Bonnes pratiques pour défendre son système informatique des menaces en ligne et sur site

Mise à jour nov. 2023

Durée 2 jours (14 heures)

« Délai d'accès maximum 1 mois »

OBJECTIFS PROFESSIONNELS

- Aider les responsables des TPE et PME à protéger leur entreprise des menaces informatiques

PARTICIPANTS

- Responsable de services informatiques et intervenants techniques (service IT)

PRE-REQUIS

- Une réelle connaissance informatique est nécessaire

MOYENS PEDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Remise d'un support de cours.

MODALITES D'EVALUATION

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

MOYENS TECHNIQUES EN PRESENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et comuniquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré. Nous préconisons 4 personnes maximum par action de formation en classe à distance

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

PROFIL FORMATEUR

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

Programme de formation

Accueil et introduction (01h00)

- Présentation de l'objectif du cours
- Brève introduction à la cybersécurité

Les menaces en ligne pour les TPE et PME (01h30)

- Les principales menaces en ligne : phishing, ransomware, malware, etc.
- Les menaces venant de l'intérieur : virus, vol de données, destruction de données...
- Exemples de cas réels de cyberattaques contre les petites entreprises
- Les conséquences financières et de réputation des cyberattaques

Bonnes pratiques et cybersécurité (02h30)

- Utilisation de mots de passe forts et uniques
- Cryptage de fichiers
- Mises à jour régulières des logiciels
- Sensibilisation à l'email et aux pièces jointes suspectes
- Sensibilisation aux bonnes pratiques : usb, échanges de documents, gestion des comptes...
- Travail à distance et prestataires extérieurs
- Accès au réseau en inter, Wi-Fi…

Comment sécuriser mon environnement (00h45)

- Le poste de travail
- Outils et conseils pour sécuriser le poste utilisateur (Windows 10/11...)

Suite de la sécurisation du poste client (01h30)

- Rappels des technologies disponibles dans Windows : Antivirus, boot sécurisé...
- Sécurisation par GPO
- Cryptage de postes et des fichiers
- Gestion des certificats

Comment sécuriser le domaine et Active Directory ? (00h45)

- Comment bien organiser Active Directory et les GPO
- Renforcer la gestion des comptes et des groupes pour éviter les failles

Comment surveiller Active Directory ? (00h45)

- Comment surveiller son SI à la recherche d'anomalies
- Bonnes pratiques et sources d'informations pour aller plus loin…

Comment sécuriser mon serveur de fichiers ? (01h30)

- Bonnes pratiques pour gérer le serveur et les permissions sur les fichiers
- Outils pour sécuriser le serveur de fichiers
- Gestionnaire de ressources, sysinternals...
- Comment surveiller les accès aux fichiers ?

Sécuriser les services réseaux du quotidien (01h00)

- Service DHCP et serveur DNS : quels risques et quelles solutions ?
- Gestion des accès depuis l'extérieur : VPN, Web, Rds...
- Gestion du Wifi : accès privé / accès public

Gestion des mises à jour serveurs et postes clients (01h00)

- Mise à jour manuelle ou automatisée
- Mise à jour des postes clients : obligatoire / falcultative
- Mise à jour des serveurs : bonnes pratiques ?

Serveurs d'impressions et serveurs applicatifs (00h45)

- Comment augmenter la sécurité de l'impression
- Bonnes pratiques pour les serveurs applicatifs

Prévoir un plan de reprise et de continuité en cas d'attaques ou de panne (01h00)

- Évaluer les risques
- Définir les priorités
- Assurer la continuité