Différents types de Cyberattaque.

Voici les plus fréquents types de Cyber attaques :

Pour les particuliers

- le cyber harcèlement via les réseaux sociaux.
- la cyber fraude (triche aux examens, faux diplômes, falsification de documents officiels, etc.) ;
- la cyber contrefaçon (musique, livre, jeux-vidéo, logiciels) et le cybermarché noir (achat en ligne de marchandises illégales)
- la cyber usurpation d'identité
  Exemple : 1 - Se faire passer pour un intermédiaire agréé de EDF pour vous vendre des panneaux solaires.
  2 - Créer un site Web Ayant le même nom qu'un site Web connu mais avec une terminaison différente. Remplacer .fr par .com (voir : Carglass, Comme-Jaime etc..) ou le même nom avec une orthographe légèrement différente. En se servant des Ads de Google on peut se faire voir sur Internet avant le site officiel. (Ce qui oblige le propriétaire légitime du site à surenchérir dans les Ads donc à enrichir google).
- la Désinformation en modifiant l'apparence d'un site, d'un blog, etc.. Propagation des Fake New (informations mensongères) pour nuire à une personne ou une entreprise. Mais aussi la désinformation en propageant des informations tronquées ou sorties de leur contexte.
  (Dans ce dernier cas la désinformation ne fait guère mieux que la télévision actuelle.)

Pour les entreprises

- les attaques par déni de service (DoS) (visant à neutraliser un système informatique et à le rendre inopérant) ;
- le cyber cambriolage (vol de données)

  Voir la page : « Cours8_18 »
- L'arnaque au président (Cours 8-19)
- Les Ramsomwares.
  Cette attaque modifie tout ou partie de votre disque dur avec une clef de cryptage sophistiquée. Et on vous demande de payer (une rançon) pour que vous puissiez récupérer vos data. C'est une attaque qui vise la plupart du temps les serveurs des grandes entreprises surtout celles qui utilisent le Cloud Hybride.

Certaines fraudes touchent autant les entreprises que les particuliers comme la fraude aux petits montants. (Cours 8-20)

Les Objectifs des cybercriminels

Les objectifs des cybercriminels peuvent être variés mais sont en très large majorité lié au profit financier.

Le profit

L'objectif principal d'un cybercriminel est de faire du profit, par exemple, subtilisant des données à un utilisateur ou une entreprise pour les revendre ou lui rendre contre rançon. En présentant de faux diplômes ou de faux certificats de travail pour obtenir un nouveau travail. Parmi les nombreuses méthodes d'arnaque en ligne, le phishing, ou "hameçonnage", reste la plus répandue auprès des particuliers et elle consiste à se faire passer pour un tiers de confiance afin de soutirer les informations personnelles d'une entreprise ou d'un particulier. Les victimes peuvent recevoir un mail frauduleux les invitant à cliquer sur un lien, puis elles sont contactées par téléphone pour prendre rendez-vous. Cela crée une relation de confiance quand le commercial passe chez vous pour vous vendre des panneaux solaires ou une pompe a chaleur.

Mais cela peut être une attaque part « Deny of Service » (Dos) d'une entreprise. Ou seulement des « fake News » tendant à discréditer un produit ou une entreprise. Ceux qui font ceci étant rémunéré par leurs concurrents. (Prendre en exemple la guerre sur les jeux internet).

Motivation économiques, politiques, sociales, militaires.

La Cybersécurité est fondamentale pour lutter contre les attaques qui ont des motivations politiques, sociales ou militaires car ce sont celles qui bénéficies de beaucoup plus de moyens logistiques. On trouve dans ce cas-là souvent des attaques par « Deny of Service » (DoS) sur des entreprises, des administrations ou autres. On passe ici à un autre niveau de Cyber attaque. (Attaque avec des « bootnet ».