



TECHNISCHE AKADEMIE
WUPPERTAL E.V.

Network-Security-Manager (TAW)

Zertifikats-Lehrgang mit Präsenzphasen und Lehrbriefen

■ Beratung und Information

Dipl.-Oec. Friedrich W. Heffels
Tel.: 0202-7495-203
Fax: 0202-7495-333
E-Mail: friedrich.heffels@taw.de

Kerstin Doege
Tel.: 0202-7495-301
Fax: 0202-7495-333
E-Mail: kerstin.doege@taw.de



TECHNISCHE AKADEMIE
WUPPERTAL E.V.

■ Teilnehmerkreis

- Administratoren und Mitarbeiter, die für Planung, Installation, Betrieb und Betreuung interner EDV- und Kommunikationsnetze verantwortlich sind
- Netzwerk- und Systemtechniker, die eine Spezialisierung im Bereich Netzwerksicherheit benötigen
- Das Elektro- und informationstechnische Handwerk, wie z.B. Errichterfirmen im Bereich der Gebäude- und Videokommunikationstechnik sowie VoIP-TK-Anlagentechnik
- Inhaber, Betriebsleiter, Meister, Facharbeiter, Techniker, die bereits Grundlagenkenntnisse im Bereich Netzwerktechnik mitbringen bzw. entsprechende Berufserfahrung aufweisen oder vergleichbare Qualifikationen besitzen und darauf aufbauend einen fundierten Einstieg in die Netzwerksicherheit benötigen

■ Veranstaltungsdaten

- Veranstaltungsort **Wuppertal**,
Hubertusallee 18
Donnerstag, 18.11. bis
Samstag, 04.12.2010
Anmelde-Nr. 5146002410



TECHNISCHE AKADEMIE
WUPPERTAL E.V.

■ Referenten

- **Dipl.-Ing. Georg Jaanineh**,
Geschäftsführer der GELTEC, Gesellschaft für Entwicklung von
Labor- und Industrietechnik, Hattingen
- **Referententeam**

Network-Security-Manager (TAW)

■ Zum Lehrgang

Die Netzwerksicherheit stellt für die meisten Unternehmen ein nicht einschätzbares Risiko dar. Als Teil komplexer IT-Sicherheitskonzepte kommt der Netzwerksicherheit im Unternehmen eine zentrale Bedeutung zu. Das Datennetzwerk als Hauptschlagader des Unternehmens ist hierbei anfällig in Bezug auf interne und externe Sicherheitsrisiken, die es einzuschätzen und zu minimieren gilt.

Der Lehrgang zeigt auf, wie reale praktische Lösungen auszu-sehen haben. Er ist somit als praxisnahe Umsetzungshilfe sicherheitsrelevanter Fragen im Bereich Netzwerktechnik anzusehen.

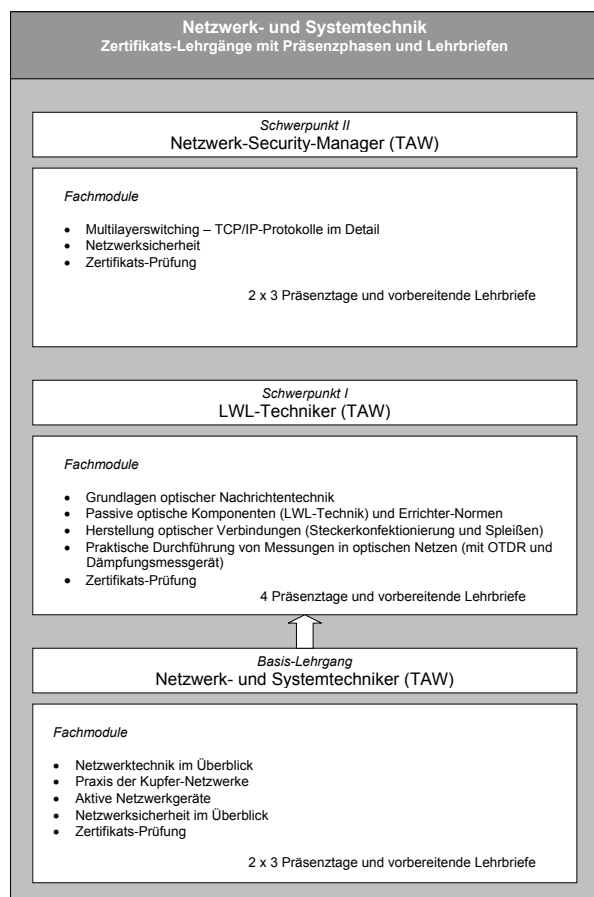
Der gesamte Lehrgang ist hierzu in zwei Fach-Module unterteilt:

Im ersten Fach-Modul wird zuerst ein tief gehender Einblick in sicherheitsrelevante Protokolle und Kommunikationsmechanismen der TCP/IP-Welt auf allen Netzwerkschichten geliefert. Hierbei kommen auch bekannte Analysetools zum Einsatz.

Danach wird das Multilayer Switching und Bridging in den Vordergrund gestellt. Selbstverständlich werden Themen wie Spanning Tree und Virtuelle lokale Netze (VLANs) auch in praktischen Szenarien trainiert.

Das zweite Fach-Modul geht dann auf typische Angriffsszenarien, TCP/IP-spezifische Gefährdungen ein. Darauf aufbauend werden Schutzinstrumente und Konzepte wie z.B. Firewall und DMZ unter die Lupe genommen. Das Thema VPN wird abschließend ebenfalls unter Sicherheitsaspekten betrachtet. Die Themen werden an praktischen Beispielen in Workshopform trainiert, sowie die Stärken und Schwächen der einzelnen Technologien herausgestellt.

Die TAW-Lehrgangsreihe zur Netzwerk- und Systemtechnik besteht aus drei Lehrgängen. Diese sind in sich abgeschlossen und einzeln buchbar, sie ergänzen sich aber thematisch.



■ Inhalte

1. Multilayerswitching – TCP/IP-Protokolle im Detail

- TCP/IP-Welt im Überblick
 - ISO/OSI-Referenzmodell
 - Netzwerkschichten und Kapselung der Daten
 - Sicherungsprotokoll Ethernet (Schicht 2)
- Vermittlungsprotokolle (Schicht 3)
 - Internet Protocol (IPv4)
 - Internet Protocol (IPv6)
 - Address Resolution Protocol (ARP)
 - Reverse Address Resolution Protocol (RARP)
- Transportprotokolle (Schicht 4)
 - Port-Nummern
 - User Datagram Protocol (UDP)
 - Transmission Control Protocol (TCP)
 - Internet Control Message Protocol (ICMP) für IPv4
 - Internet Control Message Protocol für IPv6 (ICMPv6)
- Anwendungsorientierte Protokolle (Auszug)
 - Dateitransfer: File Transfer Protocol (FTP)
 - Fernzugriff: Teletype Network (TELNET)
 - Netzwerkmanagement: Simple Network Management Protocol (SNMP)
 - E-Mail: Simple Mail Transfer Protocol (SMTP), Post Office Protocol, Version 3 (POP3), Internet Message Access Protocol, Version 4 (IMAP4)
 - Namensdienst: Domain Name System (DNS)
 - Dynamic Host Configuration Protocol (DHCP)
 - Hypertext Transfer Protocol (HTTP)
 - Windows-Anwendungsprogrammierschnittstellen (APIs)
- Multilayer Switching und Bridging
 - Layer 2-Switching: Funktionsprinzip, Switching Mode, Begrenzung des Broadcast- und Multicast-Verkehrs, Filtering, Flow Control, Link Aggregation, Remote Bridging, Translational Bridging
 - Layer 3-Switching
 - Layer 4-Switching
- Spanning Tree
 - Spanning Tree Protocol (STP)
 - Rapid Spanning Tree Protocol (RSTP)
 - Multiple Spanning Tree Protocol (MSTP)
- Virtuelle lokale Netze (VLANs)
 - VLAN-Typen
 - VLAN-Trunk-Protokolle
 - Der Standard IEEE 802.1Q: Trunking, Tagging, Die PVID (Port VLAN ID)
 - Anwendungsbeispiele: Ein Server für zwei VLANs, Heterogene Switchlandschaft
 - Lastverteilung
 - GVRP (GARP VLAN Registration Protocol)

2. Netzwerksicherheit

- Einführung
 - Die IT-Sicherheitsstruktur – die Gefährdungsgruppen
 - Die gefährdeten Geschäftsprozesse
 - Netzwerksicherheit (Verfügbarkeit, Vertraulichkeit u. Integrität)
 - Die Gesetzeslage
- Angriffsszenarien
 - Malware (Viren, Würmer und Trojaner)
 - Angriffe auf Netzwerk- und Protokollebene (Spionage, Täuschung und Tarnung, Überlastung)
 - Angriffe auf Protokollebene
- TCP/IP-spezifische Gefährdungen
 - Spionage, Maskerade, Eindringen
 - Denial of Service (DoS)
 - Weitere bekannt gewordene Angriffsvarianten
 - Empfehlungen für ICMP-Einstellungen in der Firewall
 - Port-Scanner
- Schutz-Instrumente und –Konzepte
 - Antivirenprogramme
 - Firewall: Firewall-Architekturen: Paketfilter (statisch und dynamisch), Anwendungsfilter (Proxy), Demilitarisierte Zone (DMZ), Konzeptvergleich, Personal Firewalls



- Intrusion Detection/Prevention Systeme (IDS/IPS): Aufgabe und Wirkungsweise, Grundkomponenten von IDS, das Erkennen sicherheitsrelevanter Ereignisse
- Testmöglichkeiten: Security-Test, Performance-Test
- Anforderungen an die Schutzkomponenten: Allgemeine und besondere Anforderungen an eine Firewall, Anforderungen an einen Paket-Filter, Anforderungen an ein Application-Gateway (Proxy)
- Virtuelle Private Netze (VPN)
 - VPN-Konzepte: Hardware-Lösungen (VPN-Gateways), Software-Lösungen
 - VPN-Tunneling: Der VPN-Tunnel, VPN-Topologien,
 - VPN-Typen und deren Protokolle: Point-to-Point Protocol (PPP), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), IPSec (Internet Protocol Security), IPSec secured L2TP (L2Sec), SSL-VPN
 - Verschlüsselungsverfahren: Symmetrische und asymmetrische Verschlüsselung, PKI und Digitale Signatur, Details zum Private-Key-Verfahren, Details zum Public-Key-Verfahren, Details zum Hash-Verfahren
 - Schlüsselaustausch: Pre-Shared Key, Simple Key Management for Internet Protocols (SKIP), Internet Key Exchange (IKE)
- Weitere Sicherheitsaspekte
 - Sicherheitsphilosophie des Unternehmens: Sicherheitspolitik, der Mensch als Sicherheitsrisiko
 - Betriebssysteme
 - Authentifizierungsmechanismen: Standardverfahren, Biometrische Verfahren
 - Layer-2-Security mit IEEE 802.1X: Einführung, das Extensible Authentication Protokoll (EAP), wichtige Authentifizierungsverfahren

■ Präsenzphasen / Workshops

Workshopinhalte:

- Praxisbezogene Umsetzung und Vertiefung der in den vorbereitenden Lehrbriefen gelegten Grundlagen
- Diskussion und Erfahrungsaustausch
- Gruppenarbeit
- Praktische Übungen
- Erarbeitung konkreter Instrumente und Hilfsmittel zur Umsetzung in der Praxis

Für die praktischen Übungen können Sie Ihren eigenen PC/ Laptop mitbringen.

■ Ort/Termin/Gebühr Wuppertal, Hubertusallee 18

Workshop 1
Donnerstag, 18.11.2010 bis
Samstag, 20.11.2010

Workshop 2
Donnerstag, 02.12.2010 bis
Samstag, 04.12.2010

Dauer der Präsenzphasen:
donnerstags, 09.00 - ca. 17.30 Uhr
freitags, 09.00 - ca. 17.30 Uhr
samstags, 09.00 - ca. 14.00 Uhr

Anmelde-Nr. 5146002410 / Gebühr: € 1.940,-

(für den gesamten Lehrgang, mehrwertsteuerfrei, einschließlich Pausengetränken und Mittagessen während der Präsenzphasen)

■ Lehr-/Lernmethoden

Der **berufsbegleitende Zertifikats-Lehrgang mit Präsenzphasen und Lehrbriefen** ist auf die besonderen Belange Berufstätiger ausgerichtet.

Präsenzphasen

Zwei Präsenzphasen mit Workshop-Charakter, die durch ein Selbststudium vorbereitet werden, bilden den Mittelpunkt des Zertifikats-Lehrgangs und dienen der praxisorientierten Umsetzung und Vertiefung der in den vorbereitenden Selbstlernmaterialien gelegten Grundlagen. Die Bearbeitung konkreter Praxisprobleme, die Diskussion und der Erfahrungsaustausch der Teilnehmer stellen den unmittelbaren Bezug zur beruflichen Praxis her. Außerdem können offene Fragen oder konkrete Problemstellungen hier gemeinsam bearbeitet werden.

Zusätzliche Teilnehmerunterlagen unterstützen die schnelle und effektive Umsetzung in der Praxis.

Methoden:

Vortrag, Diskussion, Erfahrungsaustausch, Gruppenarbeit, praktische Übungen.

Lehrbriefe / Selbstlernmaterialien

Lehrbriefe und Selbstlernmaterialien geben einen Überblick über das jeweilige Themengebiet. So ist eine Vorbereitung auf die Präsenzphasen möglich, die bei freier Zeiteinteilung individuell gestaltet werden kann.

Ein wesentliches Ziel ist es, mit Hilfe des Ansatzes eines vorbereitenden Selbststudiums, das Problem eines heterogenen Teilnehmerfeldes mit unterschiedlichen Vorkenntnissen und beruflichen Erfahrungen zu mindern und für ein zunächst einheitliches Ausgangswissen zu sorgen. Durch diese vorbereitende Strukturierung soll die Effizienz und Effektivität der Präsenz-Workshops erhöht werden. Die Lehrbriefe dienen ebenfalls als Nachschlagewerk während der gesamten Maßnahme und darüber hinaus. Übungsaufgaben ermöglichen eine Selbstkontrolle des Lernfortschritts

Die Bearbeitungszeit für die Lehrbriefe ist individuell verschieden und abhängig von den jeweiligen fachbezogenen Vorkenntnissen der Teilnehmer. Pro Workshop ist eine Bearbeitungszeit von ca. 10 U.-Stunden à 45 Min. vorgesehen.

■ Teilnahmebescheinigung / Zertifikat

Nach erfolgreich abgelegter Zertifikatsprüfung erhalten die Teilnehmer das Zertifikat „**Network-Security-Manager (TAW)**“



■ Übernachtung / Unser Service

Für Wuppertal: Wir bieten Übernachtungsmöglichkeiten in unserem Gästehaus direkt in der Akademie. Nähere Informationen finden Sie im Internet unter www.taw.de/uebernachtung. Bitte reservieren Sie frühzeitig schriftlich. Sollte unser Gästehaus ausgebucht sein, leiten wir Ihren Übernachtungswunsch an Wuppertaler Hotels weiter.

TAW-Bahnticket: Reisen Sie mit der Deutschen Bahn AG zum Sonderpreis zu Ihrem TAW-Seminar. Weitere Infos erhalten Sie unter www.taw.de/bahnticket.

■ Geschäftsbedingungen

Anmeldung bitte schriftlich mit folgenden Angaben: Anmelde-nummer / Lehrgangstitel, Teilnehmer-Name/-Vorname, Titel/Stellung im Betrieb, Rechnungsanschrift (Firma / Behörde / Abteilung / Anschrift / Telefon / Telefax / E-Mail). Eine frühzeitige Anmeldung wird empfohlen.

Die Teilnehmergebühr ist spätestens bis zum Beginn der Veranstaltung fällig, aber nicht vor Rechnungserhalt.

Muss eine Veranstaltung aus unvorhergesehenen Gründen kurzfristig abgesagt werden, erfolgt sofortige Benachrichtigung. In diesem Falle besteht für die TAW nur die Verpflichtung zur Rück-erstattung der evtl. bereits gezahlten Teilnehmergebühr. In jedem Fall beschränkt sich die Haftung der TAW lediglich auf die Teilnehmergebühr.

In Ausnahmefällen behält sich die TAW den Wechsel von Dozenten und/oder Verschiebungen bzw. Änderungen im Programmablauf vor.

Abmeldungen müssen grundsätzlich schriftlich, spätestens vier Wochen vor Veranstaltungsbeginn erfolgen. Bei Abmeldungen, die weniger als vier Wochen vor Veranstaltungsbeginn bei uns eingehen und bei Fernbleiben ist die gesamte Teilnehmergebühr fällig. Maßgebend für die genannten Zeitpunkte ist der Post-eingangsstempel der TAW.

■ Innerbetriebliche Seminare

Für eine größere Gruppe von Mitarbeitern bieten wir Ihnen gerne ein gezieltes Weiterbildungsprogramm als „Seminar nach Maß“ an. Der bedarfsorientierte Zuschnitt auf Ihr Unternehmen bietet die Gewähr für schnelle und effektive Umsetzung in den betrieblichen Alltag. Zu allen unseren Seminarthemen können wir individuelle Veranstaltungen für Sie entwickeln und durchführen.

Rufen Sie uns an! Wir beraten Sie gern! Für eine größere Gruppe von Mitarbeitern bieten wir Ihnen gerne ein gezieltes Weiterbildungsprogramm als „Seminar nach Maß“ an. Der bedarfsorientierte Zuschnitt auf Ihr Unternehmen bietet die Gewähr für schnelle und effektive Umsetzung in den betrieblichen Alltag. Zu allen unseren Seminarthemen können wir individuelle Veranstaltungen für Sie entwickeln und durchführen.

Rufen Sie uns an! Wir beraten Sie gern!

■ Wir sind

Außeninstitut der RWTH Aachen,
Kontaktstudien-Institut der Bergischen Universität Wuppertal

■ Veranstaltungsvorschau

02.-18.09.	Wuppertal	Netzwerk- und Systemtechniker (TAW)
01.10.-06.11.	Wuppertal	Projektmanagement
06.-09.10.	Wuppertal	LWL-Techniker (TAW)
28.10.-07.05.	Wuppertal	Fachwirt/in Facility Management (GEFMA)
05.11.-22.01.	Wuppertal	Fachkraft für Gebäudewirtschaft (TAW)
12.11.-29.01.	Wuppertal	Betriebswirtschaftliches Know-how für (technische) Fach- und Führungskräfte
18.11.-11.12.	Wuppertal	Instandhaltungsmanager (TAW) für gebäudetechnische Anlagen
24.11.-11.12.	Wuppertal	Elektrofachkraft für festgelegte Tätigkeiten (EFFT)

Aktuelle Programme finden Sie unter www.taw.de.



FAX-ANTWORT
AN 0202 / 74 95 - 333

■ Verbindliche Anmeldung / Faxvorlage

- Lehrgang** „Network-Security-Manager (TAW)“,
Wuppertal, Anmelde-nummer 5146002410,
November 2010, Gebühr: € 1.940,-

Name des Teilnehmers

Titel / Vorname des Teilnehmers

Stellung des Teilnehmers im Betrieb

Telefon / Fax / E-Mail

Zimmerreservierung Ja Nein

Anreise _____.____.____ **Abreise** _____.____.____

Rechnungs-Anschrift:

Firma / Behörde

Abteilung

Straße / Hausnummer

PLZ / Ort

Telefon / Fax / E-Mail

Die oben genannten Teilnahmebedingungen mit der Verpflichtung zur Teilnahme bzw. Zahlung der Teilnahmegebühr nach Rechnungsstellung werden hiermit akzeptiert.

Mit der Verarbeitung personenbezogener Daten zur Durchführung der Veranstaltung und zur Information über aktuelle Angebote der TAW bin ich einverstanden.

Ort / Datum

Unterschrift