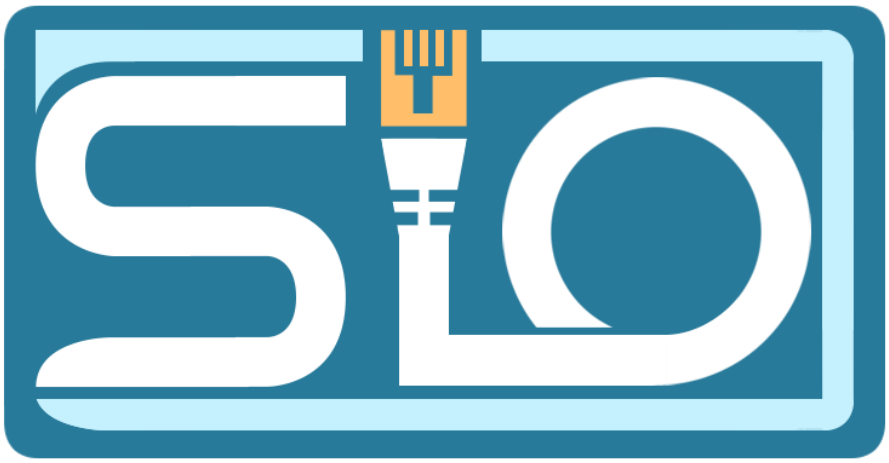
Grzesinski
Thomas

21/09/2023
Mr Fenetre

TS1SIOTP1– Respect des bonnes pratiques



SOMMAIRE

Chers salariés suites à la suite d'une récente attaque de rançon logicielle, votre entreprise m'a contacté pour vous faire une sensibilisation de cybersécurité, en effet les dangers sont de plus en plus nombreux ont peut allez a de simple mail qui contiennent des fichiers avec des logiciels malveillants qu'on appelle plus communément en informatique des MALWARE.
Le monde du travail a aussi privilégié le télétravail depuis le Covid-19, et ceci est très bénéfique pour les blacks hats (nom en anglais pour désigner les hackers malveillants) qui peuvent facilement accéder a vos données d'entreprise depuis le poste que vous vous connecté chez vous et donc récupérer des informations et des données qui ne sont pas censé être divulgué.

Donc tout d'abord essayons de voir quels sont les enjeux du télétravail d'un point de vue avantageux pour les salariés et les employeurs, mais aussi les risques potentiels.

Pour les salariés on a des économies de temps notamment celui passé dans les transports, une meilleure gestion du temps de travail, une plus grande autonomie du gestion des tâches, une meilleure concentration entrainant une meilleure productivité, un meilleur équilibre vie personnel-vie professionnelle.

Pour les employeurs c'est donc d'accroître la production, de réaliser des économies d'échelle sur les locaux et les dépenses courantes,

d'améliorer des plages horaires durant lesquelles l'employeur peut habituellement contacter le salarié en télétravail, les modalités d'accès des travailleurs handicapés à une organisation en télétravail.

Mais parmi ces nombreux avantages il y a aussi des risques, en effet nous avons :
-Les salariés qui se connectes avec leur appareil personnel au SI de l'entreprise. Cette pratique présente des risques si ces terminaux n'emportant pas le même niveau de sécurité que les appareils fournis par l'employeur.

-Le phishing est une méthode d'attaque informatique visant à tromper les utilisateurs pour leur soutirer des informations personnelles telles que les mots de passe ou des numéros de carte de crédit, les attaquants se font passer pour une personne de confiance ou de l'entreprise souvent par mail ou un faux site web pour y voler des données sensibles ou personnels.

-Se connecter avec son réseau internet personnel ou Wifi publique qui n'est généralement pas sécurisé fait partit des risques.

-Mauvaise configuration dans le cloud public risques de laisser passer des connexions non voulues

-Le piratage de webcam et Zoombombing, des gens arrivent à entrer dans des vidéos conférence et y publie des choses non voulue.

I) Comment reconnaître un fichier dangereux

Donc bien évidemment je vais donc vous montrer maintenant comment essayer de reconnaître et de repérer les formats

fichiers dangereux et les dangers qu'ils peuvent occasionnés pour vous, votre PC ou encore votre entreprise.

Tout d'abords nous avons les formats de fichiers Windows.

-LE premier format de fichier fait notamment aussi partit des plus connus sur Windows, c'est le format .EXE, en effet ce format de fichier contient un programme exécutable qu'on peut facilement exécuter en double-cliquant sur le fichier.
Le danger de ce genre de fichier, c'est qu'il est facile pour les utilisateurs malveillants de faire une attaque de malware, une attaque de **malware** en gros c'est un programme malveillants conçus pour s'introduire dans les ordinateurs et autres dispositifs connectés afin de voler vos informations personnelles.

-Le second format de est le format de fichier **.COM**, il est similaire au format ficher .EXE, mais il est enregistré dans un format binaire.
Les dangers de ce genre de format c'est qu'ils sont généralement exécutés pour un ensemble d'instructions, si elle contient des logiciels malveillants et est ouvert les instructions seront donc exécutées pour endommager votre ordinateur.

-Les formats de fichiers **.BAT** est un fichier batch DOS qui est utilisé pour exécuter des commandes dans l'invite de commande Windows, les fichiers BAT sont généralement utilisés pour lancer des programmes et exécuter des utilitaires de maintenance Windows.
Donc forcément le danger ici est que comme les fichiers .BAT sont des séries de commandes qui se dérouleront si elle est ouverte, l'hacker malveillant pourrait donc s'introduire dans votre système informatique

-Le quatrième format de fichier est le format .**CMD**, un fichier .CMD est un fichier de commande utilisé par Windows, il est similaire au fichier .BAT.
Ce genre de format de fichier est très populaire pour les logiciels malveillants.
Généralement on l'utilise pour supprimer les données dans un répertoire ou bien alors on reproduit les données/on ouvre un programme à plusieurs reprises épuiser les ressources du PC pour faire en sorte qu'il ralentit et bloque le système. On appelle cela un **forkbomb**.

-Le fichier **.MSI** est un package d'installation Windows qui contient des informations d'installation pour un particulier. Le danger est que les .MSI sont généralement fiable et utilisés pour l'installation de logiciels, donc cela est facile de créer .MSI avec un virus dedans et que la personne l'installe sans douter du contenu du fichier.

Le format .WS/.WSF sont des fichiers de fenêtres de script, ils contiennent des scripts exécutables qui utilisent le code JScript ou VBScript, le danger est que les fichier sont sous formes de de pièces jointes donc ne jamais ouvrir le fichier si on peut pas vérifier leur intégrité.

Le format de fichier **.SCF** est une commande d'explorateur Windows utilisé pour effectuer une action comme déplacer une icône sur le bureau donc le danger est que un fichier .SCF peut donc indiquer a

l'Explorateur Windows d'exécuter des commandes qui sont dangereux pour l'ordinateur.

Le fichier **.SCR** est un fichier d'économiseur d'écran qui peut afficher des animations de texte, un graphique vectoriel , animation ou vidéo… Donc le danger ce genre de fichier c'est que l'écran de veille fichiers contient du code exécutable ce qui permet aux programmeur de se cacher du code malveillant l'intérieur.

Et pour finir avec Windows il y a des fichiers **.PIF** qui contient des informations basé sur MS-DOS.
Le danger est qu'il peut exécuter les programmes exécutables donc le fichier peut transmettre des virus ou scripts nuisibles .

Il y a aussi des formats de fichiers dangereux sous Linux, en effet les formats de fichiers Exécutable and Link Format (ELF) est un format de fichier exécutable pour Linux. Ce type de Malware peut infecter et se propager à travers les exécutables ELF.
On a les scripts malicieux qui s'attaqueront aux fichiers d'utilisateur.
Comme les fichiers ne sont pas exécutable pour des raisons de sécurité i se pourrait par exemple que dans les archives compressées (.tar.gz, .tar.bz2) les fichiers conservent les droits qu'ils avaient au moment de l'archivage ainsi vous pouvez très bien tomber sur un fichier exécutable après son désarchivage .

Les attaques par dépassement de tampon « « buffer overflow » est un type d'attaque lié à l'utilisation de la mémoire, le but de se virus est de prendre le contrôle d'un programme utilisateur qui est généralement sécurisé et possède des accès ponctuels à des parties du système d'exploitation.
Mais il est plus compliqué sous Linux de tomber sur un Malware car la plupart des applications fonctionnent sans avoir le privilèges administrateurs, et la plupart des logiciels proviennent de sources bien entretenues et centralisés dans les logithèques et non sur des sites au hasard.

Les formats de fichiers qui peuvent être dangereux sous MAC sont les .zip, .rar, .pdf, doc(x), .ppt(x) et xls(x).

Sur les téléphones :

Sous Android les formats .APK peuvent être **dangereux si ils ne sont pas téléchargés dans le Google Store ,** en effet si ont télécharges des fichiers .**APK sur internet on risque de trouver des logiciel mal veillant ou virus.**

Sous IOS les formats de fichiers dangereux sont quasiment inexistants par le faits qu'ils sont très développés et limités sur le téléchargements de fichiers en dehors du store. Donc a part le phishing . Les iPhones sont très peu exposé aux formats de fichiers dangereux.

II) Les formats de fichier plus dangereux :

-Les fichiers .ISO sont généralement utilisés pour créer une copie de tout ce qui trouve sur un disque physique, ont les utilises généralement pour distribuer des systèmes

d'exploitation, tels que Windows, mais ont peut les utiliser pour distribuer des logiciels malveillants . On a aucune raison de vous envoyer un fichier ISO par mail donc si vous recevez ce genre de fichier joints, supprimez-le immédiatement.

-Les fichiers .Exe sont l'un des types de formats de fichiers avec des logiciels malveillants les plus courants. On télécharge souvent des fichiers .exe Internet lorsque vous installez des logiciels légitimes. Mais encore une fois si vous recevez dans un courriel non sollicité ou même de la part d'une personne de votre entourage, mettez-les à l'écart, c'est quasiment certains qu'ils contiennent des logiciels malveillants.

-Les fichiers compressés sont l'un des formats de fichiers avec des types de logiciels malveillants les plus difficiles à traiter car quelqu'un pourrait vous envoyer un fichier compressé pour réduire la taille d'une pièce jointe, donc ça veut que le fichier peut masquer le contenu du paquet comme les fichiers dangereux .exe, ne surtout pas ouvrir une pièce jointe contenant un fichier .zip, .rar, r09, .arc. Donc si vous voulez envoyer des fichiers volumineux à quelqu'un par courriel, envisagez d'utiliser plutôt un service rel que WeTransfer.

-Les installateurs comme MSI est un format de fichier de paquet d'installation qui est utilisé pour installer des programmes sur Windows. Toutefois, il peut également être utilisé pour installer des logiciels malveillants sur votre PC Windows donc tout courriel qui comporte un .MSI. Sur Mac, .dmg est le format le plus souvent utilisé pour distribuer des

logiciels, donc méfiez des fichiers .dmg qui arrivent en pièce jointe

-Les Documents Office peuvent contenir des macros intégrées, de petits programmes qui font des ravages sur votre système en volant des données personnelles ou en installant des chevaux de Troie sur l'ordinateur.
NE JAMAIS OUVRIR CE GENRE DE FICHIER SI VOUS N'ETES PAS SUR A 100 % de savoir ce qu'elles contiennent. Les fausses factures sont une méthode d'attaque courante, qui consiste à envoyer aux employés ce qui ressemble à une demande finale et à les pousser à ouvrir le fichier malveillant.

III) Les sources de fichiers les plus sûrs

Donc pour être sur que votre fichier est de source fiable vous pouvez par exemple :

- Vérifier si c'est un fichier PDF car l'avantage des fichiers PDF c'est qu'ils sont en lectures seules et ne permettent pas l'exécution du code.
- **Allez sur le site internet « VIRUS TOTAL** » qui est un site internet ou vous pouvez déposer pour vos fichiers et les faire vérifier pour savoir si il n'y a pas de virus ou de logiciels malveillants cachés.
- **Les fichiers .txt** car généralement ils ne contiennent que texte brut sans fonctionnalités actives.
- **Les fichiers .jpg, .png** Les fichiers images sont généralement sûrs tant qu'ils sont utilisés pour afficher des images .

- **Les fichiers audios** comme les .mp3 ou les .mp4 comme la plupart du temps ils sont utilisés à la lecture multimédia et sont considérés comme relativement sûrs.
- **Les fichiers de sauvegarde cryptés**, les fichiers de sauvegarde créés a l'aide d'outils de chiffrement (comme Bitlocker ou FileVault) sont généralement sécurisé, car ils sont chiffrés et nécessitent un mot de passe pour être ouverts.
- Pour finir **les fichiers compressés sécurisés** peuvent être sécurisées en utilisant des mots de passe pour les protéger contre un accès non autorisé.

IV) Comment se protéger d'un rançon-logiciel

Pour inciter les utilisateurs à se protéger on peut faire en sorte dans l'entreprise d'organiser une réunion de sensibilisation aux conséquences en expliquant les risques de ne pas de se protéger en ligne, tels que la perte de données personnelles, les vols d'identité, les pertes financières et la compromission de la vie privée.

On peut aussi organiser une formation en organisation des ateliers ou des sessions de formation pour enseigner les bases de la sécurité informatique, y compris la création de mot de passe forts, la mise a jour régulière des logiciels, la reconnaissance des menaces et la navigation sécurisé.

-En partageant des histoires réelles d'échecs ou de réussite en partagent des exemples de personnes qui ont été victimes de cyberattaques ou qui ont réussi à se protéger efficacement. Les témoignages réels peuvent aider à rendre les menaces plus concrètes.

En faisant des recommandations de sécurité , en effet on peut donner des conseils spécifiques, tels que l'installations de logiciels antivirus et

anti-malware, l'activation de pare-feu, la sauvegarde régulière des données et la mise a jour des systèmes d'exploitation.

-En tenant informés les utilisateurs, sur les menaces informatiques en partageant des actualités et des avertissement sur les dernières attaques.

-En expliquant comment les logiciels malveillants fonctionnent en utilisant des exemples concrets, les ransomwares, les chevaux de Troie et les logiciels espions.

-On peut aussi organiser récompenser et encouragez les comportements de sécurité en ligne par exemple en organisant des concours de sécurité ou en offrant des récompenses pour la vulnérabilité.

-Faire en sorte que les mesures de sécurité sont simple à mettre en œuvre et à suivre. C'est plus facile à une personne de se protéger s'ils trouvent les étapes à suivre facile.

-On peut aussi encourager la responsabilisation du personnel en soulignant que la sécurité en ligne est la responsabilité de chacun.

-Montrer notre exemple personnel avec les bonnes pratiques de sécurité.

-Ouvrir un support technique en des ressources en cas de question ou de problèmes liés à la sécurité informatique.

V) Deux exemples de mesure pour pas se faire prendre pour un parano

Ces mesures peuvent être très efficaces pour protéger votre entreprise en effet pour approuver ces méthodes on peut citer les plus grandes cyber-attaques qui se sont déroulés dans les

entreprises, exemple le cas de « Hôtel Marriot », en effet pendant 4 ans se réseau informatique s'est fais infiltré est ce fut voler des noms, des détails de passeports, des informations de contact, données cartes de crédit etc…

Autre très grosse cyberattaque importante est celle de Yahoo ! en 2014. Près de de 1 milliards de données personnels ont été volés c'est-à-dire que a tout le monde on pouvait accéder à des vies entières de certaines personnes si les données c'est-à-dire numéros de téléphones de naissance, votre adresse, votre nombre d'enfants etc…

Conclusion :

Les dangers sur internet existent et peuvent mettre en danger vous en premier et votre entreprise. Une mauvaise connaissance sur les d'internet peut engendrer énormément de problèmes, c'est donc pour cela que s'informer sur l'actualité des cyberattaques est très importante quand travaille dans le domaine de l'informatique.