ICT Berufsbildung
Formation professionnelle
Formazione professionale

Identification du module

Numéro du module	486
Titre	Implémenter des mesures de sécurité de réseau et de système
Compétences	Evaluer les menaces pesant sur la sécurité des données et infrastructures TIC en réseau ainsi que l'efficacité des mesures en place. Introduire si nécessaire des mesures spécifiques concernant le réseau et le système.
Actions	1. Analyser l'importance de menaces actuelles pour la sécurité d'une infrastructure TIC en réseau et de ses données. 2. Vérifier l'efficacité des mesures de sécurité en vigueur par rapport aux menaces actuelles. 3. Améliorer la sécurité des systèmes importants en choisissant et mettant en œuvre des mesures techniques adéquates et spécifiques aux systèmes concernés. 4. Améliorer la sécurité du réseau d'entreprise en choisissant et mettant en œuvre des mesures techniques adéquates et spécifiques au réseau concerné. 5. Recourir de manière ciblée à différents outils d'authentification, d'identification et de contrôle d'accès. 6. Assurer la confidentialité et l'authenticité des données transmises au moyen de méthodes cryptographiques adéquates. 7. Analyser les violations de sécurité, y réagir par des mesures permettant d'éviter d'autres violations et combler les lacunes qui en ont résulté. 8. Améliorer la prise de conscience pour les mesures de sécurité du système et du réseau par la formation et le perfectionnement du personnel.
Compétences personnelles	Faire preuve d'opiniâtreté et d'endurance dans l'identification de lacunes de sécurité ainsi que dans la mise en œuvre des mesures propres à les éviter.
Domaine de compétences	Gestion de la sécurité
Objet	Infrastructures TIC en réseau
Test	Mini-étude de cas comprenant 2-3 questions qui contrôlent plusieurs actions et d'une durée totale de 45-60 minutes.
Niveau	5
Prérequis	Mettre en service des composants réseaux (129) Exploiter et étendre un réseau (145) Réaliser la sécurité des réseaux (184) Assurer la sécurité de base des TIC (166)
Nombre de leçons	40
Reconnaissance	Informaticienne/Informaticien en technique des systèmes et réseaux TIC avec brevet fédéral
Version du module	V1.0
Version du TM	V5.0

© ICT-Formation professionnelle Suisse

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs nécessaires à l'exécution compétente des actions d'un module. Leur valeur est purement informative et leur définition non exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage incombent aux prestataires de formation.

Numéro du module	486
Titre	Implémenter des mesures de sécurité de réseau et de système
Domaine de compétences	Gestion de la sécurité
Version du module	V1.0
Version du TM	V5.0

Objectifs opérationnels et connaissances opérationnelles nécessaires	1	1.1	Connaître les menaces et possibilités d'attaque concernant les systèmes et les réseaux (déni de service*, man-in-the-middle, smurfing, replay, spoofing,* extension de droits, *phishing, pharming*, etc.) et pouvoir expliquer dans quelles circonstances elles peuvent représenter un danger pour l'infrastructure système et réseau.
		1.2	Connaître différents types d'attaque dans les applications (*cross-site scripting*, injections SQL, XML et autres, fichiers joints, *session hijacking*, débordements de fichiers, manipulation d'informations d'en-tête, etc.) et pouvoir expliquer dans quelles circonstances elles peuvent représenter un danger pour l'infrastructure système et réseau.
		1.3	Connaître différentes formes d'ingénierie sociale (*shoulder surfing*, *tailgating*, usurpation d'identité, *whaling*, *vishing*) et leur danger potentiel pour l'infrastructure système et réseau.
		1.4	Connaître les menaces actualisées en permanence que constituent les logiciels malveillants. Savoir en différencier les principaux types (*spam*, *adware*, *spyware*, virus, chevaux de Troie, *rootkits*, *botnets,* etc.) et pouvoir expliquer dans quelles circonstances elles peuvent représenter un danger pour l'infrastructure système et réseau.
		1.5	Connaître les principales menaces que constituent pour la sécurité sans fil les points d'accès interdits, les perturbations de fréquence, le *wardriving*, le piratage de Bluetooth et de WLAN ou l'interception du trafic de données. Pouvoir expliquer dans quelles circonstances elles peuvent représenter un danger pour l'infrastructure système et réseau.
	2	2.1	Connaître des outils de vérification de l'efficacité des mesures de sécurité en vigueur (tests antivirus, scans de sécurité, tests de pénétration, etc.) et les conditions à remplir pour une vérification réussie.
		2.2	Connaître les domaines d'utilisation et de fonction respectifs des pare-feu, NAT, VPN, commutateurs VLAN, serveurs proxy et appliances UTM et pouvoir en expliquer l'efficacité.
	3	3.1	Connaître des mesures de renforcement de systèmes (matériels, système d'exploitation, applications) comme la fermeture de ports non utilisés, la désactivation de services non utilisés, les mots de passe forts, la désactivation de comptes, la désactivation ou la désinstallation d'applications superflues ou encore la suppression de données obsolètes. Savoir en expliquer l'influence sur le niveau de sécurité constaté.
		3.2	Connaître des méthodes de mesure pour la surveillance des systèmes et de leur niveau de charge et savoir interpréter les protocoles de mesure.
	4	4.1	Connaître différents designs de réseaux récents permettant d'accroître la sécurité (sous-réseautage, DMZ, VLANs, NAC, routage, accès à distance, virtualisation, etc.) et savoir en expliquer l'influence sur le niveau de sécurité constaté.
		4.2	Connaître les utilisations possibles et les limites des systèmes IDS et IPS pour l'amélioration de la sécurité réseau ainsi que la fonction des réseaux leurres.

Connaissances opérationelles nécessaires

		4.3	Connaître différents principes d'administration permettant d'améliorer la sécurité réseau (management basé sur des rôles, règles de pare-feu, sécurité des ports, listes de contrôle d'accès, 802.1x, surveillance des événements).
		4.4	Connaître les principes d'exploitation sûre de réseaux sans fils (WPA/WPA2, Mac Filter, SSID, TKIP et AES, montage et orientation de l'antenne, 802.11i) et leur influence sur la sécurité réseau.
	5	5.1	Connaître les principaux protocoles d'authentification (Radius, Tacacs, Kerberos, LDAP, CHAP/PAP, EAP) et pouvoir en expliquer l'importance pour la sécurité réseau.
		5.2	Connaître des concepts d'implémentation de l'authentification (ACL, droit d'accès minimum, MAC, DAC, RBAC, etc.) et leur influence sur l'implémentation de systèmes de droits.
		5.3	Connaître des méthodes d'identification (biométrie, *proof of possession*, *one-time token*, etc.) et pouvoir en expliquer l'influence sur l'implémentation de méthodes d'identification.
		5.4	Connaître des méthodes d'implémentation de contrôles de sécurité (*policy enforcement*, complexité des mots de passe, dates d'échéance de compte et de mots de passe, administration de droits basée sur des groupes) ou des méthodes organisationnelles (vacances à date fixe, rotation des tâches ou interdictions nocturnes).
	6	6.1	Connaître des concepts fondamentaux de cryptographie (asymétrique, symétrique, non-répudiation, signification des valeurs de hachage, stéganographie, signatures numériques) et leur effet sur l'aménagement du transport et du stockage de données.
		6.2	Connaître des outils cryptographiques adéquats (AES, DES, 3DES, RSA, RC4, NTLM, Blowfish, PGP, WPA/WPA2) ainsi que des outils d'échange crypté (SSL, TLS, IPSec, SSH, HTTPS). Connaître leur effet sur l'aménagement du transport et du stockage de données.
		6.3	Connaître le concept d'infrastructure ICP et son influence sur l'aménagement de la sécurité réseau.
	7	7.1	Connaître des stratégies de sécurité permettant de déceler les violations de sécurité (gestion des risques basés sur le contrôle, maintenance proactive, management des incidents de sécurité, audits de routine des systèmes et des composants de réseau, vérification de droits et privilèges attribués).
		7.2	Connaître des méthodes d'identification de dommages (activités de première réponse), établissement d'une image, sauvegarde de procès-verbaux, enregistrements vidéo ou constat).
		7.3	Connaître le degré de risque de systèmes et composants de réseau critiques et savoir comment les restaurer en cas de dommage.
	8	8.1	Connaître les consignes de sécurité de l'entreprise.
		8.2	Connaître les principes de sensibilisation du personnel à la sécurité système et réseau, notamment en ce qui concerne les règles à respecter en matière de mots de passe, l'utilisation de données et d'informations, la sécurité physique, etc.
		8.3	Connaître les principes de formation du personnel dans le domaine de la sécurité système et réseau, comme les cours, les contrôles et les audits.