SECURITE SYSTEME ET RESEAU : LES FONDAMENTAUX

Public	Tous ceux ayant besoin d'acquérir les compétences fondamentales nécessaires pour développer et mettre en œuvre des mesures de sécurité conçues pour protéger les informations d'entreprise des menaces.
Durée	4 jours - 28 heures
Pré-requis	Une expérience pratique de l'utilisation d'un ordinateur et d'un navigateur est indispensable ainsi qu'une bonne compréhension du besoin de la sécurité informatique.
Objectifs	Aujourd'hui, les entreprises ont de plus en plus besoin d'Internet et des systèmes de réseaux. Parallèlement, la cybercriminalité s'est développée, menaçant ainsi les données et le fonctionnement de l'entreprise. Pour se protéger, sauvegarder les données importantes et maintenir une activité continue, il est essentiel que les ordinateurs et réseaux soient protégés.
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

LES VRAIES MENACES À LA SÉCURITÉ

- Intrus internes et externes
- Observation illicite du trafic sur le réseau
- Cheval de Troie
- Virus
- Mise sur écoute

UNE POLITIQUE DE SÉCURITÉ : LES BASES DE VOTRE PROTECTION

- Définition de vos objectifs de sécurité
- Évaluation de vos risques

CHIFFREMENT SYMÉTRIQUE

- Algorithmes: DES, AES, RC4 et autres
- Évaluation de la longueur et de la distribution des clés

CHIFFREMENT ASYMÉTRIQUE

- Génération de clés
- Chiffrement avec RSA
- PGP et GnuPG
- Évaluation du web of Trust et de PKI

ASSURER L'INTÉGRITÉ DES DONNÉES AVEC LE HACHAGE

- Hachage MD5 et SHA
- Protection des données en transit
- Création de signatures numériques

ÉVALUATION DES PLANS DE MOTS DE PASSE STATIQUES TRADITIONNELS

- Stratégie pour éviter le vol de mots de passe
- Protection contre les attaques d'ingénierie sociale
- Chiffrement des mots de passe pour minimiser l'impact du « sniffing » de mot de passe

MÉTHODES D'AUTHENTIFICATION FORTE

- Éviter les attaques « man-in-the-middle »
- Éviter de rejouer les mots de passe avec les mots de passe à usage unique et ceux à jetons
- Utilisation des biométriques faisant partie de l'authentification à multiples facteurs

AUTHENTIFICATION DES HÔTES

- Se méfier des adresses IP
- Problèmes des imitations d'adresses et déploiement de contre-mesures
- Solutions pour les réseaux sans fil

DÉCOUVERTE DES VULNÉRABILITÉS DU SYSTÈME

- Vulnérabilités du système d'exploitation
- Problèmes des permissions de fichiers
- Limite de l'accès via la sécurité physique

CHIFFREMENT DES FICHIERS POUR LA CONFIDENTIALITÉ

- Chiffrement avec les outils spécifiques aux applications
- Récupération des données chiffrées

RENFORCEMENT DU SYSTÈME D'EXPLOITATION

- Verrouillage des comptes utilisateur
- Sécurisation des permissions administrateur
- Protection contre les virus

SCAN DES VULNÉRABILITÉS

- Rechercher des serveurs non autorisés
- Profiler les systèmes et les services

RÉDUCTION DES ATTAQUES DE TYPE « DÉNI DE SERVICES »

- Sécurisation du DNS
- Limite de l'impact des attaques communes

DÉPLOIEMENT DE FIREWALLS POUR CONTRÔLER LE TRAFIC RÉSEAU

- Éviter les intrusions grâce aux filtres
- Mettre en oeuvre une stratégie de cybersécurité
- Déployer des firewalls personnels

PROTÉGER LES SERVICES ET LES APPLICATIONS WEB

- Valider les entrées utilisateur
- Contrôler la fuite d'informations

MENACES PROVENANT DU RÉSEAU LOCAL

- Observation illicite du réseau
- Atténuation des menaces provenant d'hôtes
- Partitionnement pour éviter les pertes de données
- Identification des faiblesses des LAN sans fil

CONFIDENTIALITÉ DES CONNEXIONS EXTERNES

- Confidentialité grâce au chiffrement
- Sécurisation de la communicaiton avec IPSec

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 03/04/2020