Mission 10 suite :

Module 1 : Panorama de la SSI :

Le cyberespace est un monde à hauts risques qu'il est important d'identifier afin de mettre en place les **mesures de protection adaptées** pour protéger les systèmes d'information visés par les attaquants.
Si malgré toutes les précautions vous êtes la cible d'une cyberattaque, quelques recommandations s'imposent :
En tant que salarié, il est tout d'abord recommandé de **débrancher son ordinateur du réseau** et de couper son Wi-Fi.
Ensuite il est important de **signaler l'attaque** à votre service informatique dans les plus brefs délais afin qu'il puisse intervenir pour évaluer les dommages et **limiter les conséquences**.
D'autre part, la plateforme **cybermalveillance.gouv.fr** mise en place par l'**ANSSI** a pour objectif de venir en aide aux victimes d'actes de cybermalveillance.

La sécurité du numérique ne doit pas se cantonner à des outils, **l'effort humain est nécessaire**.
Pour se protéger, il est nécessaire d'adopter une défense **en profondeur** qui vise à couvrir l'ensemble du spectre des menaces avec des mesures cohérentes et pragmatiques vis-à-vis de l'activité du foyer personnel ou de l'entreprise concernée.
En tant qu'utilisateur du système d'information vous devez être attentif, humble et lucide vis-à-vis des menaces.
Notez que ces mesures de sécurité seront inutiles si celles-ci ne sont pas entièrement respectées.

Module 2 : Sécurité de l'authentification :

L'usurpation d'identité peut avoir des **conséquences importantes** pour vous et par extension pour **votre entreprise**.
C'est pourquoi, **il est nécessaire de suivre les conseils suivants :**
-prévenir le responsable de la sécurité informatique
-déposer plainte auprès des services de police
-signaler immédiatement l'usurpation auprès des services administratifs sociaux,bancaires concernés,..
-demander à son entourage d'effacer les préjudiciables qui n'émanent pas de vous

Avoir une bonne sécurité de mot de passe permet la protection des données sensibles et à caractère personnels, pour cela il faut suivre les conseils émis par l'ANSSI :
-Utiliser des mots de passe forts ;
Vous assurer de connaître la procédure de changement de mot de passe pour l'utiliser le jour où vous en aurez besoin ;
-Utiliser des mots de passe différents sur les sites où vous vous inscrivez ;

-Ne faites pas confiance dans des dispositifs d'accès à Internet (PC, portables, tablettes, smartphones, etc.) dont vous ne connaissez pas le niveau de sécurité ;
-Faites attention à la sécurité de votre propre dispositif d'accès à Internet (mises à jour, antivirus, etc.) ;
-Activer les fonctions de double authentification (par SMS, application, jeton, etc.) quand elles sont disponibles.

Cependant la complexité des mots de passe ne suffit pas pour garantir la sécurité de nos authentifications.
Il est également important de rester vigilant en toutes circonstances pour détecter les pièges et éviter la divulgation de nos mots de passe.

Les bonnes pratiques de gestion de mots de passe :
-Avant d'utiliser des points d'authentification uniques, lisez les conditions générales d'utilisation et restez vigilant quant aux informations qui seraient potentiellement transmises au service en question.
-L'utilisation d'un coffre-fort de mots de passe peut être une excellente solution si elle est maîtrisée et correctement utilisée.
-Restez vigilant quant à la mémorisation automatique de vos mots de passe, configurez les logiciels manipulant vos mots de passe et les matériels (ordinateur, mobile) que vous utilisez pour accéder à vos comptes.
-Vérifiez que les protocoles que vous utilisez sont sécurisés.

Deux formes différentes de cryptographie existent et que pour plus d'efficacité celles-ci sont utilisées de façon combinée.

Les opérations de chiffrement et de déchiffrement de la cryptographie symétrique sont rapides et simples à implémenter.

Elles présentent une certaine limite : la génération, la distribution et la conservation de ses clés posent problème.
Les opérations de la cryptographie asymétrique sont beaucoup plus lentes et il n'est possible de chiffrer que de petits volumes d'information.

L'utilisation d'une clé publique permet de résoudre le problème de la transmission de la clé et l'usage d'un certificat permet d'authentifier de façon sûre cette clé publique.

-cyberattaque : atteinte à des systèmes informatiques dans un but malveillant
-système informatique (SI): lieu qui transite et traite de l'informations.
-sabotage : rendre une partie ou la totalité de la partie du système d'informations inopérante..
-attaque de masse : cyberattaque qui consiste à prendre contrôle des appareils vulnérables afin de cibler une personne morale ou physique.
-cheval de troie : est un programme renfermant un autre programme malveillant permettant à un attaquant de prendre le contrôle du terminal cible.
-DDos: rendre une partie ou totalité du SI indisponible
défense en profondeur : sécuriser chaque sous-ensemble du SI.
-Le niveau « Très Secret Défense » est le plus haut niveau de secret de l'information. Il est réservé aux informations et supports qui concernent les priorités gouvernementales en matière de défense et de sécurité nationale. On estime que la divulgation d'une telle information est de nature à nuire très gravement à la défense nationale.
-Le niveau « Secret Défense » quant à lui, est réservé aux informations et supports dont la divulgation est de nature à nuire gravement à la défense nationale.
-Le niveau « Confidentiel Défense » est réservé aux informations et supports dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié.
-D'autre part, votre entreprise peut également ajouter d'autres niveaux tels que « Restreint » et « Non-protégé/Public » visant respectivement à protéger ou non l'information.
-attaques directes : forces brutes pour obtenir des infos
--attaques indirectes : utilisation de la ruse pour obtenir des infos
-L'attaque par dictionnaire est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé.
-attaque par permutation : elle consiste à fabriquer des dictionnaires en modifiant certains caractères.
- attaque à proximité : elles recouvrent toutes les **attaques** sans intermédiaire : zoomer avec un appareil sur l'écran d'une personne dans un lieu public
-Piégeage du poste : Une autre attaque consiste à piéger un matériel informatique (poste de travail, téléphone portable, équipements de paiement, etc.).
-chiffrement : est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de chiffrement.
-cryptographie : Ensemble des procédés visant à crypter des informations pour en assurer la confidentialité entre l'émetteur et le destinataire.
-cryptage : Opération qui consiste à sécuriser l'accès à des données.

SecNum académie
ANSSI

ATTESTATION DE SUIVI

L'équipe SecNum*académie* atteste que **Robert Kuang** a suivi avec succès les cours des quatre modules de MOOC et obtenu les scores suivants aux évaluations

MODULES	DATE DE L'ÉVALUATION	SCORE
PANORAMA DE LA SSI	06/12/2023	90.0%
SÉCURITÉ DE L'AUTHENTIFICATION	06/12/2023	82.0%
SÉCURITÉ SUR INTERNET	06/12/2023	82.0%
SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME	06/12/2023	88.0%

www.secnumacademie.gouv.fr

Fait le 6 Décembre 2023
L'équipe SecNum*académie*