielle Trojanerbaukästen
- Botnetze
 - Vorstellung aktueller Botnetze
 - Analyse der Arbeitsweise von Botnetzen
 - Vom Trojanerbaukasten zum eigenen Botnetzbetreiber

Modul 7: Schutzmaßnahmen

- Logik der Informationssicherheit
- technische Maßnahmen
 - Analyse der Angriffstechnologien
 - technische Schutzmaßnahmen
- Informationssicherheitsmanagement
 - Aufgaben eines IT-Sicherheitsmanagements
 - Identifizierung kritischer Sicherheitslücken
 - Bewertung kritischer Sicherheitslücken
 - Mitarbeitersensibilisierung