



—

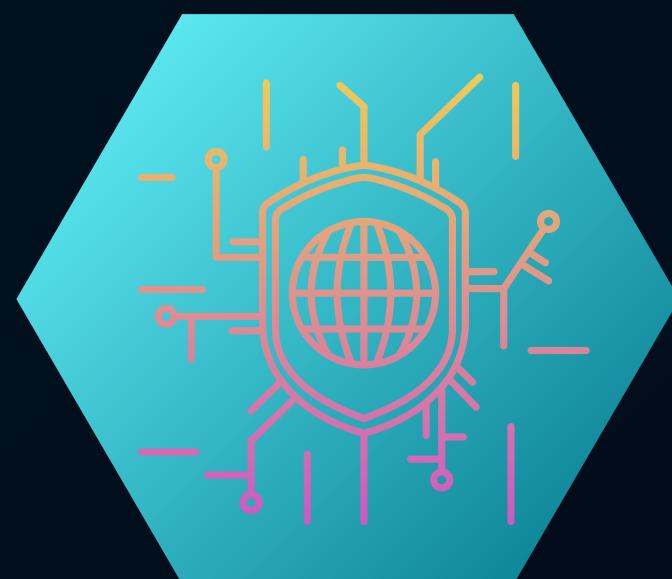


CYBER SECURITY

P R E S E N T A T I O N

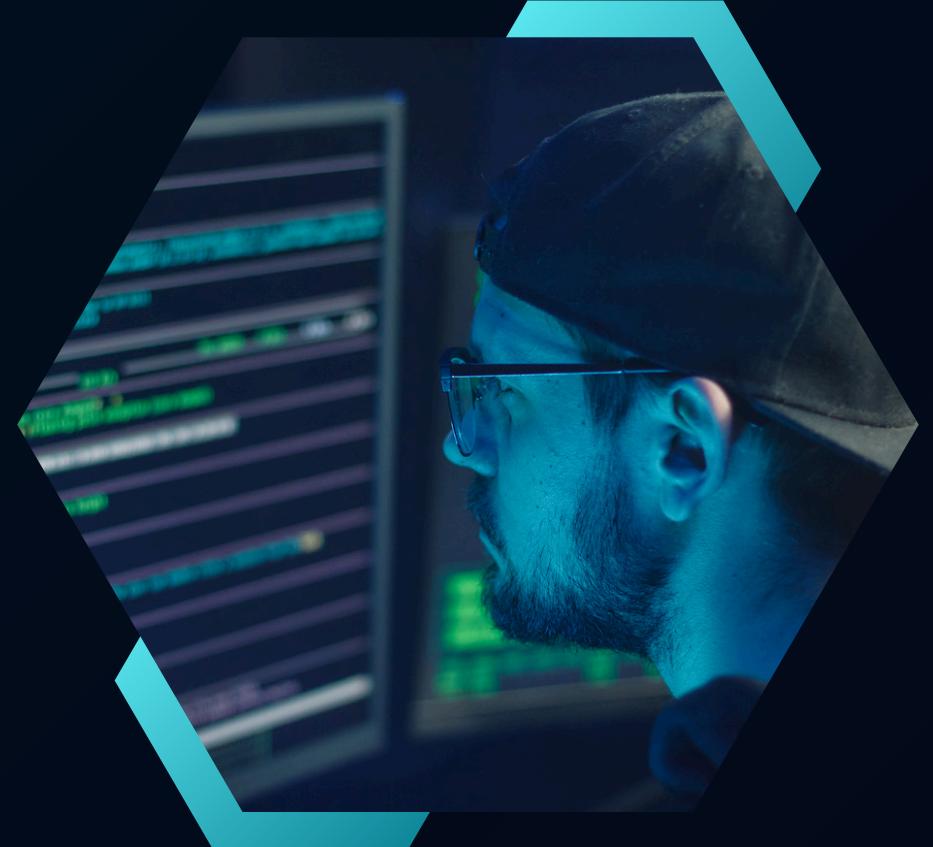


La **cybersécurité** se concentre sur la protection des systèmes d'information contre les intrusions, tandis que la **cybersurveillance** consiste à surveiller ou infiltrer des systèmes adverses. Bien que les compétences mobilisées puissent être similaires, leur objectif diffère : la cybersécurité est **défensive**, alors que la cybersurveillance peut être **offensive**. En France, l'ANSSI gère uniquement les missions de protection (défensives), séparées des missions offensives.



CYBERSÉCURITÉ ET CYBERSURVEILLANCE

Il est fréquent de voir les termes *cybersécurité* et *sécurité numérique* employés tour à tour comme des synonymes. Pourtant, il est communément accepté que la cybersécurité - à l'image d'autres termes dotés du préfixe *cyber* - renvoie à la sécurité des systèmes d'information tandis que la sécurité numérique renvoie plus largement à la sécurité des systèmes et des pratiques numériques. Ainsi, les bonnes pratiques de sécurité numérique sont aussi bien techniques que comportementales.





—



A PROPOS DE LA CYBERSECURITÉ

La cybersécurité concerne tous les utilisateurs, chacun doit être vigilant quand il utilise des outils informatiques face à des demandes suspectes, des pièces jointes ou des supports USB douteux. Au moindre doute ou constatation d'événements suspects, le responsable de la sécurité doit être alerté.

Définition : La cybersécurité consiste en la protection des systèmes contre les attaques numériques comme les malwares et intrusions. Un malware est un programme malveillant qui infecte la machine ciblée et qui peut créer diverses failles de sécurité et endommager et/ou perturber le fonctionnement d'un système informatique.



LES DIVERSES MENACES



Ransomware/rançogiciels sont des logiciels qui bloquent l'accès aux données ou aux machines afin de pousser la cible visée à effectuer un paiement en retour du service

A l'image d'un virus qui peut infecter une personne, ce virus IT est un morceau de code contagieux qui infecte un logiciel et se propage de fichier en fichier sur un système. Lorsque des logiciels ou des fichiers infectés sont partagés entre ordinateurs, le virus se propage alors au nouvel hôte.



L'adware : c'est un virus qui a pour but de gagner de l'argent en exploitant votre machine. Il vous inonde de pub



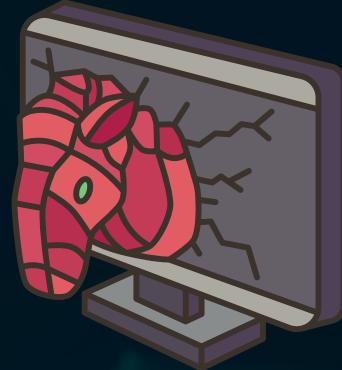
Un Logiciel destructeur est un logiciel dont le but est purement néfaste sans aucun autre but que la destruction pure ce type de menaces est très rare et consiste à détruire les éléments du pc effacer la mémoire faire surchauffer intentionnellement le pc afin de mettre ses composants à risque etc



Un scarewares (ou « logiciels alarmants ») sont un type d'arnaque recourant à l'ingénierie sociale et se servant de la peur pour pousser les gens à télécharger des logiciels malveillants, à dépenser de l'argent ou à transmettre des données personnelles.

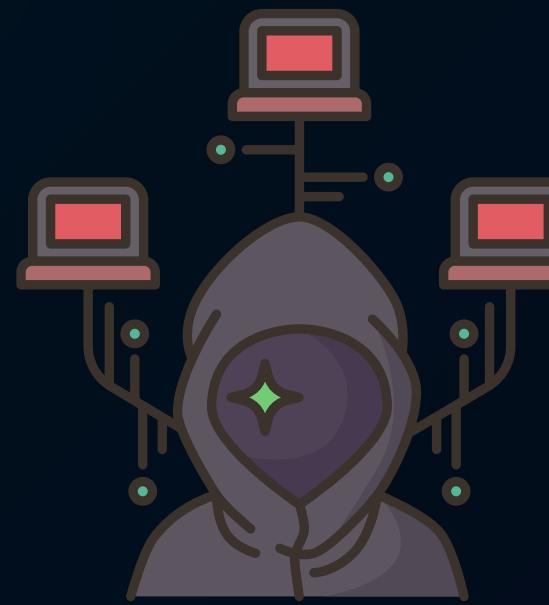


LES DIVERSES MENACES



Cheval de Troie : A l'image du cheval de Troie de la mythologie grecque, ce malware est déguisé en/dans un programme sûr conçu pour tromper les utilisateurs, de sorte qu'ils l'installent sans le vouloir sur leur propre système.

Zombie / Botnet referre a une ou plusieurs machines contrôlées à l'insu de son utilisateur par un cybercriminel. Ce dernier l'utilise alors le plus souvent à des fins malveillantes, par exemple afin d'attaquer d'autres machines en dissimulant sa véritable identité.



Un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Il a la capacité de se dupliquer une fois qu'il a été exécuté. Contrairement au virus, le ver se propage sans avoir besoin de se lier à d'autres programmes exécutables.



Le mot rootkit désigne un ensemble d'outils utilisés par les hackers pour s'infiltrer dans votre ordinateur et en prendre le contrôle, tout en étant le plus discret possible.

Le Spyware Logiciel espion qui communique des données personnelles (adresse,nom,email,) Dans les cas les plus graves il peut aussi communiquer des données plus sensible mdp données bancaire etc voir Keylogger





VOIES D'INTRUSIONS

- Via un périphérique infecté - par le biais du branchement d'une clé USB ou encore dans un disque dur par exemple.
- Phishing - cela consiste à tromper l'utilisateur en l'incitant à cliquer sur un lien à priori de confiance alors qu'en réalité il est conçu pour tromper et escroquer les utilisateurs. Dans le but de récupérer des données sensibles.
- Cheval de Troie - Il s'introduit par une faille de sécurité d'une application sous une forme innocente.
- Ver informatique/Worm - Un ver peut arriver directement par le réseau en profitant d'un port ouvert, mais la méthode la plus classique consiste à s'introduire sous la forme d'une pièce jointe attachée à un mail.
- Zombie/Botnet - Il existe deux méthodes principales d'infection que les pirates utilisent pour infecter les PC et les ajouter au botnet : les téléchargements drive-by et les courriers électroniques.

Un téléchargement drive-by est l'installation d'un malware sur un PC par simple visite d'une page WEB sans intervention de l'utilisateur.



La protection

01

Le facteur humain :

Sensibiliser et former les utilisateurs aux bonnes pratiques en matière de sécurité ,par un mot de passe complexe et la détection de tentative de phishing.

02

Les mesures techniques : utilisation de pare-feu, antivirus et systèmes de détection d'intrusions pour empêcher les accès non autorisés.

03

Mises à jour régulières afin de maintenir les logiciels à jour pour corriger les vulnérabilités.

04

Appliquer et respecter les normes et les réglementations RGPD pour protéger les données. Réaliser des audits réguliers pour vérifier la conformité et l'efficacité des mesures de sécurité mises en place.

LES BONNES PRATIQUES



La détection

05

Par l'utilisation de système de surveillance pour identifier les comportements suspects et les anomalies dans le réseau

06

Déployer des logiciels spécialisés pour analyser le trafic réseau et détecter des intrusions potentielles

07

LA GESTION DE CRISE

1. Préparation

- Plan de réponse aux incidents : Élaboration d'un plan détaillé qui décrit les étapes à suivre en cas d'incident de cybersécurité.

2. Détection

- Surveillance continue : Mise en place de systèmes de détection d'intrusions et de surveillance des réseaux pour identifier rapidement les comportements suspects.

3. Évaluation de la crise

- Analyse de l'incident : Évaluation de la nature, de la portée et de l'impact de l'incident de cybersécurité (type de malware, systèmes affectés, données compromises).

4. Réponse à la crise

- Activation du plan de réponse : Mise en œuvre des procédures établies pour contenir l'incident, réduire et réparer les dommages pour protéger les systèmes.
- Équipes de réponse aux incidents : Mobilisation des experts en cybersécurité pour analyser et gérer l'incident, en collaboration avec d'autres départements (IT, communication, juridique).





EN CONCLUSION



La cybersécurité est un domaine complexe et dynamique qui nécessite une approche proactive et préventive. Elle implique non seulement des mesures techniques, mais aussi une sensibilisation constante des utilisateurs et une conformité aux réglementations. La collaboration entre tous les acteurs est essentielle pour garantir une protection efficace contre les menaces cybernétiques.



MERCI DE VOTRE

ATTENTION

A M É L I E

A R T H U R

F A T O U M A T A

L A U R E N C E