Méthodologie d’une attaque

Point définition : -méthodologie : Manière de procédé/méthode

-Attaque : exploitation des failles d’un système à des fins non connues

Partie II : Comment se protéger ?



En sachant que tout le monde peut être une cible d’attaque informatique, il est impératif de connaitre des moyens de nous protéger, cependant tout le monde ne peut accéder au même niveau de sécurité. En effet, on peut classer la sécurité des utilisateurs en deux groupes distincts : les actions d’un utilisateur classique et les actions d’un professionnel ou d’une entreprise.

D’un côté, Un utilisateur classique peut réduire drastiquement les probabilités de se faire pirater en contrôlant mieux le contenu qu’il partage : c’est-à-dire éviter de partager des photos ou informations privées (âge, adresse, numéro de tel, sécurité sociale, etc…).

Ensuite il doit aussi surveiller attentivement son nouvel environnement : c’est-à-dire diversifier et compliquer ses mots de passe, télécharger sur des sources sûre (site https ou avec cadenas), sauvegarder régulièrement, désactiver la géolocalisation, vérifier bien si le wifi qu’il utilise est bien celui de l’établissement dans lequel il se trouve (restaurant, hôtel, centre commercial).

En appliquant ces conseils, un pirate aura plus de mal à s’infiltrer dans son réseau et ses différents appareils (smartphone, smartTV, tablette, ordinateur, etc…)

De l’autre, les professionnels ou entreprises ont beaucoup plus de connaissance et de ressource dans ce domaine. Par conséquent, un professionnel peut mettre en place d’autre type de solutions, en plus de celle déjà évoquée : configurer les règles de pare-feu et des systèmes de détection, s’assurer que les équipements informatiques soient à jour, chiffrer le trafic Wifi ou restreindre l’accès.

Une entreprise elle peut de son coté, boucher les failles d’un système ou le refaire si nécessaire et former les nouveaux employés déployer une solution de filtrage Web et isoler le réseau d’invités.