Protéger ses données

Pourquoi ?

Les objectifs des pirates informatiques :

- Atteindre les données à portée commerciale,
- Accéder aux données sensibles,
- Atteindre l'intégrité des chercheurs(ses).

Les conséquences :

- Perte de propriété intellectuelle et brevet,
- Perte de revenu potentiel,
- Contravention des lois et ou ententes sur la confidentialité des données,
- Perte de confiance envers le chercheur(se) ou son établissement.

Comment ?

1. Former les étudiants chercheurs
2. Utiliser l'authentification multi-facteurs (ex: reconnaissance faciale, empreinte digitale, code envoyé par téléphone)
3. Utiliser un mot de passe non répétitif et non utilisé sur d'autres plateformes
4. Utiliser des logiciels et services de sécurité (antivirus)
5. Faire des sauvegardes de données
6. Installer les mises à jour (permet d'éviter les vulnérabilités des systèmes)
7. Implémenter des contrôles d'accès

Attaques les plus répandues pour le vol de propriété intellectuelle

- Courriel de hameçonnage : courriel malveillant, souvent convaincant, qui incite à cliquer sur un lien qui télécharge un virus, permettant au pirate informatique d'accéder à votre ordinateurs et à vos données.
- Rançongiciel : une fois que le pirate a accès à vos données, au lieu de les voler, supprimer ou modifier – il chiffre les données et elles ne sont donc plus accessibles – jusqu'à ce que la rançon soit payée. Le pirate menace souvent également de rendre publiques les données si la rançon n'est pas payée.
- Attaque de l'intercepteur : les pirates peuvent intercepter les communications entre le routeur/serveur et votre ordinateur dans les lieux publics. Il est donc important d'utiliser des VPN.
- Menace interne : une personne ayant accès aux données et qui les utilise de manière inappropriée peut également représenter une menace. Il est donc important de retirer les accès aux personnes ne faisant plus partie du projet.
- Sécurité physique : les vols de données peuvent résulter d'une inattention concernant l'ordinateur physique et l'emplacement des données. Il est donc important de toujours verrouiller son ordinateur et de rendre inaccessibles les données par des tierces personnes.
- Usurpation d'identité : les empreintes en ligne (profil de médias sociaux, etc.) peuvent également être une source de perte de données.

Source : Ménard, V. (2021). *Sécurisez vos données contre les cybermenaces et le vol*. Colloque GDR 2021 de l'UQTR. Repéré à https://oraprdnt.uqtr.uquebec.ca/pls/public/docs/GSC6415/O0003253311_Presentation_Menard_Veronique.pdf