Recommandations de cybersécurité pour les personnes en télétravail

1. Objectif

Il est primordial de protéger les installations critiques du système d'information qui permet à l'entreprise de survivre. Lorsque vous travaillez en télétravail, Il est donc nécessaire de prendre des mesures afin de réduire le risque que représente l'accès non autorisé aux informations ou ressources par d'autres personnes et de réduire le risque de contamination du système d'information de l'entreprise à distance.

Attention : Les pirates (sociétés criminelles et/ou étatiques) ne se privent pas d'attaquer des hôpitaux et des entreprises même pendant la crise actuelle du COVID19. Aucune entreprise n'est à l'abri de cyberattaques. De plus, le risque actuel augmente avec le télétravail et la crise liée au virus.

https://www.zdnet.fr/actualites/un-hopital-tcheque-frappe-par-une-cyberattaque-en-pleine-epidemie-de-covid-19-39900659.htm

2. Les recommandations à suivre

- Il est important que l'ordinateur et l'antivirus soient mis à jour (privée et/ou professionnel)
- Ne répondez pas à l'urgence d'un message, prenez le temps de contrôler la source / le message (Technique de manipulation utilisée par les pirates), en cas de doute appelez le service IT

- Seuls les fichiers / documents / liens attendus et nécessaires doivent être ouverts

- Considérer un document comme une application dangereuse (quand il arrive par mail, par un lien de téléchargement ou un fichier ZIP)

- Les informations sensibles ne doivent pas être stockées ou transmises
- Les données de connexions au système d'information et aux applications ne doivent pas être enregistrées et/ou transmises

- En cas d'infection (ou de doute important), déconnectez et prévenez le support IT

3. Le Périmètre

Toute personne qui travaille à distance en utilisant un ordinateur (PC ou MAC), une tablette qu'il soit fourni par l'entreprise ou que ce soit un appareil privé, doit respecter au mieux les recommandations de ce document.

4. Pourquoi est-il important de suivre ces recommandations ?

Toutes les connexions à distance, VPN (Virtual Private Network), bureau à distance (Citrix, Microsoft RDP, …), VD… augmentent la surface d'attaque et représente un risque accru pour l'entreprise et ses services critiques.

4.1 Il est important que l'ordinateur et l'antivirus soient mis à jour

Un système qui n'est pas à jour peut être piraté à distance sans aucune difficulté par un pirate. Ils utilisent les failles des systèmes et des applications pour déployer des (crypto) virus, et/ou pour prendre le contrôle de l'ordinateur, puis du réseau. Pour réduire ce risque, mettez votre ordinateur (privée/pro), votre antivirus et vos applications à jour, et cela avant de vous connecter à distance.

4.1.1 Pour contrôler l'antivirus et la mise à jour sur Windows 10

Mise à jour : **Démarrer**, puis vous rendre sur **Paramètres** > **Mise à jour et sécurité** > **Windows Update**.
L'antivirus : **Démarrer**, puis vous rendre sur **Paramètres** > **Mise à jour et sécurité** > **Sécurité Windows**.
https://support.microsoft.com/fr-fr/help/4028102/windows-10-how-to-protect-your-pc

4.1.2 Pour MAC :

Mise à jour : **Préférences Système** dans le **menu Pomme** , puis **cliquez** sur **Mise à jour logicielle**
https://support.apple.com/fr-fr/HT201541
https://support.apple.com/fr-fr/HT202491

4.2 Ne répondez pas à l'urgence d'un message, prenez le temps de contrôler la source / le message

Pour manipuler les utilisateurs, les pirates créent des scénarios d'urgence (ex : faites cela immédiatement…) ou utilisent la hiérarchie (ex : je suis docteur… Veuillez ouvrir ce fichier…) pour vous faire ouvrir un fichier ou vous demander des informations de connexion. Ne tombez pas dans le panneau, ne vous laissez pas manipuler. Prenez le temps de contrôler les informations et si vous avez des doutes demandez l'aide au support IT.

4.3 Seuls les fichiers / documents / liens attendus et nécessaires doivent être ouverts

N'ouvrez pas de documents ou de liens de type google drive, one drive, wetransfert, swiss transfert, etc… qui ne seraient pas attendus ou pas nécessaires. Si vous avez un doute, consultez le support IT.

4.4 Considérer un document comme une application dangereuse (quand il arrive par mail, par un lien de téléchargement ou un fichier ZIP)

Il faut impérativement considérer un document (Excel, word, ZIP, pdf,…) comme une application dangereuse, quand il arrive par email, un lien de téléchargement ou un fichier ZIP. N'activez JAMAIS les macros de fichiers reçus de cette manière. Les fichiers stockés sur les serveurs de l'entreprise sont considérés comme sains et peuvent être utilisés sans risque.

4.5 Les informations sensibles ne doivent pas être stockées ou transmises

Les informations sensibles comme les données de clients, secrets de fabrication, données de santé, informations de facturation, code source, RH, … ne doivent pas être téléchargés et enregistrés sur les appareils privés et/ou limités sur les appareils professionnels utilisés dans un réseau privé (Home office), cela afin de garantir leurs sécurités, leurs intégrités et leurs sauvegardes.

4.6 Les données de connexions au système d'information et aux applications ne doivent pas être enregistrées et/ou transmises

Les données de connexions (mot de passe, clés de sécurité, token,…) au système d'information et aux applications ne doivent pas être enregistrées et ne doivent jamais être transmises sous aucun prétexte.
Pour rappel :

- Le support IT ne demande jamais vos mots de passe
- Les données de connexions sont des éléments sensibles et très recherchés par les pirates
- Pour un pirate, une seule connexion à distance réussie lui donne accès à toute l'entreprise

4.7 En cas d'infection (ou de doute important), déconnectez et prévenez le support IT

En cas d'infection ou de doute important de piratage, déconnectez immédiatement l'appareil du réseau (couper le wifi, ou enlever la prise réseau) et informer le support IT du problème dans les plus brefs délais. Afin que l'équipe IT puisse vous aider et gérer au mieux les éventuelles conséquences au niveau du système d'information et pour communiquer au mieux sur le problème aux autres utilisateurs.

5. Autres informations

5.1 Pour la mise en place au niveau du service IT

Le guide de bonne pratique ISO 27002 (6.2.2) et/ou NIST 800-46r1 peuvent être des sources intéressantes pour la mise en place du télétravail dans votre entreprise.

- ISO 27002 (Payant) Chapitre 6.2.2 : https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:fr
- NIST (gratuit) : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-46r1.pdf

5.2 Licence du document