

Com training and services:

„Jeder zweite Mitarbeiter öffnet Internet-Piraten Tür und Tor“

Jährlich entsteht **10 Milliarden Euro Schaden** durch Hacker in Deutschland. Doch nur jede fünfte deutsche Firma ist sich der drohenden Gefahr bewusst. Mit **FBI-Methoden** steuert das Trainingsunternehmen **Com training and services** diesem Trend nun entgegen und schult deutsche Unternehmen in einem weltweit anerkannten **Security-Kurs**.

MÜNCHEN. Wie groß die Sicherheitslücken im Internet sind und wie anfällig das World Wide Web für Angriffe von Hackern ist, zeigt der Fall, der vergangene Woche die gesamte IT-Welt hochschrecken ließ: Eine durch Zufall entdeckte Panne im Internet hätte es Hackern beinahe ermöglicht, die Kontrolle über das weltweite Datennetz zu übernehmen. Der Fehler, den der Sicherheitsspezialist Dan Kaminski entdeckte, lag am Herzstück des Internets, dem Domain Name System (DNS). Hätten Hacker denselben Fehler entdeckt, wäre es ihnen möglich gewesen, die Zuordnung jeder einzelnen Internetseite zu verändern – und das World Wide Web zu beherrschen.

„Die meisten Sicherheitslücken im Netz entstehen jedoch auf ganz banale Art und Weise. Nämlich durch Unachtsamkeiten der Mitarbeiter. Jeder zweite öffnet Internet-Piraten unbewusst Tür und Tor. Kaum eine Firma in Deutschland, die nicht davon betroffen ist“, erklärt Wolfgang Schaffer, Geschäftsführer des deutschen Trainingsanbieters *Com training and services*. Die Folgen dieser vermeidbaren Sicherheitslücken sind drastisch. In Deutschland gehe man von einem jährlichen Schaden in der Höhe von rund 10 Milliarden Euro aus, warnte zuletzt das Bundesamt für Verfassungsschutz. Weltweit sollen es mehr als 700 Milliarden Euro sein. Nur jedes fünfte deutsche Unternehmen jedoch schätzt laut einer aktuellen Studie die Gefahren richtig ein.



„Die meisten Sicherheitslücken entstehen durch Unachtsamkeit der Mitarbeiter.“

Wolfgang Schaffer, Com-Geschäftsführer

Com training and services steuert aus aktuellem Anlass diesem Trend entgegen und bietet zum Schutz der deutschen Unternehmen vor Hacker-Angriffen jene IT-Security-Ausbildung an, auf die in den USA die meisten staatlichen Institutionen setzen – wie zum Beispiel die US-Army, das FBI oder auch die CIA. *Com*-Geschäftsführer Schaffer: „In unseren 5-tägigen Seminaren lernt man unter Anleitung eines Experten nicht nur wie man die eigene Anlage durchsucht, testet und hackt, sondern auch wie man alle Sicherheitslücken schließt und die Mitarbeiter des Unternehmens auf IT-Sicherheit schult. Unser IT-Security-Zertifikat ist das einzige, das weltweit anerkannt ist.“



Com training and services bietet den Kurs an insgesamt 5 seiner 29 Standorte in Deutschland an: München Perlach, Nürnberg, Mainz, Dortmund und Leipzig.

Entwickelt wurde das IT-Security-Programm von der US-Internetorganisation EC-Council. „Das Besondere an diesem Programm ist, dass es im Gegensatz zu vergleichbaren Systemen unabhängig vom Hersteller angewendet werden kann. Egal ob man mit Linux, Windows oder einem anderen Betriebssystem arbeitet – die Anwendungen sind immer dieselben. Auch aus diesem Grund ist das Zertifikat weltweit anerkannt. Die US-Regierung arbeitet damit, ebenso renommierte Unternehmen wie American Express, Sony oder IBM Global Services“, so Schaffer. Das Programm wird von internationalen Wissenschaftlern und IT-Experten laufend auf aktuellem Stand gehalten.

Über *Com training and services*

Com training and services gehört zu den größten Trainingsunternehmen im deutschsprachigen Raum und bietet an 30 Standorten in Deutschland und Österreich erfolgsorientierte IT- und Soft Skill-Trainings im Businessbereich an.

Com bündelt – einmalig in der Schulungsbranche – das Know-how und die Ressourcen eines Global Players mit der Initiative und Flexibilität eines selbstständigen Partners. Das Kursangebot umfasst mehr als 200 Trainings und Schulungen.

Com steigert durch neue Ausbildungskonzepte und Methoden (Blended Learning) die Produktivität von Mitarbeitern aus Unternehmen und verbessert deren Job-Kompetenz. Das Unternehmen wurde 1995 als Partnernetz für IT-Trainings von Siemens gegründet und ist seit 2004 Teil der österreichischen bit gruppe. *Com training and services* ist ordentliches Mitglied im Deutschen und Österreichischen Franchise-Verband.

Detaillierte Informationen zum Kursangebot finden Sie auf den folgenden 2 Seiten sowie unter www.com-training.com

Kontakt und Informationen:

Com Computertraining und Service GmbH
Carl-Wery-Straße 42
81739 München
Tel.: (089) 450 81 660
Fax: (089) 450 81 6688
Servicetelefon: 0800 10 89 108
info@com-training.com
www.com-training.com

Das IT-Security Kursangebot:

CEH – Ethical Hacker and Countermeasures

In diesem Training erlernt man in einer interaktiven Umgebung, wie man die eigenen Systeme und Anlagen durchsucht, testet und hackt. Die praxisorientierte Arbeitsweise vermittelt detailliertes Wissen und praktische Erfahrung über die aktuellen gängigen Sicherheitssysteme.

Zunächst wird die Funktionsweise von Sicherheitssystemen kennengelernt. Indem man, unter Anleitung des Dozenten, sein eigenes Netzwerk attackiert und durchsucht, erschließt sich Ihnen die Perspektive eines potenziellen Angriffes. Selbstverständlich werden keine Echtumgebungen beschädigt.

Weitere Inhalte: Zugriffserkennung, Methodengestaltung, Richtliniengestaltung, Strategiegestaltung, Social Engineering, DDoS Angriffe, Zwischenspeicher-Überlauf sowie Viruserstellung.

Das Training ist die Vorbereitung für die EC-Council Certified Ethical Hacker Prüfung 312-50.

Dauer: 5 Tage
Termin 1: 22. bis 26. September 2008
Termin 2: 27. bis 31. Oktober 2008
Termin 3: 1. bis 5. Dezember 2008
Seminarorte: München Perlach, Nürnberg, Mainz, Dortmund, Leipzig

CHFI – Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigation ist der Prozess zwischen dem erkannten Hackingangriff und dem Analysieren des kriminellen Aktes.

Dieses Training vermittelt das notwendige Handwerkszeug, um die Spuren eines Eindringlings zu identifizieren und die nötigen Beweise für eine strafrechtliche Verfolgung zu sammeln.

Viele der heutigen Top-Werkzeuge aus dem Gerichtswesen werden in diesem Training unterrichtet, dies beinhaltet Software, Hardware und fachkundiges Methodenwissen. Wenn man das Wissen um die Identifikation, das Aufspüren und die strafrechtliche Verfolgung von Cyber-Verbrechern erlangen möchten, ist dieses Training genau das richtige.

Nach Besuch des Trainings kann die Prüfung 312-49 zum Computer Hacking Forensic Investigator (CHFI) abgelegt werden.

Dauer: 5 Tage
Termin 1: 10. bis 14. November 2008
Termin 2: 15. bis 19. Dezember 2008
Seminarorte: München Perlach, Nürnberg, Mainz, Dortmund, Leipzig

ECSA/LPT – EC Council Security Analyst

Dieses Training ergänzt die Zertifizierung zum Certified Ethical Hacker (CEH) durch die analytischen Prozesse im Ethical Hacking. Während der Certified Ethical Hacker aktiv Hacking Tools und Technologien nutzt, geht der Security Analyst weiter und verfolgt die entdeckten Angriffe mit fortgeschrittenen Methoden, Tools und Techniken und mit umfassenden IT-Sicherheitstests.

Er verringert so die Angriffsrisiken und verbessert gleichzeitig die Sicherheit der Infrastruktur. Die ersten drei Tage werden die Inhalte zur Zertifizierung als Certified Security Analyst (ECSA) behandelt. Die beiden letzten Tage widmen sich der Zertifizierung zum Licensed Penetration Tester (LPT).

Nach Besuch des Trainings kann die Prüfung 412-79 zum Certified Security Analyst (ECSA) abgelegt werden. Das Bestehen der Prüfung ist Voraussetzung für die Zertifizierung zum Licensed Penetration Tester (LPT).

Dauer: 5 Tage

Seminarorte: München Perlach, Nürnberg, Mainz, Dortmund, Leipzig