La cybersécurité

La cybersécurité désigne l'ensemble des mesures et des pratiques visant à **protéger les systèmes informatiques, les réseaux, les données et les appareils** contre les attaques, les dommages ou les accès non autorisés. Elle englobe la prévention, la détection et la réponse aux menaces dans le but de garantir la confidentialité, l'intégrité et la disponibilité des informations numériques.

Les principales menaces

Attaque par saturation (DDoS)

Attaques visant à surcharger les serveurs ou les réseaux, les rendant inaccessibles aux utilisateurs.

Exemple : un site internet de commerce en ligne est submergé de demandes de connexion, le rendant inaccessible aux acheteurs.

Logiciels malveillants (malware)

Programmes conçus pour endommager ou accéder illégalement à des systèmes informatiques.

Exemple : virus, chevaux de Troie, ransomwares.

Ingénierie sociale (piratage psychologique)

Technique utilisée pour tromper les individus afin d'obtenir des informations sensibles ou de les inciter à effectuer des actions risquées pour la sécurité.

Exemple : un pirate informatique crée un faux concours en ligne offrant de fabuleux prix pour inciter les gens à fournir leurs informations personnelles.

Cyberattaques Menaces

L'hameçonnage (phishing)

Technique utilisée pour tromper les utilisateurs en leur faisant divulguer des informations personnelles ou financières via des emails ou des messages frauduleux.

Exemple : un email prétendant être de votre banque demandant vos informations de connexion.

Cyberattaque sur les infrastructures

Attaques visant les systèmes essentiels tels que l'électricité ou les services de santé, pouvant causer des dommages considérables.

Exemple : une attaque visant les systèmes informatiques d'un hôpital, bloquant l'accès aux dossiers médicaux.

Piratage de mots de passe

Tentatives pour obtenir ou deviner les mots de passe des utilisateurs afin d'accéder à leurs comptes en ligne.

Exemple : un pirate devine un mot de passe faible à l'aide de logiciels automatisés.

Les règles pour sécuriser un environnement numérique

Gérer et sécuriser les mots de passe

Utiliser un mot de passe suffisamment long et complexe.

Se protéger des logiciels malveillants

Pour vous protéger, il est indispensable de posséder un antivirus et un pare-feu qui bloqueront les connexions non désirées.

Sauvegarder vos données

Effectuer des sauvegardes régulières de vos données pour les protéger en cas de panne, de vol ou de piratage.

Faire des mises à jour régulièrement

Un appareil ou un logiciel qui n'est pas à jour est vulnérable lors d'attaques informatiques.

Éviter les réseaux Wi-Fi publics

Ces réseaux peuvent permettre aux hackers (pirates informatiques) d'intercepter vos données.

Attention aux liens et pièces jointes

De nombreux liens ou fichiers sont infectés et peuvent contenir des virus et autres logiciels malveillants.

Diffuser un minimum d'informations personnelles

Si un hacker obtient vos données personnelles, il peut réaliser de véritables escroqueries telles que l'usurpation d'identité, le détournement de fonds, le harcèlement…

Les 5 conseils pour créer un mot de passe sécurisé

1 • **Longueur :** utilisez un mot de passe long, avec au moins 12 caractères.
2 • **Complexité :** mélangez les lettres majuscules, minuscules, chiffres et caractères spéciaux (@,!,%).
3 • **Originalité :** ne choisissez pas de mots de passe évidents ou faciles à deviner.
4 • **Variété :** utilisez un mot de passe différent pour chaque compte en ligne.
5 • **Confidentialité :** ne partagez jamais votre mot de passe avec qui que ce soit.