GUIDE DU TELETRAVAILLEUR

COVID-19

ANSSI AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

GUIDE DES BONNES PRATIQUES DE SÉCURITE DU TELETRAVAILLEUR

La pandémie actuelle du Coronavirus (Covid-19) fait des ravages et oblige les entreprises à faire usage du télétravail durant cette période.

Toutefois, les réseaux domestiques n'offrent pas les mêmes niveaux de sécurité que ceux des entreprises. La compromission de la machine d'un employé a le potentiel d'exposer tout le système d'information de l'entreprise. Mieux, pour ne rien arranger, la situation actuelle attise l'imagination des cybercriminels qui se font passer pour des organisations sanitaires, gouvernementales ou des forces de l'ordre et utilisent le sujet du COVID-19 comme appât pour inciter leurs victimes à cliquer sur des pièces jointes, des liens dangereux et au remplissage de formulaires envoyés par mail, dans le but de collecter des données confidentielles. Pour aller plus loin, d'autres incitent à télécharger des applications malveillantes simulant des applications de suivi ou de cartographie de la pandémie du Coronavirus.

L'ANSSI partage avec vous quelques bonnes pratiques de sécurité pour se mettre à l'abri d'éventuelles attaques.

A. Recommandations aux employés en télétravail

1. Quelques fondamentaux concernant le télétravail :

- Utiliser les appareils fournis par l'entreprise pour accéder aux ressources professionnelles ;
- Installer les mises à jour de sécurité ;
- Utiliser un VPN et les méthodes d'authentification doubles prévues par votre employeur afin d'accéder de manière sécurisée aux ressources de l'entreprise ;
- Ne pas désactiver ni contourner les outils de sécurité installés par votre employeur sur vos terminaux de travail (antivirus, mise à jour, outils de chiffrement de données) ;
- Ne pas installer les applications mobiles sur le thème du Covid-19 mais plutôt s'informer sur la crise à partir des canaux officiels : https://www.gouv.bj/coronavirus;

- Utiliser des mots de passe complexes pour les comptes d'entreprise et personnels ;
- Eviter l'utilisation d'outils de collaboration non adoptés par l'employeur : outils de conférence, partage de fichiers, scanner, modification et conversion de documents en ligne (PDF, Word, Excel, etc.) ;
- Faire un usage strictement professionnel du matériel de travail ;
- Eviter de connecter vos appareils professionnels à des réseaux ouverts (WiFi publics ou sans mot de passe) ;

2. Quelques recommandations pour renforcer la sécurité de votre réseau domestique :

- Changer le mot de passe de votre Wi-Fi par un mot de passe complexe en privilégiant le chiffrement WPA2 ;
- Eviter de nommer votre réseau Wi-Fi en utilisant votre nom ;
- Veiller à reconnaitre les appareils personnels connectés à votre réseau par exemple en consultant les pages d'administration de votre routeur domestique ;
- Privilégier une connexion dédiée (boitier 4G, autre SSID, etc...) à votre usage professionnel et différents du Wi-Fi utilisé pour l'usage domestique.

3. Quelques astuces contre le hameçonnage :

- Vérifier systématiquement vos emails : soyez attentif aux adresses de l'expéditeur car elles peuvent être subtilement falsifiées ;
- Ne pas cliquer sur les liens ou pièces jointes dans les e-mails non sollicités : surtout pas des documents sur le thème Covid-19 ;
- Ne pas activer les macros des documents qui proviennent d'internet ;
- Notifier systématiquement le service informatique de votre entreprise en cas d'incident lié à la sécurité des données : perte, vol de matériel, infection d'un virus, e-mail de phishing etc.. ;

B. Recommandations aux Directeurs des Systèmes d'Information

1. Quelques fondamentaux pour renforcer la sécurité de votre infrastructure pendant le télétravail

- **Activer l'authentification multi-facteur pour tous vos utilisateurs.** Cette mesure permettra de s'assurer de manière forte de l'identité des employés qui se connectent aux applications de l'entreprise ;
- **Privilégier les outils offrant des capacités de centralisation du télétravail tels que Microsoft Teams, Slack** (échanges textuels, vidéo, audio, partage de fichiers et de calendriers, etc..) de manière à éviter que les télétravailleurs se tournent vers des plateformes arbitrairement choisies au risque de perdre de contrôle de l'information.
- **Désactiver les comptes du personnel qui ne fait plus partie de l'entreprise.** Cette mesure permanente en temps normal devrait faire l'objet d'une attention particulière au risque de s'exposer à des actions malveillantes de la part d'ex-employés mal intentionnées ;
- **Redoubler de vigilance concernant les attaques de phishing et former les utilisateurs à les identifier.** Durant cette crise du COVID-19, de nombreux liens circulent pour tromper les internautes, dans l'unique but de collecter des informations sensibles sur les systèmes auxquelles ils se connectent et pour au final usurper leur identité sur les dits systèmes. Les employés de vos entreprises ayant opté pour le télétravail doivent absolument être sensibilisés sur ces risques afin de ne pas compromettre la sécurité de toute l'infrastructure.
- **Vérifier et sécuriser les sauvegardes OS, configurations, équipements réseau, etc....** Les sauvegardes de secours doivent être des sauvegardes complètes et être impérativement stockées hors ligne. **En cas de cryptovirus, les sauvegardes peuvent avoir été corrompues depuis plusieurs mois**

2. Concernant vos postes de travail physiques d'entreprise :

- Il est nécessaire de s'assurer que les politiques de mise à jour de l'antivirus, patchs Windows, applications et mots de passe sont bien implémentées sur les postes de travail en entreprise accessibles à travers un VPN.

- Quant aux postes sans accès par VPN, c'est-à-dire les postes physiques utilisés par les employés qui doivent quand même être présents physiquement, il est nécessaire d'activer la politique d'administration sur ces postes de travail qui ne sont pas munis de VPN via l'Active Directory afin de permettre les mises à jour par internet ;
- Afin de pouvoir continuer les fonctions de support aux utilisateurs, installer sur les postes de travail, des solutions de prise de contrôle à distance tels que TeamViewer, LogMeIn, etc…

3. Recommandations sur la veille sécuritaire

Il est nécessaire de maintenir une veille sécuritaire sur les outils utilisés par votre entreprise afin de remédier au plus tôt aux vulnérabilités.

- S'organiser pour prendre en compte les bulletins d'alertes publiés par les éditeurs de solutions ou des CSIRT tels que le bjCSIRT afin d'observer les recommandations de sécurité ;
- Mettre en place une surveillance en temps réel de votre infrastructure avec des outils tels que les SIEM ;
- Définir et appliquer les actions d'urgence en cas d'intrusion : par exemple, isoler le poste vérolé et suspendre son accès VPN en cas de présence de ransomware.

4. Recommandations sur la gestion du trafic

En raison d'un accroissement mondial du télétravail, la bande passante devient une donnée importante à gérer avec précaution afin de permettre son utilisation unique à des fins de travail en entreprise. Il est donc important de définir les priorités comme les appels vidéo et audio pour les téléconférences, les accès distants par VPN et autres opérations importantes pour le métier de l'entreprise et de limiter ou interdire l'accès à tout autre contenu.

C. Et pour finir…

La sécurité, c'est un ensemble de mesures permanentes à observer par les utilisateurs et à enforcer par les responsables informatiques. L'on ne se rend compte de l'importance de ces mesures que lorsque le système d'information est déjà l'otage de cybercriminels prêt à profiter de toutes les opportunités d'inattention, y compris en cette période de pandémie mondiale.

Le télétravail est un vecteur de digitalisation des entreprises mais il ne faut pas oublier qu'il augmente la surface d'attaque des infrastructures numériques.

Ensemble luttons contre le COVID-19 ! 👇👇👇👇

D. Références du guide

- Coronas virus et cybersécurité de Infortive
- Vidéo de sensibilisation de @DataProtect

ANSSI AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

MARS 2020

Palais de la Marina, 01 BP 2028, Cotonou- Bénin

Tel: (+229) 21 30 02 36 | Site web: www.anssi.bj | email: contact@anssi.bj

Twitter : @Anssi_Benin | Facebook: anssi.benin