ICT Berufsbildung
Formation professionnelle
Formazione professionale

Modulidentifikation

Modulnummer	184
Titel	Netzwerksicherheit implementieren
Kompetenz	Implementiert, testet und überwacht den sicheren Netzbetrieb sowie den Netzzugang.
Handlungsziele	1. Untersucht ein bestehendes Netz auf Sicherheitslücken und Konfigurationsmängel mit Hilfe der Netzdokumentation und geeigneten technischen Mitteln.
	2. Erarbeitet ein Konzept für ein sicheres WAN, WLAN, LAN und geeigneten Remote Zugriff.
	3. Konfiguriert und dokumentiert die Sicherheitssysteme (z.B. Remote Access, Firewall, Proxy, WLAN) gemäss erarbeitetem Konzept.
	4. Erstellt ein Testkonzept zur Überprüfung der Funktionalität, Performance und Sicherheit des Netzes und führt diese Tests aus
	5. Überwacht Netzkomponenten und analysiert Log Einträge der Netzkomponenten.
	6. Lokalisiert und behebt Fehler der Netzkomponenten und deren Konfigurationen nach strukturiertem Vorgehen.
Kompetenzfeld	Network Management
Objekt	Kommunikationsnetz in einem KMU mit Internet Zugang
Nachweis	
Niveau	2. Lehrjahr
Voraussetzungen	117 Informatik- und Netzinfrastruktur für ein kleines Unternehmen realisieren
Arbeitsaufwand ca. h	40
Anerkennung	Eidg. Fähigkeitszeugnis

ICT Berufsbildung
Formation professionnelle
Formazione professionale

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	184
Titel	Netzwerksicherheit implementieren
Kompetenzfeld	Network Management

Handlungsziele und handlungsnotwendige Kenntnisse	1	1.1	Kennt die grundlegenden Elemente einer Netzwerkdokumentation.
		1.2	Kennt verschiedene Netzwerkkomponenten und deren Sicherheitseinstellungen.
		1.3	Kennt Tools zum Entdecken und Bewerten von Sicherheitsrisiken.
		1.4	Kennt technische Hilfsmittel zur Analyse (z.B. Portscanner, Sniffer) des Datenverkehrs im Netzwerk.
		1.5	Kennt aktuelle Exploits und deren Angriffswege auf das System.
	2	2.1	Kennt technische Verfahren für einen sicheren Remote Access (z.B. Protokolle, Standards, Technologien).
		2.2	Kennt aktuelle WLAN Standards und deren Sicherheitseinstellungen.
		2.3	Kennt Konzepte und Sicherheitssysteme und deren Konfigurationsmöglichkeiten (z.B. Härten, DMZ, Remote Access, Firewall, Proxy).
		2.4	Kennt die technischen Möglichkeiten und die Funktionsweise eines NIDS.
	3	3.1	Kennt Standardverfahren für die Härtung von Netzwerkkomponenten (z.B. Router, Firewall, Proxy).
		3.2	Kennt gängige Darstellungsarten und Symbole für Netzwerkplan und Netzwerkschemata.
	4	4.1	Kennt das Vorgehen und die Dokumentation zum Testen und Überprüfen der Funktionalität, Performance und Sicherheit des Netzes.
	5	5.1	Kennt das Verfahren, um aus den Logfiles sicherheitsrelevante Informationen zu erkennen.
		5.2	Kennt Monitoring-Tools und Protokolle (z.B. SNMP) zur Überwachung der Netzkomponenten.
	6	6.1	Kennt eine strukturierte Vorgehensweise (z.B. Vorgehen Ebene für Ebene) und Tools zur Lokalisierung und Identifizierung von Fehlern auf allen Ebenen des TCP-IP Schichten-Modells.