

COMPTE RENDU 3&4

Une des principales idées reçues par les utilisateurs, tant dans la sphère privée qu'en entreprise, consiste à penser que les cybermalveillances ne les concernent pas. Si dans les débuts de l'informatique, le seul risque encouru était de voir son ordinateur dysfonctionner à cause d'un virus, les attaques peuvent désormais avoir de bien plus fâcheuses conséquences

Sans pour autant se décourager d'utiliser les nombreuses possibilités offertes par le développement d'Internet, il est au contraire important de démystifier les attaques informatiques qui touchent notre quotidien et de présenter des moyens simples et efficaces d'éviter d'en être victime. La sécurité passe avant tout par la connaissance et la compréhension des risques.

Nous allons donc voir dans les parties suivantes comment utiliser Internet de manière plus sécurisée afin d'éviter d'être victime d'actes de malveillance.

Commençons par introduire la différence entre format et extension d'un fichier.

Un fichier n'est fondamentalement qu'une suite de 0 et de 1 compréhensibles par l'ordinateur.

Chaque fichier a un format (une convention d'écriture en quelque sorte), qui lui confère des propriétés et lui permet d'être interprété par des logiciels.

L'extension, c'est le suffixe du nom du fichier, qui lui est renseigné par le créateur du fichier (exemple : logo-anssi.jpg pour une image représentant le logo de l'ANSSI).

Conclusion

Pour résumer, restez prudent sur vos téléchargements et surtout sur l'ouverture des fichiers en provenance d'Internet ou de supports externes tel les clés USB ou les disques durs externes, que vous soyez à l'initiative du téléchargement ou qu'un expéditeur vous l'adresse en pièce jointe par messagerie.

De très nombreuses affaires de cyber-attaque démarrent par un double-clic innocent, sur un simple fichier de tableur par exemple !

Installez un antivirus (lui-même obtenu sur un site d'éditeur de confiance !) pour assurer un scan ponctuel des fichiers téléchargés.

De plus un scan régulier de l'ensemble du disque est indispensable pour s'assurer qu'une propagation n'est pas en cours sur votre poste ou y remédier le cas échéant.

En contexte professionnel, ces manipulations sont du ressort des équipes de Direction des Systèmes d'Information s'il y en a une.

Le module 4 de ce MOOC sera consacré à la sécurisation du poste de travail.

En attendant, nous allons revenir plus en détails sur les bonnes pratiques à adopter lorsque vous naviguez sur Internet ou utilisez votre messagerie électronique.

Dans un navigateur, on rencontre principalement deux protocoles :

- « http » est le moyen non-sécurisé d'accéder à des ressources,
- « https » est la variante sécurisée de ce protocole.

Il est recommandé de privilégier les sites affichant le HTTPS.

Mais qu'est-ce qu'un cookie ?

Ce n'est pas seulement un en-cas !

Un cookie est un objet associé à un site web stocké sur l'ordinateur, qui permet à ce site de stocker des informations relatives au client et de récupérer ces informations lors d'une visite ultérieure du client.

Il n'existe pas de navigateur idéal, chaque navigateur a ses qualités et ses défauts.

Choisissez celui qui vous convient en fonction de vos besoins.

Bien qu'échanger du courrier électronique semble anodin, nos boîtes aux lettres électroniques ne sont pas à l'abri de menaces de toutes sortes : courrier frauduleux, virus, hameçonnage, cheval de Troie, démarchage indésirable, etc.

Il est donc nécessaire d'être vigilant au quotidien pour utiliser sa messagerie en toute sécurité

Dans cette unité, nous avons pu voir comment appréhender au mieux les menaces qui existent sur le courrier électronique et la messagerie instantanée.

Vous êtes désormais conscient que votre messagerie quelle qu'elle soit (client lourd ou léger) ainsi que vos services de messageries instantanées sont la cible de différentes formes de menaces.

Veillez à respecter les bonnes pratiques de cette unité afin de vous protéger ainsi que votre organisation des malveillances.

Pour résumer ce que nous avons vu dans cette unité, avant d'afficher une page web, le navigateur doit connaître l'adresse du serveur web correspondant à l'aide d'un ou plusieurs serveurs DNS.

Lorsque l'adresse IP est obtenue, le navigateur demande une page du site au serveur web. L'utilisation d'un (ou proxy) peut vous permettre d'optimiser l'ouverture de pages web déjà consultées, d'améliorer la sécurité de vos navigations et d'empêcher une éventuelle infection.

Pour conclure cette unité, rappelez-vous qu'il est essentiel de respecter un certain nombre de paramètres de base pour assurer la sécurité de vos appareils.

Aujourd'hui les équipements modernes disposent de nombreux outils et interfaces de communication : Bluetooth, Wi-Fi, NFC, Micro, Caméra, etc. auxquels peuvent accéder le système et les applications.

Notons que ces interfaces peuvent présenter des risques. En effet, certaines peuvent être utilisées à votre insu et présentent une surface d'attaque supplémentaire pour votre équipement ou des vecteurs supplémentaires d'atteinte à la confidentialité.

COMTE RENDUE 1&2

Le chiffrement est le mécanisme consistant à protéger une donnée en la rendant inintelligible. Nous allons donc principalement nous intéresser à la confidentialité de la donnée.

L'opération inverse, le déchiffrement, n'est possible que si l'on dispose d'un élément secret appelé « clé ».

Par convention, le message à cacher est dit « message clair » et le résultat du chiffrement s'appelle « message chiffré ».

Le chiffrement peut être un élément de défense en profondeur. Par exemple, si un message est intercepté, ou tout simplement perdu, celui-ci est quand même protégé car seules les personnes possédant la clé peuvent le lire.

Notez que le verbe « **crypter** » ne doit pas être utilisé pour dire « chiffrer ». Ce terme provient d'un anglicisme **et n'existe pas en français**. En revanche, « décrypter » existe et n'a pas le même sens que « déchiffrer ».


On parle de décryptage ou de décryptement lorsque l'on tente de retrouver un texte clair **sans connaître la clé**.

Les **protocoles sécurisés** (HTTPS, IMAPS, SMTPS, etc.) utilisent les **mécanismes de cryptographie** pour répondre à **4 objectifs**.

Dans le cadre du traitement, du stockage ou de la transmission sécurisée de données, les objectifs de la cryptographie sont :

- CONFIDENTIALITÉ
- INTÉGRITÉ
- AUTHENTICITÉ
- NON-RÉPUDIATION

Le chiffrement asymétrique repose sur des opérations plus complexes, dont les performances sont limitées. Il permet donc d'échanger efficacement un petit volume de données, mais de façon sûre avec un interlocuteur.




SecNum
académie
ANSSI

ATTESTATION DE SUIVI

L'équipe SecNumacadémie atteste que **Harris MOHAMMAD** 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 | 86.0% |
| SÉCURITÉ DE L'AUTHENTIFICATION | 06/12/2023 | 80.0% |
| SÉCURITÉ SUR INTERNET | 06/12/2023 | 84.0% |
| SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME | 06/12/2023 | 84.0% |



Fait le 6 Décembre 2023
L'équipe SecNumacadémie

www.secnumacademie.gouv.fr