Programme de Formation

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

Organisation

Durée : 14 heures

Mode d'organisation : Mixte

Contenu pédagogique

Public visé

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

Objectifs pédagogiques

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

Description

Introduction

- Présentation de la formation, des participants et de leurs attentes spécifiques
- 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
- 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
- Cryptages de fichiers
- Mises à jour régulières des logiciels
- Sensibilisation à l'email et aux pièces jointes suspectes
- Sensibilisation aux bonnes pratiques : échanges de documents, gestion des comptes…
- Travail à distance et prestataires extérieurs
- Accès au réseau en interne, 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
- Assurer la continuité

Bilan, évaluation et synthèse de la formation

Prérequis

- Une réelle connaissance informatique est nécessaire

Modalités pédagogiques

- Tour de table pour validation des attentes spécifiques, des objectifs, du programme…
- Le formateur alterne entre méthode démonstrative, interrogative et mise en œuvre par des travaux pratiques
- Ordinateurs avec environnement logiciel spécifique, connexion internet

Moyens et supports pédagogiques

- Un support de cours numérique ou papier sera remis à chaque participant.

Modalités d'évaluation et de suivi

- La validation des acquis sera réalisée à travers un quiz et/ou une certification
- Une évaluation qualitative de la formation sera complétée par le stagiaire