Cybersécurité

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

2 jours (14 heures)

Délai maximum : 2 mois.

Parcours concourant au développement des compétences. Action de formation réalisée en application des articles L 6313-1 et L 6313-2 du Code du travail.

Si vous êtes en situation de handicap, contactez-nous avant le début de votre formation pour que nous puissions vous orienter efficacement et vous accueillir dans les meilleures conditions.

Objectifs pédagogiques

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

Pré-requis

Une réelle connaissance informatique est nécessaire.

Modalités pédagogiques

Modalités de formation:

- Formation réalisée en présentiel, à distance ou mixte,
- Toutes nos formations peuvent être organisées dans nos locaux ou sur site
- Feuille de présence signée en demi-journée, questionnaires d'évaluation de la satisfaction en fin de stage et 60 jours après, attestation de stage et certificat de réalisation.
- Horaires de la formation: 9h - 12h30 et 13h30 - 17h.
- Les horaires de la formation sont adaptables sur demande.

Moyens pédagogiques

- Formateur expert dans le domaine,
- Mise à disposition d'un ordinateur, d'un support de cours remis à chaque participant,
- Vidéo projecteur, tableau blanc et paperboard,
- Formation basée sur une alternance d'apports théoriques et de mises en pratique
- Formation à distance à l'aide du logiciel Teams pour assurer les interactions avec le formateur et les autres stagiaires, accès aux supports et aux évaluations. Assistance pédagogique afin de permettre à l'apprenant de s'approprier son parcours. Assistance technique pour la prise en main des équipements et la résolution des problèmes de connexion ou d'accès. Méthodes pédagogiques : méthode expositive 50%, méthode active 50%.

Public visé

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

Modalités d'évaluation et de suivi

- Evaluation des acquis tout au long de la formation : QCM, mises en situation, TP, évaluations orales…

Programme de formation

Accueil et introduction

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

Les menaces en ligne pour les TPE et PME

¨ Les principales menaces en ligne : phishing, ransomware, malware, etc.

Contacts

Notre centre à **Mérignac**
14 rue Euler
33700 MERIGNAC
05 57 92 22 00
contact@afib.fr

Notre centre à **Périgueux**
371 Boulevard des Saveurs,
24660 COULOUNIEIX CHAMIERS
05 64 31 02 15
contact@afib.fr

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

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

Suite de la sécurisation du poste client
- 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 ?
- Comment bien organiser Active Directory et les GPO
- Renforcer la gestion des comptes et des groupes pour éviter les failles

Comment surveiller Active Directory
- 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 ?
- 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
- 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
- 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
- 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
- Evaluer les risques
- Définir les priorités

Mise à jour le 06/10/2023

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

¨ Assurer la continuité

Mise à jour le 06/10/2023