Mettre en place des mesures de sécurité pour les utilisateurs nomades et le télétravail

Référence : **SECNOMAD** Durée : **2 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Connaître et comprendre le guide d'hygiène sécurité de l'ANSSI.

PROFIL DES STAGIAIRES

• Toute personne désireuse de mettre en place des mesure de sécurité informatique pour le télétravail et le nomadisme.

OBJECTIFS

• Comprendre les mesures de sécurité informatique. • Mettre en œuvre les mesures de sécurité informatique pour les utilisateurs nomades et les télétravailleurs/télétravailleuses.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Principaux risques et cybermenaces liés au télétravail et nomadisme

• Tous lieux de travail non maîtrisés par l'entité : Domicile ; Hôtel pendant un déplacement professionnel ; Trajet domicile-travail, dans les transports en commun ; Salles d'attentes ou tout autre lieu public ; Espace de co-working

Risques exacerbés

• Perte ou vol du matériel
• Compromission du matériel
• Compromission des informations contenues dans le matériel volé, perdu ou emprunté
• Accès illégitime au SI de l'entité (et donc la compromission de celui-ci)
• Interception voire altération des informations (perte de confidentialité et / ou d'intégrité)
• Hameçonnage (phishing)
• Rançongiciels (ransomware)
• Vol de données
• Faux ordres de virement (FOVI/BEC)

Recommandations de sécurité pour les télétravailleurs

• Equipements professionnels, séparer les usages
• Appliquer strictement les consignes de sécurité de l'entreprise
• Vérifier que l'antivirus est actif et scanner les équipements
• Renforcer la sécurité des mots de passe
• Sécuriser la connexion WiFi
• Sauvegarder régulièrement votre travail
• Se Méfier des messages inattendus
• N'installer les applications que dans un cadre « officiel » et éviter les sites suspects

Recommandations de sécurité liées au télétravail pour les employeurs

- Définir et mettre en œuvre une politique/charte d'équipement des télétravailleurs
- Maîtriser les accès extérieurs (RDP) limiter / filtrer
- Sécuriser les accès extérieurs (VPN)
- Renforcer la politique de gestion des mots de passe
- Définir une politique stricte de déploiement des mises à jour de sécurité
- "Durcir" la sauvegarde des données
- Utiliser des solutions antivirales professionnelles
- Mettre en place une journalisation de l'activité des équipements de l'infrastructure
- Superviser l'activité des accès externes et systèmes sensibles
- Sensibiliser et apporter un soutien réactif aux collaborateurs en télétravail
- Se préparer / Simuler une confrontation à une cyberattaque
- Impliquer la direction afin de montrer l'exemple