



## Modulidentifikation

Modulnummer	<b>233</b>	
Titel	<b>Netzwerke schützen und warten</b>	
Kompetenz	Integriert und konfiguriert eine Firewall, um den Schutz eines Netzwerkes zu gewährleisten. Führt gemäss Auftrag Wartungsarbeiten an einer Firewall durch und dokumentiert die ausgeführten Sicherheitsmassnahmen. .	
Handlungsziele	1.	Klärt die aktuellen Sicherheitsbedrohungen für eine vernetzte ICT-Infrastruktur ab.
	2.	Integriert eine physische Firewall gemäss Auftrag.
	3.	Erstellt einfache Firewall-Regeln (Portfilter).
	4.	Konfiguriert erweiterte Funktionen einer Firewall.
	5.	Nimmt VPN-Verbindungen in Betrieb.
	6.	Bindet Authentifizierungsdienste an eine Firewall an.
	7.	Führt Wartungsarbeiten an einer Firewall durch.
	8.	Konfiguriert ein gesichertes WLAN.
	9.	Dokumentiert die Sicherheitsmassnahmen nachvollziehbar und formal korrekt.
Kompetenzfeld	Security / Risk Management	
Objekt	Netzwerksicherheit in einem KMU	
Nachweis		
Lehrjahr	2	
Niveau		
Voraussetzungen		
Arbeitsaufwand	40	
Lektionen		
Anerkennung	EFZ	
Handlungskompetenzen	a2: Technische Anforderungen, IT-Sicherheit und Datenschutz eines einfachen GKM-Projektes überprüfen und in einem Pflichtenheft festhalten	
Gebäudeinformatiker/in	d1: Datennetze für Kommunikations- und Multimediasysteme einrichten und erweitern	
EFZ	d2: Komponenten von Kommunikations- und Multimediasystemen installieren	
	d3: Komponenten von Kommunikations- und Multimediasystemen konfigurieren	
	d7: Datennetze/Netzwerke messen, analysieren und Störungen beheben	
	f4: GKM-Systeme warten und betreuen	



## Handlungsnotwendige Kenntnisse

Handlungsnotwendige Kenntnisse beschreiben Wissen, das die kompetente Ausführung der Handlungen eines Moduls unterstützt. Diese Kenntnisse dienen der Orientierung und sind nicht abschliessend definiert. Die daraus folgende Konkretisierung der Lernziele und das Festlegen des Lernwegs für den Kompetenzerwerb sind Sache der Bildungsanbieter.

Modulnummer			233
Titel			Netzwerke schützen und warten
Kompetenzfeld			Security / Risk Management
Handlungsziele und handlungsnotwendige Kenntnisse	1	1.1	Kennt die gängigen Sicherheitskriterien von Informationssystemen, verschiedenen Bedrohungsstufen sowie relevante Sicherheitsaspekte (z.B. juristisch, organisatorisch, technisch, physisch).
		1.2	Kennt verschiedene Verfahren zur sicheren Datenübertragung (z. B. asymmetrische und symmetrische Verschlüsselung).
		1.3	Kennt Methoden zur Aufteilung eines Netzwerkes in Sicherheitszonen.
		1.4	Kennt Vorgehensweisen, um die technische Sicherheit eines Netzwerkes zu überprüfen.
	2	2.1	Kennt die Zugriffsmöglichkeiten auf eine Firewall und ihre Grundkonfigurationen (z.B. Schnittstellen, IP-Adressierung).
		2.2	Kennt die Funktionen der erweiterten Netzwerkeinstellungen (z. B. Gateway, Routing, VLAN, DHCP).
	3	3.1	Kennt die Vorgehensweise einer Firewall bei Portfilterung und das Prinzip von Stateful Packet Inspection (SPI).
		3.2	Kennt die Eigenschaften der relevanten Netzwerkprotokolle und deren UDP/TCP-Ports.
		3.3	Kennt eine Vorgehensweise für die Erstellung von Regeln, um diese richtungsbezogen zwischen den Sicherheitszonen einzusetzen.
		3.4	Kennt die Funktionsweise von NAT.
	4	4.1	Kennt erweiterte Funktionen (z. B. Antivirus, Webfilter, Applikationsfilter) einer Firewall.
		4.2	Kennt die Voraussetzungen der erweiterten Funktionen bei verschlüsselten Verbindungen.
	5	5.1	Kennt die Merkmale der verschiedenen VPN-Topologien (z.B. Site-to-Site, Client-to-Site).
		5.2	Kennt gebräuchliche Protokolle (z. B. IPSec, SSL) für VPN-Verbindungen.
		5.3	Kennt die nötigen Parameter zum Aufbau eines VPN-Tunnels.



Handlungsziele und handlungsnotwendige Kenntnisse	6	6.1	Kennt die Funktionsweise verschiedener Authentifizierungsmethoden (z. B. Lokal, RADIUS, LDAP, Zwei-Faktor-Authentifizierung).
		6.2	Kennt die Voraussetzungen, um einen Authentifizierungsdienst an eine Firewall anzubinden.
		6.3	Kennt Einstellungen, um Personen- und Gruppeninformationen in die Firewall einzubinden.
	7	7.1	Kennt die Vorgehensweise für Backup und Wiederherstellung einer Firewall-Konfiguration.
		7.2	Kennt die Methodik und Voraussetzungen eines Firewall-Updates.
		7.3	Kennt Darstellungsformen für die Dokumentation von Firewall-Regeln.
	8	8.1	Kennt unterschiedliche WLAN-Verschlüsselungs-Standards (z. B. WPA3).
		8.2	Kennt unterschiedliche WLAN-Authentifizierungsmethoden (z.B. PSK, IEEE 802.1x).
	9	9.1	Kennt die Bedeutung einer Dokumentation zur Sicherstellung und Nachvollziehbarkeit von Arbeitsergebnissen.
		9.2	Kennt die wichtigsten inhaltlichen und formalen Regeln, die bei der Dokumentation von Arbeitsergebnissen einzuhalten sind.