Protection et anonymat informatique

Synthèse des meilleures pratiques

Il est absolument **impossible d'être protégé contre 100% des attaques** informatiques. Néanmoins, on peut s'en rapprocher. De plus, il ne faut pas oublier que c'est souvent le **facteur humain** qui permet l'installation de virus, trojans, etc.

Sécurité matérielle

Il est recommandé d'utiliser un ordinateur fixe afin d'en **contrôler tous les composants**. En effet, il peut être possible qu'un composant soit espion (placé par exemple par la NSA) et déjà implémenté dès l'achat de son matériel…

De plus, cela permet de changer et de mettre à jour régulièrement ses composants sans racheter tout un ordinateur, ce qui est moins cher.

Des virus à accès physique existent également, comme des keyloggers ou des stealers USB. Il faudra donc **vérifier régulièrement que rien de suspect ne soit branché** ainsi que de **ne pas connecter de clés USB ou disques dur qui ne vous appartiennent pas** sans passer par une machine virtuelle. Il faut comprendre que pirater quelqu'un grâce à un accès physique est bien plus facile que par Internet.

En effet, il y a peu est apparu dans les actualités une histoire de clés USB reçues par des personnes dans leur boîte aux lettres. Par curiosité, elles les ont évidemment connectées à leur ordinateur, ce qui les a immédiatement infectées.

Exemple de protection possible pour un professionnel

J'avais demandé à un photographe de me donner une copie informatique de sa photo en la mettant sur ma clé USB. Au lieu de brancher directement ma clé sur son ordinateur, il l'a connecté à une borne pour le faire. Cela lui permet donc de ne pas craindre d'être infecté par les clés USB des clients.

Enfin, si vous avez un ordinateur portable, **cachez votre webcam avec du scotch opaque et calfeutrez votre micro** au cas où l'on vous piraterait. Si vous avez un ordinateur fixe, débranchez la prise de ces périphériques quand vous ne vous en servez pas.

Sécurité générale

Utilisez un anti-virus. D'après la CIA, suite aux révélations par Wikileaks de Vault 7, **Bitdefender** serait très performant contre les menaces, contrairement à Kaspersky et particulièrement F-Secure qui serait "un produit bas de gamme qui présente une difficulté minimale".

Tenez votre antivirus à jour pour avoir les nouvelles menaces détectées. N'en utilisez pas deux, c'est inutile et peut amener à des conflits logiciels. Faites aussi régulièrement des scans de sécurité.

Tenez vos programmes à jour pour éviter l'exploitation de failles (Cependant, prendre garde car il peut être possible que ce soit la nouvelle version qui soit exploitable, cela s'est déjà produit…)

Changez d'adresse IP et d'adresse MAC afin d'éviter d'être tracé. Ces adresses permettent respectivement de localiser et d'identifier la personne de manière unique. Normalement, l'adresse MAC n'est connue que par notre box Internet, cependant il est possible qu'elle soit tout de même envoyée sur le réseau.

Faites attention à votre user agent, cela peut également contribuer à vous identifier. **Il vaut mieux avoir une whitelist** et bloquer toutes les autres requêtes **qu'avoir une blacklist** et tenter de bloquer les requêtes malveillantes.

Fichiers

Utilisez un programme spécifique pour **BIEN supprimer vos fichiers en écrivant par dessus plusieurs fois de suite**. En effet, quand on supprime des fichiers, en réalité ils sont toujours sur le disque dur, seul leur emplacement est retiré de l'index des fichiers. Ainsi, un jour le système écrira à cet emplacement les nouveau fichiers mais il est aussi possible que cela ne se fasse jamais… et donc que l'on puisse récupérer les fichiers "effacés".

Ne pensez donc pas à tort que simplement effacer un fichier le supprime. Pour éviter que les personnes aux outils informatiques développés y accèdent, détruisez le disque dur ET les restes de celui-ci. Le cas des SSD est plus difficile car c'est une mémoire flash et non un disque en rotation comme les HDD.

Pour la désinstallation de programmes, il restera toujours des fichiers. On pourra par exemple utiliser Revo Uninstaller pour bien désinstaller ses programmes sur Windows.

Prenez garde aux **données Exif** des photos que vous transmettez qui peuvent vous trahir. Ces informations invisibles contenues dans les documents renseignent sur l'appareil utilisé, la localisation, etc. Pareil pour les autres documents comme les documents Word qui contiennent le nom de l'auteur et la date de création.

Sécurité du navigateur

Désactivez les cookies ainsi que l'historique. Ne sauvegardez aucun mot de passe sur le navigateur car **un simple stealer peut les récupérer**. (À la limite, s'il le faut, protégez alors votre liste de mots de passe enregistrés par un mot de passe principal).

Pas d'add-on, ne pas ouvrir directement ses fichiers téléchargés mais plutôt dans une machine virtuelle non connectée à Internet.

URLs

- ➢ Attention aux URLs des sites pour le phishing…
- ➢ Prendre garde au phishing par URI, c'est-à-dire que le code source de la page est directement dans le lien.
- ➢ https : quand c'est sécurisé par SSL (ou son évolution TLS).

Réglages Firefox

- ➢ Bloquez les trackers (HTTP Referer) qui disent au site de là où l'on vient : Taper dans le champ URL

"about : config" puis "network.http.sendRefererHeader" et mettre sur 1 au lieu de 2.

- ➢ Bloquez tout le javascript en utilisant Noscript. Attention, enlevez les exceptions en liste blanche pour bien être sûr. Pour être certain : aller dans le champ URL et taper "about:config". Ensuite taper "javascript.enabled". Double-cliquer pour mettre la valeur sur False.

Vie privée

Si possible, ne rien poster sur Facebook ni sur d'autres sites. **Tout ce qui est posté sur internet est impossible à effacer**. Par exemple avec les archives de l'Internet Archive (archive.org/web), la mise en cache ou encore le téléchargement du contenu par certains utilisateurs. Dans l'idéal, utiliser un pseudo différent pour chaque site, associé à une adresse mail différente.

- ➢ Ne pas communiquer sur des plates-formes non sécurisées comme Facebook Messenger…
- ➢ Se déconnecter de Google pour les recherches car tout l'historique est enregistré. Utiliser un autre navigateur, voire un métamoteur de recherche.
- ➢ Crypter ses données.
- ➢ Machine virtuelle/Sandbox pour les fichiers louches. Les scanner sur Virus Total.
- ➢ Adresse mail spécifique + avec PGP.

L'adresse IP

Elle sert à reconnaître un utilisateur sur Internet. Cependant, les personnes se connectant à la même box Internet auront la même adresse IP, ce qui **ne permet donc pas une identification unique**. Les habitants d'une même maison ont ainsi la même adresse IP mais peuvent être reconnus par une adresse unique sur le réseau local. C'est l'**adresse MAC** qui les différenciera pour l'envoi des données venant d'Internet.

Des services peuvent être indisponibles pour des IP spécifiques, comme regarder des contenus vidéo sur des sites américains, etc. Il suffira de **changer d'IP** pour une américaine afin d'y accéder.

Il est très facile de récupérer une adresse IP, mais **on ne peut pas faire grand chose avec**. On peut : **localiser approximativement** la personne, **la DDOS**, déterminer si elle a créé plusieurs comptes. Pareil pour le bannissement, on peut vérifier si votre adresse IP se connecte au site et ainsi bloquer l'accès si elle n'est plus autorisée.

Il est facile de récupérer une IP, mais elle ne sert à rien si elle a été modifiée, notamment à l'aide de l'un des moyens ci-dessous. Avec une vraie IP, si la personne est connectée à son réseau internet domestique, on peut la localiser. Mais si le réseau est un réseau téléphonique tel que le réseau 3G, c'est impossible.

Trois solutions possibles pour masquer son IP et en utiliser une autre

- Utiliser un proxy (sorte de VPN mais que pour le navigateur).
- Utiliser un VPN (Plus conseillé que proxy car des données transitant par l'ordinateur peuvent révéler votre vraie IP. Cela irait plus vite que les proxies et serait plus sécurisé).
- Utiliser Tor Browser. Possibilité de failles 0day : donc coupler avec un VPN si réelle volonté d'être anonyme, sinon c'est suffisant pour la plupart des usages… Utiliser un VPN en plus de Tor !**IMPORTANT**! Obligé de payer ou de s'en créer un car : D'après vous, d'où vient la gratuité des VPNs gratuits… ?

À vérifier : redémarrer la box pour changer simplement d'adresse IP ?