Parcours TAI – Module Installation et sécurisation des équipements

Partie 1 : Les fondamentaux de la sécurité numérique (20 mins)

Q1. Expliquez clairement et simplement le modèle C.I.A (Confidentialité, Intégrité et Disponibilité).

-Donnez une définition brève de chaque terme
-Illustrer chaque terme par un exemple pratique en milieu professionnel.

-Confidentialité : Protection des informations contre les accès non autorisés.

Exemple : Restreindre l'accès aux fichiers sensibles par des droits d'utilisateurs.

-Intégrité : Assurer que les données restent exactes et inchangées sauf par des actions autorisées.

Exemple : Utilisation de contrôles d'intégrité pour éviter les modifications malveillantes.

-Disponibilité : Garantir l'accès aux données et aux services quand nécessaire.

Exemple : Mise en place de sauvegardes et de serveurs redondants pour éviter les interruptions.

Q2. Citez et décrivez brièvement trois types de menaces informatiques courantes auxquelles vous pourriez être confronté(e) en tant que technicien d'assistance informatique.

-Logiciels malveillants (Malware) : Programmes nuisibles comme les virus et ransomwares.

-Phishing : Usurpation d'identités pour obtenir des informations sensibles via e-mails trompeurs.

-Attaques par injection SQL : Exploitation de failles dans une base de données via des entrées malveillantes.

Partie 2 : Logiciels de sécurités (20 mins)

Q3. Vous devez sécuriser un poste Windows pour un nouvel employé. Quelles sont les trois étapes essentielles de configuration d'un antivirus ?

Installation et mise à jour : Télécharger, installer et s'assurer que l'antivirus est à jour.

Configuration des analyses automatiques : Planifier des scans réguliers pour détecter des menaces.

Activation de la protection en temps réel : Surveiller les fichiers et connexions pour bloquer les logiciels malveillants immédiatement.

Q4. A quoi sert un pare-feu sur un poste informatique ?

-Décrivez précisément deux actions que vous effectuez systématiquement pour configurer efficacement un pare-feu sur un poste utilisateur.

Rôle : Filtre les connexions réseau, bloque les accès non autorisés et prévient les intrusions.

Actions essentielles :

Définir des règles strictes : Bloquer les connexions suspectes et autoriser uniquement les flux nécessaires.

Activer les alertes et les journaux : Surveiller les tentatives d'accès et détecter des activités suspectes.

Partie 3 : Gestion des mises à jour et des applications (15 mins)

Q5. Pourquoi est-il essentiel d'effectuer régulièrement les mises à jour des logiciels ?

-Décrivez précisément une conséquence possible si cette pratique n'est pas suivie.

Essentiel : Corrige les vulnérabilités, améliore la sécurité et les performances.

Conséquence : Une absence de mise à jour expose aux failles connues et facilite les cyberattaques.

Q6. Citez deux paramètres de confidentialité que vous vérifiez systématiquement sur un navigateur internet utilisé en entreprise.

Blocage des cookies tiers : Empêche le suivi et collecte abusive d'informations.

Paramétrage des autorisations : Contrôler l'accès des sites aux caméras, micros et autres données sensibles.

Partie 4 : Politiques de sécurité, mots de passe et contrôle d'accès (20 mins)

Q7. Proposez une règle claire et complète sur la gestion des mots de passe que vous pourriez inclure dans une politique de sécurité informatique d'entreprise.

Longueur minimale : 12 caractères (mélange de majuscules, minuscules, chiffres et symboles).

Aucun mot du dictionnaire, éviter les informations personnelles.

Renouvellement tous les 90 jours.

Utilisation d'un gestionnaire de mots de passe recommandé.

Q8. Expliquez le principe du contrôle d'accès informatique.

-Donnez un exemple concret de mise en œuvre de ce principe dans une entreprise.

Principe : Restreindre l'accès aux systèmes et données selon les rôles et besoins des utilisateurs.

Exemple : Un employé de la comptabilité peut accéder aux factures, mais pas aux dossiers techniques du service IT.

Partie 5 : Gestion des incidents et cryptographie (15 mins)

Q9. Vous constatez une infection par ransomware sur un poste utilisateur. Décrivez succinctement les quatre premières étapes que vous mettez en place immédiatement après la découverte de l'incident.

Déconnexion immédiate du réseau pour éviter la propagation.

Identification du ransomware pour évaluer les dégâts et les méthodes de récupération.

Préservation des preuves pour une éventuelle analyse et enquête.

Restauration depuis une sauvegarde sécurisée (non compromise).

Q10. A quoi sert une signature électronique ? Décrivez un exemple pratique d'utilisation de la signature électronique en entreprise.

Utilité : Authentifier et garantir l'intégrité d'un document numérique.

Exemple : Signature électronique d'un contrat pour éviter les falsifications et sécuriser la validité juridique.