Sécurité Numérique

Enjeux et réponses
pour une utilisation sereine de l'informatique

Vu dans la presse

- **Stuxnet (2010)**
  attaque des centrifugeuses Iraniennes

- **l'affaire Snowden (2013)**
  ancien de la NSA et lanceur d'alertes

- **prise de contrôle d'une voiture (2015)**
  prise de contrôle complet d'une voiture à distance

- **Wannacry (2017)**
  cryptage de données

Les Menaces

Finalités poursuivies

ATTEINTE À L'IMAGE

CYBER CRIMINALITÉ

ESPIONNAGE

SABOTAGE

Les Menaces

Motivations et profils d'attaquants

LUCRATIVE
Cyber-mercenaires
Officines
Escrocs

IDÉOLOGIQUE
Hacktivistes
Cyber-terroristes
Cyber-patriotes

ÉTATIQUE
Unités spécialisées

LUDIQUE
Adolescents désœuvrés ou non (script-kiddies)

TECHNIQUE
Hackers chevronnés

PATHOLOGIQUE
Vengeurs
Employés mécontents

Pourquoi les attaques réussissent-elles ?

- Systèmes et applications pas à jour.
- Politique de gestion de mots de passe insuffisante.
- Pas de séparation des usages (utilisateur/ administrateur) et des réseaux.
- Laxisme dans la gestion des droits d'accès.
- Absence de surveillance des Systèmes informatiques.
- Pas d'anticipation des menaces souvent pour des raisons financières.
- Cloisonnement insuffisant des systèmes (propagation latérale).
- Nomadisme / télétravail incontrôlé.
- Sensibilisation et maturité insuffisante des utilisateurs.

Les Cyber-attaques les plus courantes

- Les malwares
- Le phishing
- Le Man-in-middle
- Le Ddos ou déni de service distribué
- L’attaque par injection SQL
- L’attaque zéro-day
- Le ransonware
- Le cryptojacking

Les Cyber-attaques les plus courantes

- **- Les malwares**
  Ce sont des programmes malveillants souvent installés par une pièce jointe d'un mail ou par une connexion d'une clé USB inconnue.
  - les virus et certains malwares souvent détectés par des outils spécifiques.
- **- Les chevaux de Troie**
  ils ressemblent à des programmes légitimes donc peuvent passer inaperçus; ils servent à préparer la future attaque d'un malware.
- **- Le Phishing**
  c'est une demande d'informations personnelles par mail ou SMS en se faisant passer pour un site connu (banque, assurances, impôts, Caf, etc)

Les Cyber-attaques les plus courantes

- **Le Man-in-middle**
  c'est la copie d'un site web qui se place entre l'utilisateur et le site réel afin de récupérer vos coordonnées et mots de passe, et plus si le site est marchand.
- **Le DDos ou déni de service distribué**
  c'est une saturation d'un serveur web par un afflux de connexions de machines zombies que ce serveur ne peut pas traiter. Le pirate demande une rançon pour faire cesser la saturation
- **L'attaque par injection SQL**:
  le hackeur insère une ligne de code dans un programme pour rendre visibles les données utilisateur .

Les Cyber-attaques les plus courantes

- **L’attaque zéro-day**:
  Si un hébergeur annonce une opération de maintenance il s’expose à un fort risque de piratage car les pirates vont immédiatement se lancer à la recherche de nouvelles failles à exploiter.
- **Le ransonware** :
  le pirate accède aux fichiers sensibles et verrouille les accès au système.
- **Le cryptojacking**:
  le pirate vous a injecté un programme de minage de crypto-monnaie.

Comment éviter les cyber-attaques

- **Utiliser un VPN est une bonne solution**:
  Les données sont cryptées entre votre ordi et le VPN et votre adresse IP change à chaque connexion donc vous pouvez surfer anonymement.
- **Garder votre Antivirus et votre pare-feu à niveau**:
  Windows defender sous Win 10 & Win11.
- **Utiliser l'authentification multi-facteurs**
  contre l'usurpation d'identité : login et mot de passe ne seront plus suffisants pour le pirate s'il n'a pas le code envoyé par le site sur un autre appareil.
- **Ne pas baisser votre niveau de vigilance**

Le Phishing ou Hameçonnage

- C’est le danger principal pour nous, utilisateurs. Il cible notre naïveté, notre goût du confort d’utilisation.
- Ce manque de vigilance nous rend complice du hameçonneur. (argument utilisé par la police et les assureurs).
- Il se diffuse principalement par 3 moyens:
- Par téléphone.
- Par mail.
- Par Sms.

CONSEILS & SENSIBILISATION

- Choisir avec soin ses mots de passe et leur gestion.
- Mettre à jour régulièrement votre système et vos logiciels.
- Effectuer des sauvegardes régulières (système & données.
- Etre prudent, voire suspicieux lors de la réception de messages et de SMS.
- Se méfier des clés USB extérieures à votre environnement,
- Relever votre niveau de prudence dans les lieux publics où le wifi est gratuit et pas toujours sécurisé.

CONSEILS & SENSIBILISATION

- **Ne pas sous-estimer les pirates**
  dont l'inventivité et la ténacité est sans limite.
- **Restez un utilisateur vigilant**
  même si vous devez flirter parfois avec la paranoïa.
  Ne les laissez pas s'introduire dans votre intimité numérique.

- **Mieux vaut prévenir que guérir**

CONSEILS & SENSIBILISATION

- **Vous avez des questions ?**
  c’est bien de vous les poser avant de faire une bêtise,

- **Je n’ai sûrement pas toutes les réponses**
  car tous les jours surgissent de nouvelles menaces.

Merci pour votre attention
Gardez votre esprit en éveil