

Introduction à la cybersécurité

BTS SIO 1ere année

# Les débuts de la cybersécurité

Dès le début d’internet, les virus ont commencé à voir le jour de manière plus importante. Mais comme le parc machine était encore mince, la probabilité d’une attaque était presque nulle pour les particuliers et les petites entreprises.

Ensuite, dans les années 90 et au début des années 2000, la sécurité informatique se résumait souvent à :

• Installer un antivirus : Pour éviter qu'un virus ne ralentisse ou bloque ou encore supprime les données de nos ordinateurs.

• Installer un firewall : Pour les sociétés, afin de bloquer les échanges non autorisés sur Internet, en interdisant la communication sur une partie des ports, en entrée comme en sortie. Eh oui, le fait d’aller sur internet était à l’époque considéré comme une distraction.

• ... et voilà…

Le premier antivirus date de 1987 et s’appelait VirusScan de la société McAfee. Auparavant, les virus informatiques n'était même pas une préoccupation.

La cybersécurité était simple. Internet démarraitet les données étaient rarement dématérialisées, sauf certaines sauvegardes.

# La cybersécurité aujourd’hui

Le monde d’aujourd’hui est hyperconnecté. Presque tout est géré en ligne ou peut l’être. On gère ainsi des accès à l’électricité, aux hôpitaux, à son domicile.

Les attaques informatiques ont évolué. Maintenant les hackers ont développé de multiples types d’attaques, les virus ont une nouvelle branche, les ransomwares. Avec eux, vos données sont cryptées et vous ne pouvez les récupérer qu’en payant une rançon. Les brèches de données sont aussi plus nombreuses, et engendrent des pertes massives de fichiers confidentiels, revendus ensuite sur le darkweb.

On estime qu’en 2017, 2 milliards de données personnelles ont été volées.

Le gouvernement français a mis en ligne une page d'information sur les risques, qui sont regroupés en 4 catégories :

• Cybercriminalité : Le plus souvent avec motif pécunier.

• Atteinte à l'image : pour décrédibiliser une personne ou un groupe.

• Espionnage : pour récupérer des informations secrètes.

• Sabotage : pour déclencher une panne, un incident.

En 1997, la première valeur de l’entreprise était son capital immobilier et mobilier. Aujourd'hui, ce sont les données (brevets, fichiers clients, recettes…).

Très peu des entreprises sont préparées à un risque cyber (environ un tiers). Une brèche de données coûte en moyenne 3,5 millions d’euros à une entreprise.

# Quelques exemples

Equifax est une société américaine qui évalue les personnes et les sociétés pour les obtentions de crédit. Si vous avez une bonne note avec Equifax, la banque vous accorde un crédit. Pour ce faire Equifax stocke les informations personnelles et confidentielles de millions de personnes et de sociétés. Les données archivées sont du type Nom, Prénom, date de naissance, N° de sécurité sociale, N° de carte de crédit, ...

Mi-2017, un oubli de patch du framework Java Struts chez Equifax a engendré un piratage et le vol de données personnelles de 150 millions d’américains.

Aux Etats Unis, le N° de sécurité sociale est LA donnée qui caractérise un individu. Donc, une personne qui récupère l’identité et le N° de sécurité sociale associé peut ouvrir un compte en banque, avoir un crédit, … Que la personne volée devra rembourser, ou prouver qu’elle a été victime du vol de son identité.

WANNACRY

Windows XP est un système sorti en 2001 et dont le support par Microsoft s’est arrêté en 2014. La NSA avait trouvé une faille qui figurait encore dans l’exploitation du système, mais l’avait tenue secrète. En 2017 les hôpitaux du Royaume -Uni utilisaient encore Xp car leur logiciels étaient adaptés à ce système, et n’avaient pas envisagé de le changer, comme plusieurs centaines de millions d’utilisateurs dans le monde. La NSA s’étant fait pirater, la faille de sécurité est passée chez les hackers. Le Ransomware Wannacry a bloqué environ 230 000 PC dans 150 pays. L’attaque a commencé massivement le 12 mai 2017. Au Royaume-Uni, les hôpitaux ont été touchés, et ont dû repasser en urgence à un traitement « papier » avec tous les risques d’erreurs associés.

La rançon était demandée en bitcoin, intraçable.

# Les types d’attaque

## Les failles logicielles

Les failles logicielles sont des bugs logiciels. Il y en a dans tous les logiciels, des systèmes d'exploitation Windows, Linux, Android... aux logiciels comme Skype, Word, Excel, Chrome, Firefox, ...

Les impératifs économiques et la façon de coder impliquent que le risque zéro n’existe pas. A la base, tout logiciel est faillible.

Pour remédier à cela, des campagnes de tests sont menées, ainsi que la prise en compte des retours utilisateurs. Des correctifs sont ainsi proposés régulièrement, dès qu’une faille est détectée et que son correctif est prêt. Il convient donc de maintenir à jour les logiciels le plus souvent possible.

## Les failles réseau

Les failles peuvent aussi venir de faiblesses au niveau du réseau.

Par exemple, un wifi non chiffré peut contenir des cookies, avec des données d’authentification. Les serveurs installés par une société extérieure qui oublie de personnaliser le mot de passe chez le client et on se retrouve avec admin/password par défaut.

Il faut utiliser un chiffement des mots de passe fort, et les faire varier.

## Les droits d'accès

Il faut donner un accès au juste nécessaire aux données. Tout le monde n’a pas à avoir les codes du serveur de messagerie, ou les clés de l’armoire de brassage. Après tout, vous ne donnez pas vos clés de maison à vos collègues.

## L'ingénierie sociale

Ici il s’agit de tromper les gens en les forçant à vous donner leur mot de passe. Et c’est plus facile qu’on pourrait le penser.

Souvent, au téléphone, le pirate joue sur l’urgence de la chose. On peut également avoir affaire à un faux site internet, recevoir un mail qui vous demande vos coordonnées bancaires, …

Souvent les attaques de ce type étaient grossières, bourrées de fautes d'orthographe, avec un aspect visuel différent du site ou du logo officiel, avec une adresse mail chez un fournisseur générique (Hotmail, Gmail, ...). Maintenant, les attaques sont beaucoup plus ciblées. Elles peuvent se référer à une personne réelle, dont les coordonnées ont été prises sur un site.

Par exemple, vous êtes chercheur d’emploi, et on peut vous trouver sur internet par le biais de sites spécialisés. Vous êtes contacté pour un petit travail par Monsieur X, société Y. Si vous allez vérifier sur internet, vous voyez que Monsieur X est le Directeur de la société Y, donc à priori une personne de confiance. Sauf que ce Monsieur X et sa société ne vous ont jamais contacté. Le pirate, lui, va continuer en disant qu’il vous apporte un colis, que vous devez traiter, par exemple mettre sous plis des prospectus. Comme il vous confie du matériel, il vous demande de le payer. Il vous remboursera ensuite en venant chercher les prospectus dans les enveloppes et vous paiera aussi pour votre travail. Si vous êtes crédule, vous payez, et en ouvrant le carton, vous voyez un tas de vieux prospectus. Et ensuite, en téléphonant au véritable Monsieur X, vous vous apercevez de la supercherie. Il faut avoir conscience que ce type d’attaque existe.

L’attaque commence par le biais de l’informatique et se poursuit au domicile. C’est une combinaison de différentes supercheries.

C’est également le cas pour Equifax, qui avait une faille logicielle non patchée, en plus de droits d'accès trop ouverts.

On retrouve sur le site de l’ANSSI, une plaquette dédiée aux métiers de la cybersécurité :

https://www.ssi.gouv.fr/particulier/formations/panorama-des-metiers-de-la-cybersecurite/