

 **ERNST & YOUNG**

# **eXtreme Hacking – Defending Your Site**

**Schulung**

## Warum Ernst & Young?

Die Sicherheit der Informationstechnik ist heute für den Erfolg und den Bestand eines Unternehmens ein entscheidender Faktor. Als eine der drei größten globalen Wirtschaftsprüfungsgesellschaften arbeiten wir täglich mit diesen Faktoren: Zur Feststellung der ordnungsgemäßen Rechnungslegung wird sowohl die Sicherheit der Anwendungssysteme als auch der Netzwerke und Betriebssysteme mit einbezogen. IT-Sicherheit ist für uns daher ein integraler Bestandteil bei der Planung, der Umsetzung sowie dem Betrieb von Informationstechnik.

Für die Prüfung der technischen IT-Sicherheit hat Ernst & Young praxiserprobte Vorgehensweisen entwickelt, die permanent an aktuelle Gegebenheiten und Technologien angepasst werden. Für die Betriebssystem- und Netzwerksicherheit hat sich unsere Vorgehensweise bereits als Quasi-Standard etabliert und wurde unter anderem in den Büchern „Hacking Exposed – Network Security Secrets & Solutions“ und „HackIT – A Guide To Security Through Penetration Testing“ von Ernst & Young-Mitarbeitern publiziert.

Die Vermittlung dieser Kenntnisse bieten wir als Dienstleistung – losgelöst von der Abschlussprüfung – am Markt an. Denn in Zeiten immer knapper werdender Budgets ist es wichtig, eigene Kompetenzen im Unternehmen aufzubauen, um die Sicherheit gewährleisten zu können. Aus diesem Grund haben wir vor mehr als sechs Jahren die fünftägige Ernst & Young „eXtreme Hacking Class“ Schulung entwickelt und seit dem stetig aktualisiert.

Unser Ansatz ist es, Sie in die Lage zu versetzen, technische Sicherheitsprüfungen selbstständig durchzuführen. Somit können Sie Einsparungen durch ansonsten extern zu vergebende Penetrationstests realisieren bzw. externe Dienstleistungen optimieren.

Ziel der Schulung ist es, Administratoren, IT-Revisoren, Sicherheitsverantwortlichen und Entwicklern Methoden und Vorgehensweisen von „Hackern“ zu vermitteln und somit auf potenzielle Schwachstellen bei der Konzeption, Umsetzung und dem Betrieb von Informationssystemen und Netzwerken hinzuweisen.

Hierbei legen wir größten Wert auf den Praxisbezug. Daher sind ca. 50 Prozent der Zeit für praktische Übungen vorgesehen, bei denen die Teilnehmer aktiv in IT-Systeme eindringen und technische Schutzmaßnahmen umgehen.



## Agenda

### Beginn der Schulung:

Montag, 19. März 2007, 10.00 Uhr

### Ende der Schulung:

Freitag, 23. März 2007, 16.00 Uhr

### Tagesablauf:

Die Schulung beginnt täglich um 9.00 Uhr und endet um circa 18.00 Uhr mit der Option, sich auch nach 18.00 Uhr noch mit den Übungen zu beschäftigen (open end). Am Tag der gemeinsamen Abendveranstaltung endet der Schultag pünktlich um 18.00 Uhr.

**Tag 1: Discovery/Scanning** Target Acquisition, Host Discovery, TCP Fingerprinting, Port Scanning, Banner Retrieval, Intrusive Techniques, Custom Tools, Automated Scanners, War Dialing, Putting it all together – Hands on Exercise.

**Tag 2: Profile Windows** Background NT, 2000, 2003 and XP, Methodology, Target Identification, Windows Security Model, Registry, Active Directory Security, NetBios Hacking, Enumeration, LDAP Security, Authentication and Authorization, LSA-Secrets and Password Cracking, IPSec and Kerberos, Routing over Non-Routable Protocols, Terminal Services and Remote Desktop Security, Local Privilege Escalation, „20 Things To Do After You Hacked Admin“, WFP, DEP, Encrypted File System, Hands on Exercise, Countermeasures.



**Tag 3: Profile Unix** Discovery/Scanning, Target Acquisition, Remote Information Gathering, Vulnerability Mapping, Remote Access, Buffer Overflow Attacks, Local Information Gathering, Local Privilege Escalation, Further Exploits, Hacking the Next Hop, Hands on Exercise, Countermeasures

**Tag 4: Web Applications** Web Applications: Information Gathering/Host Identification, General Web Server Vulnerabilities, Basic Webserver Misconfigurations (Attacking Webbased Authentication, SSL Attacks, Webproxies, Cookies, IDS Evasion), Web Application Exploits (SQL Injection, Cross Site Scripting, Phishing, Session Ids, Session Replay, Session Hijacking), Hands on Exercise, Countermeasures.

**Tag 5: Datenbanken/Advanced Techniques** Databases: Oracle, MS-SQL, SYBASE – Hacking, Hands on Exercise. Advanced techniques: Port Redirection, Backdoors, Tunneling, Sniffing, Eavesdropping, Keystroke Capturing, TCP Session Hijacking, GUI Hijacking, DNS & IP Spoofing, Metasploit Framework, Hands on Exercise (Final Lab: All OS/Databases/Advanced Techniques).

### Referenten

Wir setzen ausschließlich speziell geschulte und erfahrene Ernst & Young „eXtreme Hacking Class“ Trainer ein. Alle unsere „eXtreme Hacking Class“ Trainer haben umfangreiche mehrjährige Erfahrung in Attack & Penetration-Projekten gesammelt und sind durch kontinuierliche Weiterbildung stets auf dem neuesten Stand der Technik und Methodik.

Nähere Informationen zu der Schulungsinhalten und den Referenten erhalten Sie auf unserer Webseite: <http://www.de.ey.com/hacking> oder telefonisch unter: (06196) 996 10246.

## Teilnahmebedingungen

Folgende Voraussetzungen gelten für die Teilnahme an unserer „eXtreme Hacking“ Schulung:

### **Sprache:**

Die Schulung wird in deutscher Sprache gehalten. Unterlagen gibt es wahlweise in deutscher oder englischer Sprache.

### **Technisches Verständnis:**

Ein Verständnis von TCP/IP und ein gewohnter Umgang mit den Betriebssystemen Microsoft Windows NT/2000/XP und Unix/Linux Varianten sind notwendig. Für beide Betriebssysteme sollten den Teilnehmern die folgenden Tätigkeiten geläufig sein: Benutzerkonten erstellen,

Dienste installieren und benutzen, Patches installieren, Modifikation von Systemdateien, Identifikation von TCP/IP Ports für gängige Services sowie ein Verständnis der verschiedenen Authentisierungsmechanismen von Betriebssystemen.

### **Ethische Grundeinstellung:**

Das im Rahmen dieser Veranstaltung vermittelte Wissen ist hochsensibel, so dass es ohne ethisch verantwortlichen Umgang ein hohes Gefährdungspotenzial darstellt. Alle Teilnehmer müssen daher vor der Schulungsteilnahme schriftlich einem selbstverpflichtenden, ethischen Kodex zustimmen.

### **Non-Compete Agreement:**

Wir bieten diese Art von Schulungen ausschließlich im Interesse unserer Mandanten an. Aus diesem Grund müssen sich alle Teilnehmer in Form eines „Non-Compete Agreements“ dazu verpflichten, das erworbene Wissen nicht zum Zwecke des Wettbewerbs gegen Ernst & Young zu benutzen.



### Ort

Die Schulung findet in den Schulungsräumen von Ernst & Young statt.

Ernst & Young AG  
Mergenthalerallee 3-5  
65760 Eschborn/Frankfurt am Main  
Telefon (06196) 996 10246  
Telefax (06196) 8024 10246

### Gebühren

Die Teilnahmegebühr für die „eXtreme Hacking“ Schulung beträgt EUR 3.990,- zzgl. 19 % MwSt. Bei zwei oder mehreren Teilnehmern der gleichen Firma gewähren wir einen Rabatt von 10 % pro Teilnehmer. Frühbucher erhalten bei Anmeldungen bis 4 Wochen vor Schulungsbeginn zusätzlich 10 % Rabatt.

**Bedingungen:** Eine garantierte Schulungsplatzzuteilung kann von unserer Seite erst nach Bestätigung der Anmeldung erfolgen.

**Rücktrittsrecht:** Anspruch auf eine komplette Rückerstattung der Schulungsgebühren besteht nur bei einer schriftlichen Stornierung mindestens 21 Tage vor Schulungsbeginn. Ein Austausch des Schulungsteilnehmers kann unter Vorbehalt unserer schriftlichen Zustimmung



vor Schulungsbeginn vorgenommen werden. Für Stornierungen nach 21 Tagen vor Schulungsbeginn können wir leider keine Gebühren zurückerstatten. Eine Anrechnung auf einen späteren Kurstermin ist jedoch zu 75 % möglich.

Ernst & Young behält sich das Recht vor, die Schulungstermine aus wichtigem Grund zu verschieben, zu streichen bzw. Teilnehmer abzulehnen. Eine Schulung findet nur bei mindestens 10 Teilnehmern statt. Sollte eine Terminverschiebung unvermeidbar sein, so werden die Kursteilnehmer spätestens 7 Tage vor Schulungsbeginn per E-Mail/Telefon von uns benachrichtigt.

### Inklusivleistungen

Die Teilnahmegebühr beinhaltet folgende Leistungen:

- Teilnahme an der Schulung inkl. der Benutzung eines Schulungs-Computers pro Teilnehmer, alle notwendigen Programme, gemeinsame Nutzung einer Internetanbindung
- Zertifikat über die erfolgreiche Teilnahme
- Schulungsordner
- Täglich Erfrischungen und Mittagessen
- Eine gemeinsame Abendveranstaltung
- Ein „eXtreme Hacking“ Polo-Shirt

## Anreise

Die Anreise erfolgt auf eigene Kosten der Teilnehmer.

**Anreise mit dem PKW:** Von der Autobahn A5 aus Richtung Norden: Fahren Sie am Nordwestkreuz auf die Autobahn A66 Richtung Wiesbaden bis zum Dreieck Eschborn und nehmen dort die Ausfahrt Eschborn/Kronberg.

Von der Autobahn A5 aus Richtung Süden: Fahren Sie am Westkreuz auf die Autobahn A648 Richtung Wiesbaden. Am Dreieck Eschborn führt die A648 auf die A66. Nehmen Sie die Ausfahrt Eschborn/Kronberg.

Von der Autobahn A66 aus Richtung Wiesbaden: Fahren Sie bis zum Dreieck Eschborn und nehmen dort die Ausfahrt Eschborn/Kronberg.

Nach der Ausfahrt Eschborn/Kronberg biegen Sie an der ersten Ampel-Kreuzung rechts in die Frankfurter Straße ab und fahren die erste Möglichkeit links in die Mergenthalerallee. Unser Gebäude befindet sich nach ca. 400 Metern auf der linken Seite. Besucherparkplätze stehen Ihnen jeweils zur Verfügung.

**Anreise mit der Bahn:** Vom Flughafen Frankfurt: Mit der S-Bahn, U-Bahn oder der Deutschen Bahn Richtung Hauptbahnhof.

Am Hauptbahnhof umsteigen in die S-Bahn-Linie S3 Richtung Bad Soden oder in die S4 Richtung Kronberg bis zur Haltestelle Eschborn-Süd. Ca. 10 Minuten Fußweg bis zu den Büros.

**Anreise mit dem Taxi:** Fahrtzeit (abhängig von der Verkehrslage) vom  
- Hauptbahnhof ca. 20 Minuten  
- Flughafen ca. 25 Minuten

## Service-Hotline

Haben Sie noch Fragen? Rufen Sie uns an! Wir helfen Ihnen gerne.

## Anmeldung/Kundenservice:

Frau Susann Schwendke  
Ernst & Young AG  
Mergenthalerallee 3-5  
65760 Eschborn/Frankfurt am Main  
Telefon (06196) 996 10246  
Telefax (06196) 8024 10246  
E-Mail [susann.schwendke@de.ey.com](mailto:susann.schwendke@de.ey.com)

## Schulungsinhalt:

Herr Lars Weimer  
Ernst & Young AG  
Mergenthalerallee 3-5  
65760 Eschborn/Frankfurt am Main  
Telefon (06196) 996 27489  
Telefax (06196) 8024 27489  
E-Mail [lars.weimer@de.ey.com](mailto:lars.weimer@de.ey.com)

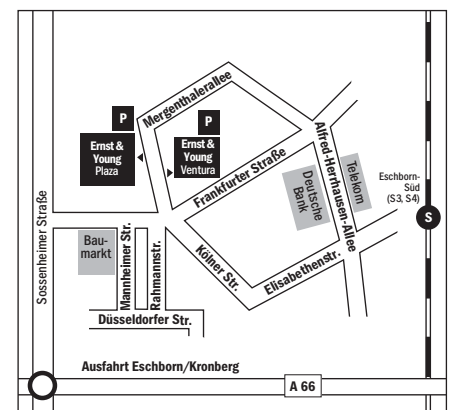
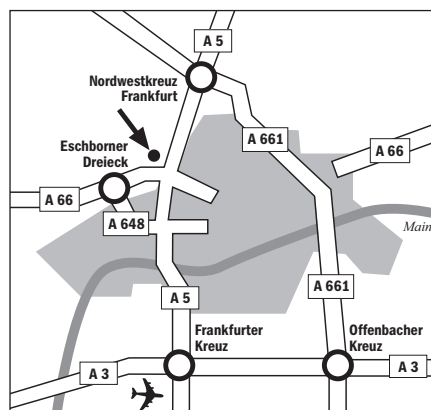
## Unterkunft

Für Teilnehmer, die eine Unterkunft in Frankfurt/Eschborn benötigen, steht im Mercure-Hotel ein begrenztes Zimmerkontingent zu einem Preis von ca. 110 Euro pro Nacht zur Verfügung. Der Preis kann durch Messen, die zum gleichen Zeitpunkt in Frankfurt stattfinden, variieren.

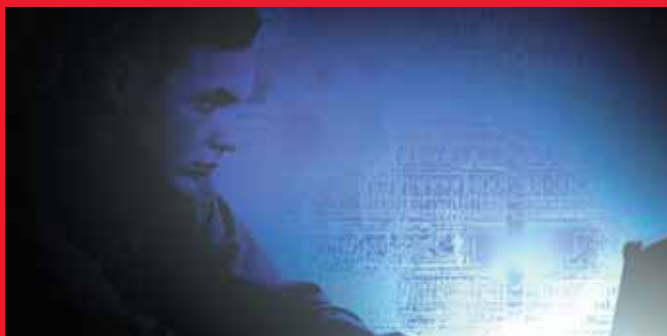
Bitte buchen Sie direkt im Hotel unter Angabe des Buchungscode „eXtreme Hacking“.

Die Hotelkosten werden von den Teilnehmern selbst getragen.

Mercure Hotel Eschborn  
Frankfurter Str. 71-75  
65760 Eschborn/Frankfurt am Main  
Telefon (06196) 7790 0  
Telefax (06196) 7790 500







ERNST & YOUNG AG  
WIRTSCHAFTSPRÜFUNGSGESELLSCHAFT  
STEUERBERATUNGSGESELLSCHAFT

[www.de.ey.com](http://www.de.ey.com)