157 Security im Netzwerk

K2010 Release 2.1

Inhaltliche Richtziele der Modulprüfung:

- ❑ Aktuelle Risiken und Sicherheitsprobleme im IT-Umfeld eines KMU kennen.
- ❑ Netzwerken unter Berücksichtigung sicherheitsrelevanter Themen planen.
- ❑ Netzwerkgeräte zur Optimierung der Sicherheit konfigurieren.
- ❑ Massnahmen zur Gewährleistung der Datenintegrität, -verfügbarkeit und vertraulichkeit planen und umsetzen.

Empfohlene Vorkenntnisse:

Module 144, 145

		Tax:
1	**Grundlagen der IT und Informationssicherheit**	
1.1	**Kennt die Grundlagen der Informationssicherheit.**	
1.1.1	Zweck eines IT-Sicherheitsmanagement erläutern	2
1.1.2	Schutzanforderungen nach Vertraulichkeit, Integrität und Verfügbarkeit kategorisieren	2
1.1.3	die wichtigsten Methoden (Gefährdungsanalyse, Bedrohungsanalyse, Schwachstellenanalyse, Risikoanalyse) zur Einschätzung einer Situation verstehen	2
1.1.4	Grobstruktur der Sicherheitsstandards (ISO27001/ISO27002, BSI-Grundschutzkataloge, InfoSurance 10-Punkte-Katalog) kennen	2
1.1.5	Kriterien der Datenklassifikation erläutern	2
1.1.6	Inhalt und Bedeutung einer Sicherheitspolicy/ eines Sicherheitsleitbildes kennen	2
1.1.7	möglichen Aufbau einer Sicherheitsorganisation kennen	2
1.1.8	Funktionen und Pflichtenheft eines Sicherheitsbeauftragten kennen	1
1.2	**Kennt die rechtlichen Aspekte der Informationssicherheit.**	
1.2.1	die für einen Systemadministrator relevanten Inhalte folgender Gesetze (ZGB, OR, DSG, StGB und Urheberrecht) kennen	1
1.3	**Kann organisatorische Massnahmen zur Informationssicherheit umsetzen.**	
1.3.1	Bedeutung der Sensibilisierung und Schulung von Benutzern über den sicheren Umgang mit Informationen verstehen	2
1.3.2	Regeln für Umgang mit Passwörtern kennen und eine Weisung an die Benutzer über die Generierung und Verwendung von sicheren Passwörtern erstellen	3
1.3.3	Problematik der Datenlagerung auf mobilen Geräten verstehen und Weisungen an die Benutzer über den sicheren Umgang mit mobilen Geräten erstellen	3

157 Security im Netzwerk

			Tax:
2	**Risiken innerhalb eines Netzwerkes**		
2.1	**Kennt relevante Angriffsmethoden in vernetzten Umgebungen.**		
	2.1.1	Angriffstechniken (wie Man-in-the-middle-, DOS-, DDOS-, Back Door -, Spoofing-, Replay-, BruteForce-, Dictionary Attacks und SQL-Injection) verstehen und mit entsprechenden Tools nachvollziehen	2
	2.1.2	strukturierte Vorgehensweise (Footprinting, Scanning, Enumeration) eines Angriffs verstehen und mit entsprechenden Tools nachvollziehen	3
	2.1.3	relevante Begriffe wie Rootkits, Exploits, Sniffer, Wardialing und Wardriving erläutern	2
	2.1.4	Schwachstellen von Web-Add-ins (Active X, Buffer Overflows, Cookies, Cross-Site Scripting (XSS), Input Validation, Java Applets, JavaScripts, Popups Sign Applets) erläutern	2
	2.1.5	Vorgehensweise bei einem Social Engineering Angriff verstehen und erläutern	2
2.2	**Kennt die Sicherheitsrisiken des TCP/IP Protokolls.**		
	2.2.1	Risiken der verschiedenen TCP/IP-Protokolle (http, ftp, Telnet, POP3/POP4, SMTP, TCP/UDP, IP, ICMP, ARP, IGMP, PPP, SNMP) kennen	1
	2.2.2	Funktionsweise von TCP/IP Drei-Weg-Handshake verstehen	2
	2.2.3	IP Attacken (Sniffing, Port Scanning, TCP Syn or TCP Flood Attack, Sequence Number-Attack, TCP/IP Hijacking) kennen	1
	2.2.4	UDP Attacken (ICMP Attacken, Smurf Attacken, ICMP Tunneling) kennen	1

			Tax:
3	**Malware**		
3.1	**Kennt wichtige Malwaretypen und ihre Mechanismen.**		
	3.1.1	verschiedene Malwarekategorien (Viren, Trojaner, Spam, Phishing, Spyware) kennen	1
	3.1.2	verschiedene Virenarten wie Bootsektorviren, Dateiviren, Makroviren, Skriptviren, Slackviren, selbstverschlüsselnde Viren, polymorphe Viren, Stealthviren, Würmer, Hybridviren, Hoax und deren Wirkungsweise verstehen	2
	3.1.3	Vorgehensweise und Problematik von Trojanern verstehen	2
3.2	**Kann Massnahmen zum Schutz vor Malware im Netzwerk umsetzen, installieren und konfigurieren.**		
	3.2.1	Früherkennung durch Firewalls auf Application-Level erläutern	2
	3.2.2	Lösungsmöglichkeiten bei der Malwarebekämpfung aufzeigen	3
	3.2.3	lokale und zentral gesteuerte Software zur Bekämpfung von Malware installieren und konfigurieren	3

157 Security im Netzwerk

		Tax:
4	**Massnahmen zur Erhöhung der Sicherheit im Netz**	
4.1	**Kennt die Funktionsweise und Möglichkeiten von Intrusion Detection Systemen.**	
4.1.1	die Begriffe Signature-based detection IDS und Anomaly detection IDS, Host-Based IDS, Network Based IDS und Honey Pots erklären	2
4.1.2	die Schritte eines Incident (Identifikation, Analyse, Massnahmen, Based IDS, Network Based IDS und Honey Pots erläutern	2
4.2	**Kann IP-Konzepte unter Berücksichtigung von Sicherheitsaspekten planen und umsetzen.**	
4.2.1	das Konzept von NAT (Network Address Translation) und PAT (Port Address Translation) erläutern	2
4.2.2	NAT/PAT den entsprechenden Netzwerk-Zonen zuweisen	3
4.2.3	IP-Netzwerke (inkl. Subnetting) konzipieren und umsetzen	3
4.2.4	VLAN konzeptionell planen	3
4.2.5	mittels statischem Routing Zugriff auf andere Netze steuern	3
4.2.6	dynamische Routing-Protokolle wie RIP, BGP und OSPF kennen	1
4.3	**Kann grundlegende Firewallfunktionen einrichten.**	
4.3.1	unterschiedliche Firewall-Typen (Packet Filter, Proxy Firewall, Stateful Inspection Firewall) und ihre Funktionsweise erläutern	2
4.3.2	Firewallregeln planen und einrichten	3
4.3.3	erweiterte Firewall-Funktionen (URL-Content Filtering, SPAM Filtering, Antiviren-Gateway) und ihre Einbindung im Zonenkonzept verstehen	2
4.4	**Kennt kryptographische Verfahren und kann diese einsetzen.**	
4.4.1	relevante Begriffe wie Hashing, symmetrische Verschlüsselung (AES-256, TripleDes, CAST, Rivests Cipher, Blowfish), asymmetrische Verschlüsselung (RSA, Diffie Hellman, Elliptische Kurven, El Gamal) verstehen	2
4.4.2	Grundlagen einer Public-Key-Infrastruktur verstehen	2
4.4.3	Funktionsweise des Keymanagement im Zusammenhang mit Public-Key-Infrastruktur erläutern	2
4.4.4	Inhalt und Aufbau eines Zertifikats kennen	1
4.4.5	Funktionsweise von digitalen Signaturen und Authentifizierung erläutern	2
4.4.6	kryptographische Protokolle (Public-Key-Infrastrukture X.509/Public-Key, X.509, SSL/TLS, Certificate Management Protocol (CMP), S/MIME, SET, SSH, HTTPS, IPSEC, WTLS) und ihre Einsatzgebiete kennen	1
4.4.7	IPSec mittels Global Policies konfigurieren und anwenden	3
4.4.8	gemäss Vorgaben eine IPSec Regel erstellen	3
4.4.9	Dateiverschlüsselung mittel EFS durchführen	3

	4.4.10	Harddiskverschlüsselung mit spezifiziertem Tool durchführen	3
4.5	**Kennt verschiedene Authentifizierungsmethoden.**		
	4.5.1	Einsatzgebiete von RADIUS, TACACS/TACACS+ erläutern	2
	4.5.2	Funktionsweise des Kerberos-Protokolls verstehen	2
4.6	**Kann sichere Verbindungen über öffentliche Netze einrichten und Daten verschlüsselt übertragen.**		
	4.6.1	Protokolle PPTP, L2TP, SSL, TLS, SSH, IPSec, S/MIME, SFTP verstehen	2
	4.6.2	Site-to-Site-Verbindungen (preshared key) mittels VPN einrichten	3
	4.6.3	sichere Emailübertragung mit S/MIME verstehen	2
	4.6.4	Zertifikat-gestützte VPN-Verbindug einrichten	3
	4.6.5	SSL und Server-Authentifizierungsmethoden (inkl. Web-Server-Zertifikat) einrichten	3
4.7	**Kann einen Wireless Access Point sicher konfigurieren.**		
	4.7.1	aktuelle Wireless Standards kennen	1
	4.7.2	Risiken im Zusammenhang mit Wireless-Verbindungen erläutern	2
	4.7.3	Wireless Access Point sicher konfigurieren	3
			Tax:
5	**Massnahmen proaktiver Sicherheit**		
5.1	**Kann Client- und Server-Systeme härten.**		
	5.1.1	nach Vorgaben Applikationen und Dienste (Web Server, E-Mail Server, FTP Server, DNS Server, NNTP Server, File und Print Server, DHCP Server) härten	3
	5.1.2	IT System mit gegebener Sicherheitsvorlage analysieren	3
	5.1.3	Sicherheitsvorlage importieren, anpassen und verteilen	3
5.2	**Kann Risiken im Browser mit entsprechenden Einstellungen begegnen.**		
	5.2.1	die verschiedenen Zonen im Browser, den Sicherheitsanforderungen entsprechend, konfigurieren	3
	5.2.2	Sicherheitseinstellungen im Browser anforderungsgemäss lokal oder mittels Benutzerrichtlinien konfigurieren	3
5.3	**Kann Massnahmen zur Datensicherheit und Datenverfügbarkeit planen und umsetzen. Kann Hardware und Tools zur Verhinderung von Datenverlust einsetzen und konfigurieren.**		
	5.3.1	relevante Begriffe wie System- und Datenverfügbarkeit, Ausfallsicherheit, Disaster Recovery, Onsite- und Offsite Backup erläutern	2
	5.3.2	wichtige zu sichernde Dateien und deren Bedeutung im Zusammenhang mit der Datensicherung kennen	2
	5.3.3	Backup Typen (Full Backup, Incremental Backup, Differential Backup) kennen	2

157 Security im Netzwerk

5.3.4	Sicherung nach dem Generationenprinzip planen	3
5.3.5	Datensicherung mittels geeigneter Tools ausführen und automatisieren	3
5.3.6	Vor- und Nachteile von Hardware- und Software-RAIDs kennen	3
5.3.7	Software RAID implementieren	3
5.3.8	Vorlage für Datensicherungsprotokoll erstellen	3
5.3.9	gewähltes Datensicherungsmodell dokumentieren	3
5.4	**Kennt die Möglichkeiten zur Verbesserung von Systemverfügbarkeit und Systemoptimierung durch Virtualisierung.**	
5.4.1	Einsatzgebiete und Möglichkeiten von virtualisierten Servern nennen	2
5.4.2	lizenzrechtliche Aspekte beim Einsatz in virtuellen Umgebungen kennen	2
5.4.3	Server- und Client-Installation mittels Imagingtools sichern und wiederherstellen	3
5.5	**Kennt die physikalischen Massnahmen zur Sicherung von IT-Systemen.**	
5.5.1	die wichtigsten baulichen Massnahmen (Zugangskontrollsysteme, Brand- und Wasserschutz) erläutern	2
5.5.2	Möglichkeiten zur Sicherung der Stromversorgung und ihre Einsatzgebiete erläutern	2

Empfohlene Unterrichtszeit (Lektionen): 60

- Diese Empfehlung ist als Richtwert zu verstehen. Sie beinhaltet keine Qualitätsaussage.
- Die Empfehlung muss dem Wissensstand und der Praxiserfahrung der Kandidaten angepasst werden.
- Der Unterricht erfolgt im Rahmen eines Weiterbildungslehrgangs.
- Zusätzlich ist mit einem wöchentlichen Aufwand 6-10 Stunden in Form von Selbststudium zu rechnen (Umsetzen von Erlerntem, eventuellem Einsatz von Lernvideos).
- Der Richtwert ist abhängig von den Möglichkeiten, das Erlernte in der Praxis anzuwenden.

Version	Datum	Bemerkung - Änderungsnachweis	
K2010 R2.1	15.02.2016	Version:	K2010 Release 2.1 (Korrekturen und 4.6.5 neu)
K2010 R2	18.07.2014	Version:	K2010 Release 2 (keine Änderung)
final 1.0	01.11.2009	Version:	Final 1.0, Ausgabedatum 31.1.2010