Bloc 3: TP 1 – Respect des bonnes pratiques

Travail à réaliser :

1. Présentez à vos utilisateurs les formats de fichiers qui peuvent être dangereux sur un PC (Windows, Linux, Mac), sur un smartphone ou une tablette (Android, IOS).
2. Déterminez si des formats de fichiers sont plus dangereux que d'autres. Argumentez.
3. Y a-t-il des sources plus sûres que d'autres ? Explicitez avec des exemples.
4. Comment allez-vous inciter vos utilisateurs à se protéger des menaces informatiques, dans notre cas d'un rançongiciel.
5. Vos utilisateurs vont certainement vous prendre pour un « parano ». Comment allez-vous démontrer que ces mesures peuvent être vitales pour le bon fonctionnement de l'entreprise ?

---

1. Sur un PC sous Windows/Linux :

Les fichiers programmes (.exe, .dll, .sys), *les fichiers de commandes* (.cmd et .bat).

Des macros incluses dans des fichiers Microsoft Word (.docx) ou bien aussi le fichier en .txt

Des fichiers de script dans Microsoft Access (.mdb)

 Des fichiers avec macro sur Microsoft Excel (.xls/.xlsx)

 Des fichiers PDF

 Des fichiers en .zip

 Des fichiers en .iso/.img

 Des fichiers multimédias en .wma/.wmv/.mkv/.mp3/.mp4

 Des fichiers en .htm/.html

 Des fichiers de scripts en .js/.vbs

<u>Concernant les smartphones/tablettes (Android, IOS) :</u>

 Le format .apk sous Android (si l'on télécharge en dehors du store Google Play ou autres alternatives officiels)

Des fichiers en .ipa (si télécharger en dehors de l'App Store)

2. Il existe des formats de fichiers qui sont plus dangereux que d'autres dû à leur fréquence d'utilisation par les cyberpirates.
   Pour ce faire, nous allons voir des attaques informatiques qui ont été très impactante pour les entreprises/utilisateurs.

   Le cheval de Troie Locky : Ce rançongiciel est apparu en 2016, il a pour particularité d'être caché dans un document Word (.docx) prenant la forme d'une facture. Une fois le fichier ouvert sur votre ordinateur, Locky va crypter toutes les données et demander de payer une rançon pour les récupérer.

   GoldenEye : celui-ci est une combinaison de virus qui délivre des courriels avec une fausse offre d'emploi avec du texte en allemand ainsi que deux fichiers joints. Le premier est un faux CV, l'autre est un fichier Microsoft Excel (.xls) malicieux. En effet comme Locky, une fenêtre apparaîtra (pop-up) demandant d'activer les macros. Alors, le fichier génèrera un exécutable et le rançongiciel se lancera.

   Emotet : attaque qui vise à infecter des boîtes mails afin de récupérer les données présentes sur l'ordinateur ou bien le réseau. Celui-ci se présente sous la forme d'une pièce jointe qui est souvent un document Word (.doc) représentant aussi une facture comme Locky.

   En sommes, nous pouvons voir une récurrence dans les formats de fichiers notamment Microsoft Word avec les formats ".doc" et ".docx" qui sont majoritaires mais aussi d'autres tels que le ".PDF" ou bien Microsoft Excel avec le ".xls".

3. Il existe des sources de format de fichiers considérés comme plus sûr que d'autres tels que :

   - Le format .txt (impossible de créer du code dedans)
   - Le format .png (pas d'exécution de code)
   - Le format .wav/.flac (aucune exécution de code)

4. Il est important de rappeler les conséquences qu'un rançongiciel pourrait provoquer que ce soit en interne par le management et en termes de coûts financiers pour l'entreprise. Je rappellerai dans un premier temps, au cours d'une réunion de sensibilisation, l'accessibilité aux données personnelles pouvant compromettre les salariés eux-mêmes, ce qui les touche de prime abord sera pris avec plus de sérieux.

   Il est important de rappeler régulièrement par le biais d'affiche de sensibilisation dans l'entreprise, comment cela peut-il se produire ainsi que les potentiels conséquences possibles pour les salariés, les clients ainsi que l'entreprise. (Exemple d'affiches : https://www.cybermalveillance.gouv.fr/medias/2019/02/kit_complet_de_sensibilisation.pdf).

   Il est important de créer des ateliers de formation à la cybersécurité afin de faire comprendre visuellement l'impact d'une mauvaise manipulation et de ce que cela peut engendrer sur l'entreprise, de ses salariés et de ses clients. De plus, cela permettra de développer des nouvelles compétences pour ces dits salariés.

   Le concept de **BYOD** ("Bring Your Own Device") a pour intérêt de ramener son propre outil informatique dans lequel le salarié est habitué et dont il maîtrise l'usage. Celui-ci peut s'avérer utilise dans le cadre où des règles au préalable ont été fixé entre le salarié et l'entreprise.
   Le **CYOD** ("Choose Your Own Device") permet aux collaborateurs de choisir

leur appareil parmi une liste préétablie. L'entreprise paie les frais nécessaires, contrôle les mises à jours et l'installation des applications. Pour le salarié, celui-ci bénéficie d'un matériel qui lui convient.

Concernant des solutions plus concrètes permettant de protéger son environnement numérique, il faut toujours penser à avoir un antivirus, une solution permettant de filtrer les fichiers dangereux sans qu'ils ne peinent à arriver dans la messagerie comme le logiciel **MimeCast Advanced Email Security CG**, de mettre à jours régulièrement le système ainsi que ses applications.

5. Il est toujours bon de rappeler qu'un rançongiciel est à but monétaire pour le cyberpirate.
   Ainsi, en chiffrant les données, celui-ci pourrait compromettre l'intégrité financière de l'entreprise mais aussi de compromettre les données à caractères personnelles des salariés, des clients, etc...
   Leur rappeler que ce genre de conséquence pourrait être très grave pour eux (perte d'emploi car coût financier exorbitant ou bien du danger de voir leurs informations circuler à des buts malicieux par exemple).
   D'une paralysation du travail pendant une durée indéterminé (indexé par rapport à la gravité des données compromis et de la dernière backup effectué par le service informatique).