# La sécurité: matériels et logiciels

## L'Internet

Si l'Internet est un endroit où on peut trouver tout ce qu'on veut, on y trouve aussi ce qu'on ne veut pas, et les états et les criminels ont développé au fil des ans des moyens sophistiqués d'en profiter et de voler les données, les biens et même la réputation des internautes.

## Menaces

Virus, ver, cheval de Troie, ransomware, rootkit, logiciel malveillant, faux antivirus, phishing, scanneur de ports, enregistreur de frappes au clavier, prise de contrôle à distance, etc. la liste est longue et s'allonge au fil du temps.

Ces dernières années l'utilisation de techniques d'ingénierie sociale s'est beaucoup développée. Elles consistent à leurrer l'utilisateur en utilisant ses faiblesses, envie de posséder, croyance aux contes de fées, etc.

La constitution des réseaux d'ordinateurs zombis, les botnets, permet au crime organisé de monnayer ses services auprès d'acteurs tout à fait légaux.

## Virus

Un virus est un programme ou un morceau de code qui se reproduit en infectant un autre programme, un document ou un secteur de démarrage.

Un ver est un virus qui se reproduit lui-même, en général il est invisible par le système d'exploitation. Il est découvert par la place ou les ressources qu'il consomme. Il se répand en s'expédiant lui-même ou dans un fichier attaché à un courriel.

Un cheval de Troie est un virus qui n'est pas actif immédiatement et qui devient actif plus tard. Souvent il ouvre un port sur l'ordinateur qu'il infecte, se connecte à un agent extérieur et télécharge d'autres virus.

Un rootkit est un virus qui permet un accès privilégié à l'ordinateur ou au réseau. Il fusionne avec le système d'exploitation, ce qui lui permet de mener son activité de manière furtive et donc de cacher l'intrusion d'un attaquant.

Les virus modernes combinent souvent plusieurs de ces aspects.

## Logiciel espion et logiciel malveillant

Les logiciels espions comportent tous ceux qui enregistrent les données de l'utilisateur sans qu'il le sache: les enregistreurs de frappe au clavier, les voleurs de mots de passe, les enregistreurs de profil de navigation, etc.

Le phishing est une technique pour amener l'utilisateur à divulguer son nom d'usager et son mot de passe, ou son PIN, sur un site spécialement agencé dans ce but, ressemblant à s'y méprendre à un portail officiel de banque, par exemple.

Les dernières tendances montrent le développement de faux antivirus qui font du racket (ransomware) directement. Ils fondent leur modèle d'affaire sur le fait que quelques personnes paieront sur un grand nombre d'infections.

## Vol de renseignements personnels ou d'entreprise

Il faut bien comprendre que les activités nuisibles dans l'Internet ne sont plus seulement l'affaire de quelques nerds en mal de reconnaissance – il y en aura toujours bien sûr – mais sont devenues l'affaire du crime organisé. En conséquence ces activités ont pris le caractère d'une véritable industrie qui vend ses services et les renseignements volés, et participe de la guerre économique entre les entreprises, voire les États, comme les récents vols de comptes chez eBay et l'espionnage par la NSA et les services secrets de différents pays.

## Réponses

Que faire? Il faut garder une attitude méfiante envers les courriels provenant d'inconnus, et envers les documents attachés dont on ne peut voir l'extension. Il faut aussi rester en éveil vis-à-vis de comportements inhabituels de l'ordinateur ou de ses contacts.

Il est très important d'utiliser un parefeu, en général logiciel, qui va filtrer les communications entrantes et sortantes avec l'Internet. Il permet aussi de cacher les ports de communication et donc le PC d'observateurs extérieurs et surtout des programmes automatiques qui scannent ces ports.

Des programmes de détection des intrusions existent pour compléter cette défense. Encore mieux, on trouve des programmes de prévention d'intrusion.

La plupart des antivirus actuels comportent des moyens de combattre à peu près tous les types de virus et de malware. Certains sont très complexes et grèvent la performance de l'ordinateur. Les antivirus gratuits ne sont pas plus mauvais que les payants : on paie pour l'automatisation des processus et la simplicité de la configuration du logiciel.

Il ne faut pas installer deux antivirus différents sur un PC car ils peuvent entrer en conflit l'un avec l'autre et faire geler l'ordinateur.

Ces programmes souffrent d'un handicap par rapport aux fabricants de virus : ils sont toujours en retard par rapport à eux. Des antivirus différents ont des façons différentes de repérer les virus.

La prolifération des smartphones et des tablettes a entraîné celles des menaces qui s'attaquent à ce genre d'ordinateurs. La plupart des fabricants d'antivirus ont donc développé des programmes adaptés à la technologie mobile.

## Quelques mesures protectrices

La première, c'est d'ouvrir une session protégée quand on se logue à l'ordinateur, de façon à ce qu'un virus ne s'installe pas automatiquement. Les meilleurs mots de passe ont une longueur de 12 à 14 lettres et sont composés de deux mots qui n'ont aucun rapport entre eux, mais qui ont du sens pour l'utilisateur, et on peut y adjoindre des chiffres et certains caractères spéciaux. Certaines politiques d'entreprise obligent à former ces mots de passe de manière très codifiée et avec des contraintes dont il faut tenir compte.

Une autre mesure de sécurité consiste à vider régulièrement les dossiers des fichiers temporaires dans Windows (C:\Windows\Temp) et dans les répertoires personnels des utilisateurs (C:\Users\nom de l'utilisateur\Appdata\Local\Temp) et l'historique de navigation des fureteurs.

## PC

La meilleure façon consiste donc à installer un antivirus, et à scanner régulièrement l'ordinateur avec un scanneur en ligne d'une marque différente.

L'Internet offre une ressource à ne pas négliger : les secours d'informaticiens qui inventent ou perfectionnent des moyens de défense. Il faut bien sûr être prudent.

## Entreprise

L'entreprise dispose de matériels et de logiciels sophistiqués et coûteux pour sa défense : parefeux et appliances, routeurs gérés pour les matériels, et surtout infrastructure avec des domaines, comme Active Directory, logiciels de prévention et de détection d'intrusion, pour les logiciels. Ces programmes sont utilisés d'une manière spéciale sur les serveurs.

Tout ce qui est valable pour un ordinateur de particulier reste valable pour un ordinateur dans l'entreprise.

## Sauvegarde des données et de l'ordinateur

Malgré toutes les précautions toutes ces menaces peuvent endommager les données et l'ordinateur lui-même. Ça nécessite le besoin de créer des sauvegardes régulières qui maintiendront leur intégrité et permettra de les ramener à leur place.

Les sauvegardes peuvent se faire manuellement ou à l'aide de logiciels.

- Xcopy, robocopy
- Historique des fichiers à partir de Windows 8 et les versions suivantes
- Les solutions intégrées avec l'antivirus

Les différents types de sauvegarde sont la copie simple, la sauvegarde quotidienne, la sauvegarde totale, différentielle et incrémentielle.

La validité des supports, la vérification de la sauvegarde et la restauration des fichiers sont importants.

## Mises à jour de sécurité de tous les logiciels

Les mises à jour de sécurité ne concernent pas seulement Windows, mais aussi une foule d'autres logiciels courants, comme par exemple Office, Adobe Reader, tous les fureteurs, les logiciels de courriel, de messagerie instantanée, etc. Il convient de les mettre à jour aussi.

- Windows Update, Microsoft Update, Browsercheck

## Outils importants

https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

## Scanneurs en ligne

https://housecall.trendmicro.com/