integrata Cegos Group | inspire qualify change

SICHERHEIT IN VERNETZTEN SYSTEMEN

Methoden, Konzepte, Lösungsansätze

Dauer: 3 Tage

Durchführungsart: Präsenztraining

Zielgruppe: Fach- und Führungskräfte, IT-Sicherheitsverantwortliche, Systemadministratoren, Netzwerkadministratoren, Datensicherheitsbeauftragte.

Voraussetzungen: 5260 oder vergleichbare Kenntnisse.

Nr.: 5226
Preis: 1.590,00 € (netto) / 1.892,10 € inkl. 19% MwSt.

Schulungsmethode: Vortrag, Diskussion, Fallbeispiele, Demonstrationen.

Das Seminar "Sicherheit in vernetzten Systemen" befasst sich mit der Fragestellung "Aus welchen Komponenten setzt sich ein IT-Sicherheitskonzept zusammen?" und beschreibt die einzusetzenden Methoden und Verfahren zur Bewertung und Verbesserung des IT-Sicherheitsstatus.
Auf der Basis verfügbarer Sicherheitsmechanismen/-standards, realisierbarer Funktionen und Komponenten können Sie die Anforderungen an die Sicherheit von vernetzten Systemen und Unternehmensnetzwerken bestimmen. Sie sind in der Lage, geeignete Komponenten auszuwählen und in einen bestehenden IT-Betrieb zu integrieren.

Voraussetzungstest zu diesem Seminar

Programm

IT-Sicherheit und aktuelle Risikobewertung:
Grundbegriffe - Vielfalt der Bedrohungen - Risiko-Analyse/-Management - Sicherheitskonzepte - Security Scanner - Business Contingency/Disaster Recovery - Security Management

Sicherheitsstandards:

Gesetze - Standards (BS und ISO/IEC 27001) - IT-Grundschutz nach BSI - Aktuelle Entwicklungen

Grundschutz in WAN und Mobil:

Benutzer- und Berechtigungsverwaltung - Verzeichnisdienste (LDAP-Verzeichnisse, ADS) - Single SignOn - Firewalltechniken - Viren- und Trojanerschutz - Intrusion Detection / Prevention Systeme (IDS / IPS) - Content Security - Mobile Sicherheit

Angriffsszenarien im Netzwerk und gegen Systeme:

Spezifische Probleme TCP/IP, Wireless LAN, Betriebssysteme - Applikationen - Lösungsansätze - Mobile Endgeräte

Einführung in kryptografische Mechanismen:

Digitale Signaturen - Zertifikate - Hash-Code - KERBEROS - IPSEC - Public Key Infrastructure (PKI) - Authentifizierung - Biometrik

Sicherheitsoptionen im Internet/Intranet/e-Commerce:

Einsatz kryptografischer Mechanismen und Standards (z.B. PGP, S/MIME, SSL, HBCI, Kerberos, X509) - Virtual Private Networks (VPN)

Computer Forensik:

Forensische Untersuchungen - Datenanalyse - Gerichtsverwertbare, reproduzierbare Ereignisse

Termine und Orte: 19 März 2019 – Nr.: 5226

Stuttgart

20 Mai - 22 Mai 2019 Garantietermin

Hamburg

04 Sep - 06 Sep 2019 Garantietermin

Düsseldorf

02 Dez - 04 Dez 2019

integrata Cegos Group | inspire qualify change

MALWARE UND COMPUTERVIREN

Definitionen, Wirkungsweisen, Schutz- und Notfallmaßnahmen

Dauer: 3 Tage

Nr.: 8042

Durchführungsart: Präsenztraining

Schulungsmethode: Vortrag, Diskussion, Übungen, Fallbeispiele, ganztägiges Praktikum mit echter, in der Praxis vorkommender Malware.

Zielgruppe: Administratoren, Organisatoren, Systemplaner, IT-Führungskräfte, Netzwerkverantwortliche.

Voraussetzungen: Gute IT-Kenntnisse.

Nach diesem Seminar kennen Sie die Wirkungsweisen von Malware und wissen, wie man sie erkennen und beseitigen kann. Sie sind mit den notwendigen Client- und Serverschutzmaßnahmen vertraut und lernen die wichtigsten Antivirenprogramme kennen. Praktische Beispiele mit echter Malware unterstreichen die theoretischen Ausführungen

Programm

Einführung:
Geschichte der Computerviren/Malware - Definitionen und Wirkungsweisen - Quellen der Verbreitung - Schäden durch Malware - Arbeitsweisen der unterschiedlichen Typen und Varianten

Aktuelle Bedrohungen:

Spyware - Phishing - Würmer - Rootkits

Typen von Malware:

Trojaner - Würmer - Bot-Viren - Adware - Rootkits

Infizierungsabläufe und Verhalten bei Befall:

Reproduktionsteil, Erkennungsteil, Schadensteil, Bedingungsteil, Tarnungsteil - Datensicherung - Rechnerstart ohne Virus - Entfernung von File-, Boot-, Makroviren, Würmer und Rootkits - Wiederherstellung eines infizierten Systems

Schutzmechanismen gegen Computerviren:

Einsatz von Anti-Malware-Programmen - Schutz durch speicherresistente Programme - Antivirus Client- und Serverkonzepte - Distribution von Virensignaturen - Online Scanner - Schutz bei mobilen Geräten (z.B. Smartphones, Tablets)

Verwendung von Viruswalls:

Funktion und Varianten - Virenscanner am Gateway oder als Proxy - HTTP-, FTP-, SMTP-Schutzmechanismen

Allgemeine Informationen zur Virenproblematik:

Allgemeine Forderungen an Viren-Suchprogramme - Funktionsklassen für Antivirusprodukte

integrata Cegos Group | inspire qualify change

WORKSHOP: ADVANCED HACKING

Angriffe auf Server und Applikationen erkennen und abwehren

Dauer: 5 Tage

Durchführungsart: Präsenztraining

Zielgruppe: Systemadministratoren, Netzwerkadministratoren, Sicherheitsbeauftragte.

Voraussetzungen: Praxiserfahrung mit TCP/IP. Fortgeschrittene Kenntnisse von Linux- und Windows-Servern.

Nr.: 5199
Preis: 2.290,00 € (netto) / 2.725,10 € inkl. 19% MwSt.

Schulungsmethode: Bei diesem Seminar handelt es sich um einen Praxisworkshop. Zu jedem Thema werden Übungen mit den behandelten Tools und Servern durchgeführt.

Nach diesem Hacking Workshop kennen Sie die Methoden und Tools der Hacker. Sie können Angriffe auf Ihre IT-Infrastruktur, Ihre Server und Ihre Applikationen erkennen und zur Beweissicherung dokumentieren. Sie können Schutzmaßnahmen ergreifen, die Einbrüche verhindern und Angriffe erschweren

Programm

Preparing the attack:

- Information Gathering
- Fingerprinting
- Port Scanning
- Google Hacking
- Buffer Overflows

Hacking Operating Systems:

- Enumeration
- Attacking Windows
- Attacking Unix
- Privilege Escalation
- Exploiting Trust Relationships
- Password Cracking
- Reverse Shells

Client-side Attacks:

- Browser Attacks
- Mediafile Attacks
- Bluetooth Attacks
- Mobile Devices als Client im Netz

Exploit Frameworks:

- Metasploit
- CORE Impact

- CANVAS
- BEEF

Hacking Databases:

- MS SQL Server
- Oracle
- My SQL

Social Engineering:

- The Human Factor
- Exploit the weakest Link
- Fear, Uncertainty and Doubt
- Role Playing

Hacking Web Server:

- Unterschiede Apache, IIS
- Web Scanner
- Attack Proxies
- Browser Plugins
- SQL Injection
- Cross-Site Scripting

Hacking Networks:

- Layer 2-Angriffe
- SNMP
- Authentifizierung
- Konfiguration
- NAC
- Wireless Attacks
- VPN Attacks

Termine und Orte: 19 März 2019 – Nr.: 5199

Berlin

12 Aug - 16 Aug 2019

Stuttgart

25 Nov - 29 Nov 2019

integrata Cegos Group | inspire qualify change

SECURE PROGRAMMING FOUNDATION

Dauer: 2 Tage

Durchführungsart: Lehrgang

Zielgruppe: Anwendungsentwickler, Entwickler, Programmierer, Webentwickler, IT-Sicherheitsbeauftrage, Softwarearchitekten.

Voraussetzungen: Kenntnisse in den Bereichen Webtechniken, Webentwicklung, Netzwerktechniken und Datenbanken sind von Vorteil, aber keine Voraussetzung.

Nr.: 5215
Preis: 1.190,00 € (netto) / 1.416,10 € inkl. 19% MwSt.

Schulungsmethode: Demonstrationen, Praktikum am System, Übungen, Vortrag.

Internetkriminalität, Datenlecks und Informationssicherheit erhalten in den Nachrichten mehr Beachtung. Regierungen und Firmen investieren mehr und mehr Ressourcen in diesen Bereichen.

Das Problem dabei ist, dass meist ein reaktiver, statt einem präventiven Ansatz verfolgt wird.

Der Schlüssel der Softwareerstellung ist die Weiterbildung. Wenn ein Programmierer die Sicherheit seiner zu erstellenden Software nicht kennt, sind alle restlichen Investitionen in den Entwicklungsprozess nutzlos.

Das EXIN Secure Programming Foundation Examen testet das Wissen der Kandidaten im Hinblick auf die Grundsätze sicherer Programmierung. Dabei wird auf alle gängigen Probleme eingegangen: Authentifizierung und Sitzungsverwaltung; Behandeln von Benutzereingaben; Autorisierung; Konfiguration, Fehlerbehandlung und Protokollierung; Kryptographie; Sichere Softwareentwicklung.

Das Seminar ist gedacht für Programmierer und Softwareentwickler, die ein Interesse daran haben sichere (Web-)Anwendungen zu entwickeln und für Auditoren, die mit Framework Secure Software arbeiten werden.

Programm

Verständnis für sicheres Programmieren:

- Sicherheitsbewusstsein
- Grundsätze
- STRIDE Bedrohungsmodell
- Websicherheit

Authentifizierung und Sitzungsverwaltung:

- Passwörter
- Sitzungsverwaltung
- Cross-Site-Request-Forgery (CSRF/XSRF)

Benutzereingaben behandeln:

- Injection Angriffe
- Eingabe Validierung
- Buffer Overflows
- Cross-Site-Scripting (XSS)

Autorisierung:

- Autorisierung
- Session Poisoning
- Race Conditions

Konfiguration, Fehlerbehandlung und Protokollierung:

- Komponenten von Drittanbietern
- Konfiguration und Abhärtung
- Datenlecks
- Fehlerbehandlung und Protokollierung
- Denial of Service (DoS)

Kryptographie:

- Kerckhoff's Prinzip
- Schlüsselverwaltung
- Zufälligkeit
- Asymmetrische Kryptographie
- SSL/HTTPS

Sichere Softwareentwicklung:

- Sicherheitsanforderungen
- Sicheres Design
- Sicherer Code
- Testen der Sicherheit

Hinweis

Am Ende des zweiten Seminartags findet das EXIN Examen für Secure Programming Foundation statt. Die Examensgebühr in Höhe von EUR 200,- zzgl. gesetzlicher MwSt. ist im Seminarpreis nicht enthalten und wird gesondert in Rechnung gestellt.

Multiple-Choice-Prüfung mit 40 Fragen, welche in 60 Minuten beantwortet werden müssen. Weitere Hilfsmittel sind nicht gestattet. 26 von 40 der EXIN Secure Programming Foundation Prüfungsfragen müssen richtig beantwortet sein, um das Zertifikat zu erhalten.

Das Seminar wird von akkreditierten EXIN Secure Programming Foundation Trainern durchgeführt.

Termine und Orte: 19 März 2019 – Nr.: 5215

München

23 Mai - 24 Mai 2019

Hamburg

16 Sep - 16 Sep 2019

Stuttgart

11 Nov - 12 Nov 2019

Online Anmeldung:
Kundenservice | Tel. 0711 62010 100 | Fax: 0711 62010 267 | seminaranmeldung@integrata.de
URL: https://www.integrata.de/5215

integrata Cegos Group | inspire qualify change

ETHICAL HACKING FOUNDATION

Dauer: 3 Tage

Durchführungsart: Lehrgang

Zielgruppe: Der Ethical Hacking Foundation Kurs richtet sich Sicherheitsbeauftragte, Netzwerkarchitekten, Netzwerkadministratoren, Sicherheits-Auditoren, Sicherheitsexperten, Programmierer und Netzwerk-Experten.

Voraussetzungen: Grundkenntnisse in Linux und Computernetze erforderlich.

Nr.: 5216
Preis: 1.190,00 € (netto) / 1.416,10 € inkl. 19% MwSt.

Schulungsmethode: Unsere praxiserfahrenen Trainer erläutern Ihnen die theoretischen Grundlagen und demonstrieren Beispiele aus dem Bereich des Hacking. Das vermittelte Wissen wenden Sie anhand von praktischen Übungen direkt am Rechner an.

In diesem Seminar lernen Sie die notwendigen Informationen zu erheben und zu analysieren, um das Sicherheitsniveau eines Systems oder eines Netzwerks zu bestimmen und Maßnahmen zur Sicherung einzuleiten. Zudem erwerben Sie das notwendige Wissen, um das Examen zum Ethical Hacking Foundation EXIN zu bestehen.

Nach dem Seminar haben die Teilnehmer Kenntnisse über folgende Themen gewonnen:

- Gewinnung von Informationen
- Das Arbeiten mit Penetrationstests Software
- Die Suche nach möglichen Schwachstellen und Behebung der Schwachstellen
- Penetrationstests auf Web-Anwendungen
- Aufdeckung von Schwachstellen in Netzwerken

EXIN

Programm

Agenda:

- Einführung in Ethical Hacking
- Einführung in Kali Linux
- Metasploit
- Informationsbeschaffung
- Aufdecken von Schwachstellen
- Netzwerk Traffic
- Web Application Testing
- Wireless-Angriffe

Hinweis

Am letzten Seminartag erfolgt die Ethical Hacking Foundation Prüfungsvorbereitung mit einem Musterexamen. Am Nachmittag findet die Prüfung für die offizielle Zertifizierung zum Ethical Hacking Foundation EXIN statt. Die Prüfungsgebühr in Höhe von derzeit EUR 200,- zzgl. gesetzlicher MwSt. ist im Seminarpreis nicht enthalten und wird gesondert in Rechnung gestellt.

Das Seminar wird von akkreditierten Ethical Hacking Foundation Trainern durchgeführt.

Termine und Orte: 19 März 2019 – Nr.: 5216

Hamburg

24 Jun - 26 Jun 2019

Frankfurt

19 Aug - 21 Aug 2019

Berlin

11 Nov - 13 Nov 2019

integrata Cegos Group | inspire qualify change

MOBILE SECURITY

Dauer: 2 Tage

Durchführungsart: Präsenztraining

Zielgruppe: IT-Leiter, Administratoren, Sicherheitsbeauftragte, Projektverantwortliche.

Voraussetzungen: Es werden keine besonderen Kenntnisse vorausgesetzt.

Nr.: 5313
Preis: 1.190,00 € (netto) / 1.416,10 € inkl. 19% MwSt.

Schulungsmethode: Vortrag, Demonstrationen, Praktikum am System.

Das Seminar behandelt Security-Aspekte beim Einsatz mobiler Endgeräte im Unternehmen. Es werden die spezifischen Risiken von Smart Phones und Tablets ebenso behandelt, wie die Möglichkeiten zur sicheren Integration und die Selektion geeigneter Maßnahmen

Programm

Grundlagen:
Definition - Besonderheiten - Bedrohungen und Schwachstellen - Risiken

Architektur und Sicherheitsfunktionen, spezifische Schwachstellen:

Apple - iOS - Android - Windows Phone 8 - Blackberry

Spezifische Schwachstellen:

Jailbreak - Mods - Vulnerabilities

Schutz mobiler Systeme:

Integrierte Sicherheits-Mechanismen - Verschlüsselung - App Überprüfung und Freigabe - Patch Management - Acceptable Use Policy

Management und Integration:

MS Exchange Active Sync - Zertifikate - VPN Unterstützung - Groupware - Management Lösungen - Spezifische Management Schnittstellen - Remote Wipe - Alternative Ansätze (Container, App, Verschlüsselung) - Herausforderung bei der Integration (iTunes und andere Client Software im Unternehmen)

BYOD - Bring your own Device:

Private Geräte und private Nutzung von Firmengeräten - Herausforderungen - Richtlinien

Termine und Orte: 19 März 2019 – Nr.: 5313

Frankfurt

25 Mrz - 26 Mrz 2019 Garantietermin

Hamburg

12 Jun - 13 Jun 2019

München

30 Sep - 01 Okt 2019