Sensibilisation à la sécurité informatique

Référence : **SECUSER** Durée : **1 jour** Certification : **Aucune**

CONNAISSANCES PREALABLES

- Utilisateurs des outils informatiques et communicants (téléphone, ordinateur, messagerie, Internet, …)..

PROFIL DES STAGIAIRES

- Toute personne souhaitant être sensibilisé à la sécurité informatique.

OBJECTIFS

- Prendre conscience des comportements à risque et apprendre les principales règles d'usage en matière de sécurité informatique.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Histoire des virus et vers

- Quelques exemples concrets de piratage
- Statistiques et exemples de situations réelles marquantes
- Les moyens pour garantir une meilleure sécurité

Loi et sécurité informatique : Le cadre législatif de la sécurité

- Les responsabilités civile et pénale
- Le rôle de la CNIL et son impact pour la sécurité en entreprise

Règles à respecter

- Les devoirs et comportements à adopter vis-à-vis des tiers.
- Les comportements à l'intérieur de l'entreprise. (Le règlement intérieur)
- Les comportements à l'extérieur de l'entreprise. (Les principales lois.)
- Les réseaux sociaux
- Synthèse : charte morale / charte interne / loi

Présentation des 5 piliers de la sécurité informatique

- Intégrité : certificat
- Non-répudiation : certificat
- Authentification : mot de passe / carte à puce
- Confidentialité : cryptage
- Disponibilité : sauvegarde

Raison d'une attaque

- Employés mécontents
- Vengeance concurrent / malveillance / sabotage / incompétence
- Contrat cybercriminalité

Méthodologie d'une attaque : modèle STRIDE

- Spoofing

- Tampering
- Repudiation
- Information disclosure : par les réseaux sociaux
- Denial of service
- Elevation of privilege

Moyens mis à disposition

- Antivirus
- Antivol
- Formation, charte informatique
- Équipement spécialisé (Firewall, IDS …)

Ressources

- RSSI (responsable)
- PRA PCA RTO
- ISO ITIL
- VPN

Type de Menace et Risques

- Virus
- SPAM
- SPOOFING
- SMURFING
- MTM
- HIJACKING

Présentation des situations à risques

- Le téléphone portable
- Le poste de travail (PC, ordinateur portable)
- Les périphériques et le poste de travail (Les risques encourus avec les périphériques USB, CD, DVD Disque interne/externe, clé USB, réseau : quelles différences pour les risques ?
- Ex : Une donnée effacée (ou formatée) ne l'est pas totalement – démonstration

Règles à respecter

- Exemple de propagation de virus par clef USB
- Les réflexes à adopter avec les « corps étrangers »
- Protection contre le vol ou le piratage de données - démonstration

La sécurité et l'entreprise et impact du BYOD

- Cryptage des données – démonstration
- Règles à respecter

Les mots de passe

- Règles d'utilisation et vulnérabilité des mots de passe – démonstration
- Ce que l'on peut faire avec le mot de passe d'autrui / Qu'est-ce qu'une attaque par dictionnaire ?
- Pourquoi peut-on être forcé de respecter une stratégie de nomenclature ?
- Ne pas confondre mot de passe local des serveurs

La messagerie électronique et Internet

- Les dangers et leurs conséquences : spams, spywares, DDoS, phishing, trojans, Adwares,
- Virus
- Traces laissées – démonstration
- Usurpation d'identité – démonstration
- Signature électronique, intérêt – démonstration
- Règles à respecter

Le Wi-Fi

- Principes de fonctionnement et niveaux de sécurité
- Visibilité " de vos données – démonstration
- Ecoute " de vos transactions – démonstration
- Règles à respecter