Formation Sécurité Informatique SI – Sensibilisation des Utilisateurs

Code : SE02 **Durée** : 1 jour **Classe** : Présentiel / à distance

Public

- Cette formation sécurité informatique s'adresse à toute personne concernée par une démarche sécurité au sein de l'entreprise.

Prérequis

- Aucune connaissance technique requise

Objectifs

- Comprendre les risques liés à la sécurité informatique
- Identifier les menaces courantes en entreprise
- Adopter des comportements sécurisés au quotidien
- Appliquer les bonnes pratiques de protection des données

Programme détaillé

1- La sécurité et l'entreprise

- Quelques exemples concrets d'incidents et de piratages en entreprise
- Les « briques » concernées par la sécurité : système, logiciel, réseau, web, données
- Le facteur humain, un enjeu central développé tout au long de la formation
- Distinguer ce qui peut être perdu sans conséquence grave
- Identifier les biens à protéger en priorité
- Les moyens permettant de garantir un meilleur niveau de sécurité
- Le rôle et l'utilité d'une charte d'utilisation des ressources informatiques

2- Loi et sécurité informatique

- Le cadre législatif de la sécurité
- Les responsabilités civile et pénale
- Les principales lois
- Le rôle de la CNIL et son impact pour la sécurité en entreprise
- Le règlement intérieur
- Synthèse : charte morale / charte interne / loi

3- Les mots de passe

- 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 la base de compte locale et celle du serveur
- Les devoirs et comportements à adopter vis-à-vis des tiers
- Les comportements à l'intérieur de l'entreprise
- Les comportements à l'extérieur de l'entreprise

4- Les périphériques et le poste de travail

- Les risques encourus avec les périphériques USB, CD, DVD
- Le poste de travail pour Windows (C :, D :, E :, ...)
- Disque interne/externe, clé USB, réseau : quelles différences pour les risques ?
- Exemple de propagation de virus par clef USB
- Les réflexes à adopter avec les « corps étrangers »

5- Comprendre les bases du réseau

- Chaque équipement (PC, serveur, etc.) dispose d'une adresse IP
- Vocabulaire réseau de base : passerelle, DNS, DHCP
- Chaque application est identifiée par un numéro de port
- Le rôle d'un firewall d'entreprise

Formation Sécurité Informatique SI – Sensibilisation des Utilisateurs

Code : SE02 **Durée** : 1 jour **Classe** : Présentiel / à distance

- Les limites du firewall : ce qu'il ne remplace pas en matière de vigilance des utilisateurs
- Les risques liés à la connexion du portable d'un visiteur au réseau de l'entreprise
- L'intérêt d'utiliser un serveur proxy en entreprise pour l'accès au Web

6- Inventaire du matériel et des logiciels

- L'automatisation de la remontée d'information
- Comparaison des deux plugins Fusion Inventory et OCS Inventory NG
- Installation de Fusion Inventory sur les clients
- Gestion des équipements « identiques » (gabarit)

7- Comportement par rapport à la messagerie

- Le mail un simple fichier texte ?
- La réception des messages (SPAM, faux messages...)
- Le mauvais usage de la retransmission des messages
- Les courriers électroniques de taille importante
- L'usurpation d'identité

8- Risques liés à Internet

- Navigation et surprises !
- Les problèmes liés au téléchargement de fichiers
- Limites de l'ultra protection des navigateurs
- Peut-on « rattraper » une information divulguée ?
- La téléphonie utilise maintenant les réseaux de données