GUIDE DU TELETRAVAILLEUR

COVID-19

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

Table des matières

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 à la recherche de gain facile. Ils utilisent les failles souvent béantes laissées par les employés en situation de télétravail, usent de la crédulité humaine pour mener des attaques qui seraient autrement plus difficiles à exécuter. Liens malveillants, applications vérolées, sites web frauduleux, mots de passe faibles, usurpation d'identité, hameçonnage sont autant de vecteurs que ces cybercriminels utilisent.

Ainsi, dans une démarche de réduction des risques liés au télétravail, l'ANSSI partage avec vous quelques bonnes pratiques de sécurité pour vous mettre à l'abri d'éventuelles attaques.

A. Recommandations aux employés en télétravail

1. Quelques fondamentaux concernant le télétravail

- Utiliser les terminaux fournis par l'entreprise (ordinateurs portables, poste de travail, tablettes, etc…) 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 ;
- Les mesures de sécurité implémentées par votre entreprise sur vos terminaux (antivirus, pare-feu, VPN, proxy) sont essentielles à votre sécurité et à celle de votre organisation. Il faut éviter de les désactiver ;
- Des nombreuses applications concernant le COVID-19 abondent sur internet. Il est crucial de n'installer que celles provenant du Gouvernement béninois ou d'initiatives citoyennes et dont les applications ont été recommandées par le Gouvernement béninois. A cet effet les comptes Twitter de l'ANSSI-Bénin ou du Gouvernement du Bénin sont disponibles pour vous conseiller sur la sûreté d'une application ;
- Utiliser des mots de passe forts c'est-à-dire longs et complexes pour vous authentifier sur tous vos comptes. Les mots de passe doivent différer par application ;

- 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.) ;
- Réserver les terminaux professionnels (ordinateurs, clés USB, tablettes, etc…) à des usages uniquement professionnels pendant votre période de télétravail ;
- Eviter de connecter vos terminaux professionnels à des réseaux sans fil ouverts (Wi-Fi publics ou sans mot de passe).

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

- S'assurer que votre réseau sans fil Wi-Fi est protégé avec un mot de passe long et complexe ;
- S'assurer que votre réseau sans fil Wi-Fi utilise le protocole de chiffrement WPA2 ;
- Pour votre réseau sans fil Wi-Fi, choisir des noms (SSID) qui n'évoquent ni votre identité, ni celle de votre entreprise. Mieux, vous pourriez cacher votre réseau Wi-Fi ;
- Inspecter régulièrement les appareils connectés à votre réseau sans fil Wi-Fi depuis la page d'administration de votre routeur afin d'identifier d'éventuels attaquants ;
- Privilégier une connexion dédiée (boitier 4G, autre SSID, etc…) à votre usage professionnel et différent du Wi-Fi utilisé pour l'usage domestique.

3. Quelques astuces contre le hameçonnage

- Vérifier systématiquement vos e-mails : 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 ;
- Informer 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-facteurs 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 intentionnés ;
- **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 auxquels 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 ;
- En ce qui concerne les 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