UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Améliorer la sécurité en télétravail

INTRODUCTION

La pandémie a mené les organisations à repenser et à transformer leurs méthodes de travail. Les règles de confinement obligatoire ont accéléré un mouvement qui prenait déjà lentement de l'ampleur, c'est-à-dire le travail de la maison.

Les organisations ont investi énormément d'efforts à mettre en place tous les outils requis pour assurer la continuité de leur prestation de services, tout en assurant un respect des normes de sécurité pour la santé physique et mentale de leurs employés, mais aussi la sécurité des informations qui sont requises pour le travail quotidien.

Malgré tous les efforts déployés par les organisations afin de sécuriser leurs appareils et les données corporatives, la vigilance des utilisateurs est requise afin de sécuriser leurs propres appareils à la maison et de maintenir de bonnes habitudes en cyberhygiène.

Considérant que le télétravail est effectué dans des environnements personnels, il faut se conformer aux meilleures pratiques afin de rehausser la sécurité à la maison tout en protégeant les données corporatives qui sont traitées dans le quotidien.

SÉCURISER SON ROUTEUR POUR INTERNET

Cet équipement permet aux appareils de la maison de communiquer entre eux ainsi qu'avec le réseau Internet. Il est commun que les utilisateurs configurent leur réseau sans-fil sans modifier les accès par défaut ou sans configurer de clé d'accès au réseau sans-fil, laissant ainsi le routeur non protégé.

Pourtant, le routeur est un peu le cerveau de toute la communication qui a lieu dans votre réseau à domicile. Un acteur malveillant y ayant accès pourrait conduire plusieurs types d'attaques. En laissant le mot de passe administrateur par défaut configuré dans l'appareil, la sécurité du réseau en entier est à risque.

Il est donc important de modifier les identifiants ayant le privilège administrateur de l'appareil afin d'être uniques et difficiles à déchiffrer. L'implémentation d'une clé réseau forte permet aussi de sécuriser les réseaux sans-fil qui sont diffusés à la maison, et de réduire les risques d'une intrusion dans le réseau par des acteurs qui seraient en mesure de capter le signal.

Vous pouvez aussi modifier l'adressage réseau configuré par défaut dans le routeur afin de rendre l'adresse IP du routeur plus difficile à déterminer. Habituellement, un routeur résidentiel a une adresse IP qui ressemble à 192.168.0.1 ou encore 192.168.1.1. Ceci est dû au fait que l'adressage configuré dans le routeur est de 192.168.0.0/24 ou 192.168.1.0/24. Afin de modifier l'adressage, vous pouvez lui donner un adressage qui respecte une des trois plages IP réservées à cet effet :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

Vous pourriez donc utiliser, par exemple, la plage 10.15.25.0/24. L'adresse IP de votre routeur deviendrait 10.15.25.1.

ÉTABLISSEZ UN RÉSEAU VISITEUR POUR INVITÉS ET LES OBJETS CONNECTÉS (IOT)

Il est recommandé d'établir un réseau sans-fil supplémentaire à la maison pour les visiteurs et tous les appareils qui se connectent à l'Internet (Internet des objets, téléviseur intelligent, etc.). Ce réseau visiteur permettra de séparer votre réseau personnel du reste des appareils dans la maison.

Il est connu que les appareils intelligents qui communiquent avec Internet (téléviseurs, Google Home, Amazon Echo, interrupteurs intelligents, etc.) ne sont pas maintenus aussi fréquemment que les ordinateurs et appareils mobiles, laissant souvent des vulnérabilités exploitables pendant de longues périodes. S'ils se trouvent sur le même réseau que votre réseau personnel, un acteur malveillant pourrait utiliser un de ces appareils intelligents pour naviguer sur votre réseau personnel, et procéder à des attaques. La séparation de ces appareils du réseau personnel réduit la surface d'exposition à ces risques dans votre environnement de travail à la maison.

APPLIQUER LES MISES À JOUR DE VOS ORDINATEURS ET APPLICATIONS

Avec l'automatisation des attaques informatiques, il est devenu une priorité d'installer les correctifs de sécurité afin de corriger les failles exploitables sur nos systèmes d'exploitation et dans nos applications. Que ce soient des vulnérabilités connues ou encore des vulnérabilités « jour zéro », un retard dans des correctifs de sécurité pourrait permettre à des acteurs malveillants de prendre possession de votre ordinateur et de procéder à une attaque sans que vous en soyez conscient, pouvant causer des dégâts importants.

ORDINATEURS GÉRÉS PAR L'ORGANISATION

Il est généralement d'usage que les utilisateurs travaillant de la maison le fassent sur des appareils fournis et gérés par leur organisation. Dans ce cas, il est probable que l'organisation distribue par des processus différents les mises à jour requises sur vos appareils. N'ayant pas de privilèges élevés sur les ordinateurs, il revient donc à l'organisation de vérifier les correctifs de sécurité requis pour vos logiciels et systèmes d'exploitation. Si vous avez des doutes sur les mises à jour de vos appareils corporatifs, n'hésitez pas à communiquer avec les services des technologies de l'information de votre établissement.

ORDINATEURS PERSONNELS

Sur vos ordinateurs personnels, il faut vérifier que les mises à jour automatiques soient activées afin de bénéficier de ces correctifs à partir du moment où ils sont disponibles, permettant de vous protéger le plus rapidement possible contre des failles exploitables. Il en va de même pour vos applications. Plusieurs applications affichent, lors de leur ouverture, des messages indiquant qu'une nouvelle version de l'application est disponible. Ces mises à jour incluent souvent des correctifs de sécurité qui corrigent des vulnérabilités dans l'application en question.

Il ne faut pas oublier qu'un appareil à risque sur votre réseau peut devenir une porte d'entrée pour un acteur malveillant, lui permettant de lancer des attaques sur n'importe lequel de vos appareils branchés sur votre réseau de maison.

UTILISER DES MOTS DE PASSE COMPLEXES

Les mots de passe complexes sont aussi importants à la maison qu'au bureau. Un acteur malveillant aurait plus de facilité à s'introduire dans vos appareils ou usurper votre compte si vous conservez des mots de passe simples à deviner.

Il est donc important de vous assurer que vos mots de passe soient suffisamment élaborés qu'ils nous procurent une vraie sécurité. C'est-à-dire qu'il faut éviter d'utiliser des éléments simples tels que des couleurs, des noms, une date de naissance, ou tout autre élément qui pourraient se retrouver publiquement sur vos réseaux sociaux, et qu'un attaquant pourrait utiliser pour décoder vos accès.

D'autres stratégies importantes à considérer afin de sécuriser vos mots de passe incluent :

- Éviter de réutiliser les mêmes mots de passe
- Changer les mots de passe régulièrement si possible
- Ne pas utiliser des mots de passe professionnels dans vos comptes personnels

ACTIVER L'AUTHENTIFICATION MULTIFACTORIELLE, LORSQUE DISPONIBLE

L'authentification multifactorielle est une méthode où l'accès est octroyé uniquement à la suite de la validation de deux ou plusieurs preuves d'identité telles que :

- Mot de passe
- Code temporaire (SMS, Courriel)
- Application d'authentification
- Reconnaissance faciale
- Empreintes digitales.

Lorsqu'activée, l'authentification multifactorielle peut réduire de façon importante les risques d'infection et de vol d'identité puisqu'une personne non autorisée ne sera pas en mesure d'obtenir accès seulement avec votre mot de passe.

Voici certaines suggestions d'application d'authentification que vous pourrez trouver dans les magasins de votre téléphone intelligent : **Microsoft Authenticator**, **Google Authenticator, Authy.**

ÉVITER D'UTILISER DES POINTS D'ACCÈS PUBLICS

Plusieurs lieux publics mettent à la disposition des gens des points d'accès afin de conserver un accès à l'Internet lors de leurs déplacements. En théorie, ce service offert est très attirant et apprécié par les utilisateurs. Cependant, ces réseaux publics offrent peu ou pas de fonctions de sécurité. Un acteur malveillant qui se retrouverait sur à proximité pourrait observer toutes les données qui transigent sur le signal (incluant vos mots de passe lorsque vous ouvrez une session sur un site, les fichiers que vous téléchargez, l'historique des sites que vous visitez, etc.). Malheureusement, ces réseaux publics non sécurisés sont souvent la source d'attaque et de vol d'identité.

Une bonne stratégie à employer, lorsque l'utilisation du point d'accès public est requise, est de chiffrer tout ce que vous faites grâce à un outil VPN (réseau privé virtuel) fourni par votre employeur. Ce logiciel fera de sorte qu'aucun intermédiaire sur le point d'accès ne puisse déchiffrer votre activité et vos mots de passe.

Si vous êtes dans l'impossibilité d'utiliser un VPN (parfois, les réseaux publics interdisent leur utilisation), vous pouvez partager vos données LTE cellulaires afin d'établir un lien sécurisé vers l'Internet.

ÊTRE VIGILANT AUX TENTATIVES D'HAMEÇONNAGE

Encore aujourd'hui, malgré les campagnes de sensibilisation et toute l'information de prévention qui est disponible et diffusée, l'hameçonnage reste la méthode la plus efficace utilisée par les acteurs malveillants d'obtenir de l'information privilégiée.

Il est donc primordial de toujours vérifier si les courriels que nous recevons sont légitimes.

Voici quelques aide-mémoires qui peuvent aider à identifier un courriel d'hameçonnage :

REPÉRER LES ERREURS

Les courriels frauduleux sont souvent porteurs de fautes d'orthographe et d'une mauvaise structure de texte. Souvent, avec une lecture attentive, nous pouvons identifier un courriel d'hameçonnage par sa piètre qualité.

DEMANDE D'INFORMATION SENSIBLE

Les organisations établies ne demanderont jamais de renseignements personnels par courriel. Si vous recevez un courriel qui demande des informations sensibles, il est important de ne pas les fournir et de signaler le courriel comme étant potentiellement frauduleux.

MESSAGE ALARMANT AVEC BEAUCOUP D'AVERTISSEMENTS ET DE CONSÉQUENCES

Certains messages peuvent provoquer un sentiment d'urgence en prétextant un compte expiré, piraté, ou une perte de service importante. C'est impératif de ne jamais ouvrir les liens dans ces messages, et de valider en consultant directement le site officiel des organisations en question.

OFFRE URGENTE

Certains acteurs malveillants concevront un message qui propose une offre limitée sur le point d'expirer afin d'attirer les victimes vers un site trafiqué. Si une victime tente de réclamer l'offre, le site enregistre ses informations de paiement pour de la fraude ultérieure. Il est important de ne pas fournir vos informations à des commerces qui vous sont inconnus ou pour lesquels vous n'êtes pas déjà abonnés.

SITE WEB NON SÉCURISÉ

Un élément indicateur d'un site web frauduleux est l'absence de certificat sécurisé. Lorsqu'on laisse notre souris survoler un lien dans un courriel, nous pouvons voir dans une boite l'adresse complète du lien. Souvent, il est recommandé de ne pas cliquer sur des liens qui débutent par « http ». Un site sécurisé par un certificat et qui proviendrait d'une organisation réputée avec de bonnes pratiques en sécurité aurait une adresse web débutant par « https », ou le « s » signifie « sécure ».

UTILISER UN GESTIONNAIRE DE MOT DE PASSE

Les gestionnaires de mots de passe vous permettent d'utiliser des mots de passe complexe pour tous les sites et services que vous consultez, tout en évitant de réutiliser un mot de passe à plus d'un endroit. Donc, si un de vos comptes est exposé à la suite d'une compromission d'un site, vos autres comptes resteront à l'abri.

Il prévient aussi les habitudes risquées de conservation de mot de passe dans des documents texte, ou même sur des papiers cachés sous les claviers.

RESSOURCES

Français – Conseils pour du télétravail en toute sécurité

Français – Trucs et conseils de cybersécurité pour le télétravail

Anglais - 25 working from home security tips

Anglais - Awareness while working remotely

Anglais - Cyber security tips and advice for remote workers

Anglais - Keep your home and family safe with these 3 smart cybersecurity steps

Français - Les risques du WiFi public

RÉVISIONS

Date	Action	Auteur	Ver.
2023-01-18	Ajustement du modèle du document	Jean-François Blais CESI de l'UQ	1.1
2022-09-30	Première version	Jean-François Blais CESI de l'UQ	1.0