efcse.eu

CYBERSECURITE ET TRAVAIL A DISTANCE

Auteur : EFCSE, Working Group Education et Formation
09/03/2020

Un contexte inédit

Un contexte exceptionnel de confinement qui oblige les personnes et les organisations à travailler majoritairement à distance, pas nécessairement avec un temps de préparation à cette forme de travail, tant humainement que techniquement, nous voici en terrain propice pour les piratages informatiques (entre autres).

Etant occupés ailleurs, notamment à organiser en mode dégradé leur activité, toutes les entreprises n'ont pas nécessairement renforcé la protection de leur information. D'autant que celle-ci circule plus largement entre des postes de travail situés à distance (hors périmètre de l'entreprise), ce qui représente potentiellement des points d'entrées supplémentaires pour les cyberpirates.

Ajoutons à cela des personnes confinées chez elles, par définition seules devant un écran d'ordinateur, en télétravail, donc plus en risques et en vulnérabilité face à des escroqueries ou des attaques, car moins vigilantes et / ou moins bien protégées et pas, ou mal préparées.

Une touche supplémentaire de stress car la connexion réseau n'assure pas bien, une pincée d'inquiétude sur l'évolution de la situation sanitaire, trop de précipitation dans l'usage du clic sur un lien d'information Covid-19, voici les ingrédients parfaits pour faciliter les activités malveillantes des cybercriminels.

A propos du télétravail

Le télétravail est nécessaire et les travailleurs y sont contraints, n'étant pas un choix, son efficacité peut ne pas être au rendez-vous, d'autant plus dans un contexte anxiogène comme celui que nous vivons actuellement.

Le lieu physique est important, il est bon de pouvoir s'isoler (autant que faire se peut) du reste des habitants de la maison afin de travailler plus sereinement. Bien qu'il ressorte que seul on se trouve parfois « trop tranquille » et en famille « pas assez tranquille » …

Il n'y a pas de solution idéale mais bien une nouvelle forme d'organisation chez soi, chacun devant trouver son propre mode de fonctionnement.

Pour éviter l'explosion du nombre d'heures passées devant son écran à travailler parce qu'il n'y a rien d'autre à faire, ou le trop peu de temps consacré au travail, parce qu'il y a toujours quelque chose à faire chez soi, tout ce qui peut apporter un cadre à son autodiscipline est fondamental, rythme, horaires, objectifs de la journée, réunions programmées, etc.

Il s'agit ici de rappeler quelques bons usages lorsque l'on travaille à distance.

efcse.eu

Télétravail et bonnes pratiques (non exhaustif)

Connexion internet, quelques fondamentaux

- Désactivation des applications qui consomment de la bande passante pour rien (surveillance régulière), un réseau très sollicité affecte la rapidité de connexion,

Utilisation du VPN[1] de l'entreprise pour rester en sécurité,

- Pas de mixe entre le temps de loisir et le temps de travail sur son ordinateur (utilisation conseillée d'un appareil dédié à la partie personnelle),
- Utilisation d'un réseau internet domestique séparé de celui dédié au travail, si possible,
- Le mot de passe du routeur internet domestique doit être renforcé si besoin (plus de caractères, combinaison alphanumérique et caractères spéciaux), utilisation d'un gestionnaire de mot de passe de préférence,
- Antivirus et protection des machines à jour.

Pièges quotidiens potentiels

Phishing (hameçonnage)

1er vecteur d'attaque pour voler des informations professionnelles ou personnelles.

Principe : entraîner la personne vers un faux « vrai site officiel » qui affiche une information soit alléchante (remboursement, très bonne affaire, …) soit « pseudo » sérieuse (confirmation de commande, livraison en attente, …) où il suffit de cliquer sur un lien pour être pris dans les mailles du filet, entrainant infection de l'ordinateur et du réseau auquel il est connecté.

Ransomware (rançongiciel) - Demande de rançon

Principe : une fois un virus informatique installé (parfois via une pièce jointe) : demande de rançon contre déblocage de l'ordinateur ou décryptage des fichiers.

Vecteurs : SMS, Email, discussion instantanée (chat), appels téléphoniques inconnus …

Action : prendre le temps d'analyser la situation avant de cliquer ou de fournir toute information.

Téléchargement d'applications

Outils gratuits (parfois pour des applications normalement payantes) pour « mieux » communiquer avec les autres, naviguer sur internet, consulter ses mails, jouer, prendre des photos, travailler, regarder des vidéos, etc.

Principe : installation d'applications piégées en vue de vol de données ou d'installation de virus.

Action : ne télécharger qu'à partir des sites officiels des éditeurs, en prenant le temps de lire les informations présentées.

Réputation et garanties des sites web

Affichage de références, proposition d'informations sérieuses, proposition de services existants, achats, cartes de fidélité, informations réelles, etc.

Principe : sites web malveillants qui collectent des informations personnelles, bancaires ou autres à des fins d'escroquerie (ransomware, usurpation d'identité, détournement financier, dons frauduleux, vente de produits de contrefaçon, etc.)

La situation actuelle de crise sanitaire est propice à ce type de pratique avec des pièges potentiels derrière les mots clefs tels que : Coronavirus, Covid-19, masque de

[1] VPN : Virtual Private Network (Réseau Virtuel Privé), permet de créer un lien entre des postes de travail distants (ordinateurs) isolant ainsi les échanges entre ces postes par rapport au reste du trafic public (télécommunication).

protection, Chloroquine, attestation de déplacement[2], gel hydroalcoolique, Hydroxychloroquine, confinement, Azithromycine, pandémie, vaccin, etc.

Actions : prendre le temps d'analyser la situation avant de fournir toute information ;

Croiser les informations, se méfier des fausses informations, prendre le temps de lire les informations affichées ;

S'abstenir d'aller plus loin dans le processus en cas de doute …

Pièges : focus sur l'activité professionnelle

Sur le plan financier / bancaire

Principe : usurpation d'identité d'un salarié ou d'un dirigeant pour effectuer des demandes de changement de RIB ou de virements exceptionnels, modification de coordonnées de virement bancaire, règlement d'un fournisseur, règlement d'un salaire, ….

Actions : politique de communication renforcée au sein de l'organisation ;

Lecture avisée des messages ;

Pas de précipitation dans les réponses à toute sollicitation ;

Demande de validation par la hiérarchique pour toute opération financière ;

Contact direct avec le demandeur (le vrai) ;

Augmentation de sa concentration sur chaque tâche dans un processus en cours, …

Sur le plan de la sécurité et de la protection du SI de l'organisation

Principe : intensification des cyberattaques de type ransomware, vol de données, saturation des serveurs (via attaque par déni de service – Ddos), implantation d'un ver dans le SI. Dans le contexte de crise sanitaire actuelle il s'agit par exemple pour les pirates de déstabiliser les plans d'urgence sanitaire en ralentissant les systèmes (attaques contre les établissements de soins).

Actions : politique de communication renforcée au sein de l'organisation,

Vigilance accrue sur la provenance des messages et des pièce jointes,

Sauvegardes régulières des données (avec copie déconnectée),

Mesures renforcées pour prévenir les cyberattaques,

Mesures de supervision de la sécurité,

Mises à jour régulières de sécurité des appareils connectés,

Consolidation des accès (mot de passe unique et plus fort, authentification forte, …)

Pour finir, rappelons que les règles de confidentialité, lors d'échanges téléphoniques ou en visioconférence, ou encore lorsque l'on s'absente, même quelques instants, de son poste de travail (verrouillage du clavier), restent bien évidemment applicables en télétravail.

Contactez-nous sur efcse.eu

[2] Attestation de déplacement dérogatoire et justificatif de déplacement professionnel disponibles en France sur le site officiel du Ministère de L'intérieur.