ICT Berufsbildung
Formation professionnelle
Formazione professionale

Modulidentifikation

Modulnummer	185
Titel	Sicherheitsmassnahmen für KMU IT analysieren & implementieren
Kompetenz	Untersucht, überprüft bei einem bestehenden Netzwerk Sicherheitsvorkehrungen und schlägt wenn nötig geeignete Massnahmen vor
Handlungen	1. Wendet bekannte Sicherheitsstandards systematisch an. 2. Untersucht vernetzte ICT-Infrastrukturen und deren Daten auf aktuelle Sicherheitsbedrohungen. 3. Unterstützt bei der Überprüfung der Wirksamkeit von vorhandene Sicherheitsvorkehrungen. 4. Analysiert Sicherheitsberichte und setzt vorgeschlagene Massnahmen um. 5. Unterstützt bei der Analyse von eingetretenen Sicherheitsverletzungen und deren Bewältigung.
Persönliche Kompetenzen	
Kompetenzfeld	ICT Sicherheit
Objekt	
Nachweis	
Niveau e-CF	4
Voraussetzungen	• 182 Systemsicherheit implementieren • 184 Netzwerksicherheit implementieren
Arbeitsaufwand ca. h	40
Anerkennung	Eidg. Fähigkeitszeugnis
Modulversion	1.0
MBK Release	

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			185
Titel			Sicherheitsmassnahmen für KMU IT analysieren & implementieren
Kompetenzfeld			ICT Sicherheit
Modulversion			1.0
MBK Release			
Handlungsziele und handlungsnotwendige Kenntnisse	1	1.1	Kennt mindestens einen aktuellen Sicherheitsstandard (z.B. BSI Grundschutzkompendium, ISO 27001, PCI-DSS, CIS, OSSTMM)
		1.2	Kennt das dem Sicherheitsstandard entsprechende Vorgehen für die Analyse, Umsetzung von Massnahmen und deren Kontrolle
	2	2.1	Kennt aktuelle Bedrohungen und Angriffsformen auf Systeme und Netzwerke, kann erläutern unter welchen Bedingungen diese für eine spezifische vernetzte ICT-Umgebung eine Bedrohung darstellen können.
		2.2	Kennt unterschiedliche Angriffsarten rund um den Betrieb von Web-Applikationen wie Cross-Site Scripting, SQL-, XML oder andere Injektionen, Dateianhänge, Session Hacking, Dateiüberläufe oder die Manipulation von Headerinformationen und kann erläutern, unter welchen Gegebenheiten diese in Bezug auf die System- und Netzwerkinfrastruktur eine Gefährdung darstellen können.
		2.3	Kennt aktuelle Verfahren und Mittel um Schwachstellen und Verwundbarkeiten aufzuspüren und leitet Massnahmen zu deren Behebung/Entschärfung ab.
	3	3.1	Kennt das Einsatzgebiet und das Zusammenspiel unterschiedlicher Sicherheitsmechanismen wie z.B. Firewalls, Authentifizierungssystemen, Dateiberechtigungen, VPN-Lösungen, Switches (VLAN, NAC), Proxyservern, Malware-Erkennung, IDS und kann deren Wirksamkeit erläutern.
		3.2	Kennt Mittel & Methoden zur Überprüfung der Wirksamkeit vorhandener Sicherheitsmassnahmen (z.B. AV-Tests, Security Scans, Penetration Testing etc.) sowie die Bedingungen einer erfolgreichen Überprüfung.
	4	4.1	Kennt den Aufbau eines Auditreports und kann darin beschriebenen Schwächen identifizieren, priorisieren und entsprechenden Massnahmen zuordnen.
	5	5.1	Kennt das dem Sicherheitsstandard entsprechende Vorgehen für die Analyse und Ergreifen von Massnahmen zur Gefahrenabwendung