Fiche conseil - Sécurité SSI
Risques Cyber issus du télétravail

La situation de crise générée par l'épidémie du CORONAVIRUS – COVID-19 a généré depuis 15 jours une augmentation importante des attaques cyber.

Les cybercriminels cherchent à tirer profit de la baisse de vigilance des personnes directement ou indirectement concernées pour les abuser et qui va se retrouver amplifiée par l'accroissement de l'usage numérique lié aux mesures de confinement.

Ainsi compte tenu de l'accroissement du télétravail et de la dématérialisation des procédures qui en découlent, associé aux difficultés économiques risque d'escroquerie et cyber attaque accru. Il est donc primordial de transmettre aux collaborateurs en télétravail les quelques mesures résumées ci-dessous.

REGLES IMPORTANTES

- **Méfiez-vous des messages (mail, SMS, chat, …) ou appels téléphoniques d'origine inconnue.**
- **Ne téléchargez vos applications que depuis les sites ou magasins officiels des éditeurs.**
- **Vérifiez la fiabilité et la réputation des sites que vous visitez.**
- **Soyez attentifs aux fausses commandes ou aux modifications de virements bancaires frauduleux.**

SOMMAIRE

A. Évaluation

Dans le but d'une prévention efficace des risques cyber liés au télétravail, l'entreprise doit procéder à l'évaluation de ce risque :

Il est donc nécessaire de se poser les questions suivantes :

- Estimez-vous que **votre entreprise soit une cible potentielle** pour des pirates informatiques ?
- Pensez-vous que **les salariés en télétravail soient protégés convenablement** sur leur réseau personnel contre les actes d'intrusions, de sabotage ou de piratages ?
- Les salariés en télétravail ont-ils la possibilité de faire appel à une (/des) entreprise(s) extérieure(s) pour **la maintenance de leur réseau informatique & téléphonique personnel ?**
  Si oui, avez-vous pris des renseignements sur sa (leur) fiabilité et sa (leur) notoriété ?
- Avez-vous procédé à **un inventaire du matériel informatique fixe et mobile**, périphériques, câblages, etc. confiés aux salariés en télétravail ?
- Avez-vous procédé à un inventaire des **OS & logiciels, installés sur le matériel fixe et portable** de l'entreprise ?
- Le matériel informatique fixe et portable des salariés en télétravail est-il équipé **de logiciels de sécurité et d'un VPN** ?
- Le matériel nomade de l'entreprise (PC portables, téléphones mobiles, tablettes, etc.) est-il protégé en cas de connexion à des bornes Wifi implantées dans des lieux publics ou privés ?
- Vos salariés en télétravail **ont-ils été informés sur les dangers des réseaux sociaux et sur les conséquences encourues en cas de non-respect d'une certaine éthique** (communication sur des sujets sensibles, sur les rapports humains internes, etc.) ?
- Effectuez-vous une **veille des accès au réseau de l'entreprise** (Logs, tentatives d'accès, attaques, etc.) ?
- Avez-vous mis en place une **politique d'attribution et de gestion des droits d'utilisation** du Système d'Information en fonction des besoins de chaque salarié en télétravail ?
- **Réglementez-vous l'installation de tout nouveau matériel ou logiciel sur les ordinateurs** fixes et mobiles de l'entreprise ?

- Avez-vous mis en œuvre une **procédure d'authentification** (identification par login & mot de passe) des salariés en télétravail pour accéder au système d'information par VPN ?
- **Les salariés ont-ils été sensibilisés et/ou formés sur la confidentialité** qu'ils doivent accorder à leurs login et mots de passe ?
- Une **politique de changement des mots de passe** est-elle imposée aux utilisateurs ?
- Le personnel est-il sensibilisé aux **règles « élémentaires »** en matière de sécurité informatique (fermeture de session, etc.) ?
- Réglementez-vous la **connexion du matériel informatique mobile personnel** sur le réseau de l'entreprise (PC portables, clés USB, disques durs externes, PDA, cartes flash, etc.) ?
- Connaissez-vous **les organismes publics** (nationaux (ANSSI, CERTA, CLUSIF, etc.) et régionaux (CLUSIR, ENE, etc.)) susceptibles d'apporter une aide ou des conseils pour les salariés en télétravail ?

B. Classement par risque détecté pour mettre en place des actions de prévention

De cette évaluation doivent découler :

- Les processus de télétravail à risques,
- Les procédures de traitement et d'élimination des risques et la conduite à tenir en cas d'attaque détectée par le salarié à son domicile

L'évaluation des risques permet de déterminer, pour les collaborateurs en télétravail occupant des fonctions particulièrement exposées, les actions à mener face au risque Cyber.

L'employeur doit prendre les mesures de prévention nécessaires pour maîtriser ce risque sur les thèmes suivants :

- Information et mise en place
- Formation des salariés
- Acquisition d'équipement de protection de type VPN…

C. Préconisation sur la gestion des données sensibles en télétravail

- Dresser l'inventaire des informations à protéger selon leur niveau de confidentialité et de sensibilité accessibles à distance (celles qui procureraient un avantage à la concurrence).
  - Appréhender les enjeux liés aux informations détenues par l'établissement en concertation avec l'ensemble des services :
    - en établissant une grille de questions permettant d'apprécier la sensibilité de l'information en fonction de l'activité ;
    - en hiérarchisant la sensibilité des informations en fonction du préjudice qu'engendrerait leur divulgation (impact faible, moyen, fort) pour la vie de l'établissement ;
    - en évaluant les risques de fuite lors de la « vie opérationnelle de l'information », tout en appréciant en particulier s'il s'agit de risques humains et/ou techniques.
  - Toujours considérer comme d'une sensibilité stratégique les informations ayant un impact fort sur l'établissement. Elles doivent faire l'objet d'une protection spécifique, quelles que soient la difficulté d'accès et la probabilité de fuite.

  - Organiser la gestion des informations stratégiques tout au long de leur vie : qualification/déqualification, diffusion, reproduction, conservation, destruction.
- Définir, en fonction du support et de la "vie opérationnelle de l'information", les moyens les plus adaptés de protection et d'échange : meuble ou pièce sécurisés, conditions de stockage, chiffrement des données, code d'accès, utilisation d'une plateforme d'échange sécurisée, clauses spécifiques dans les contrats de travail, formation, etc.

D. Préconisation des situations à risques

- Désigner un responsable ou référent dans la gestion des télétravailleurs sur les risques cyber.
- Élaborer un document fixant les règles à mettre en œuvre selon les niveaux d'accessibilité aux informatios durant la période de télétravail.

E. Préconisation sensibilisation du personnel

- Expliquer au personnel en télétravail les enjeux de la sécurité des informations et présenter les bonnes pratiques ou les procédures adoptées lors de la mise en place de la politique de sécurité économique propre à l'entreprise.
- Mettre en place les moyens de sensibilisation et d'implication

F. Mesures et consignes a fixer avec le personnel en télétravail

- Détruire les informations sensibles et devenues inutiles durant le télétravail (
- Verrouiller les ordinateurs lors des absences du domicile (fermeture de session).
- Utiliser des codes d'accès complexes.
- Imposer aux télétravailleurs d'adopter une attitude vigilante envers les personnes étrangères à l'entreprise (visiteurs, stagiaires, clients, fournisseurs, etc.).
- Adopter une attitude réservée lors de la communication d'éléments concernant l'entreprise, surtout par téléphone.
- Se méfier des sondages et sensibiliser le personnel en télétravail sur les risques de phishing et alerte durant le COVID-19.
- Effectuer des sauvegardes périodiques de toutes les données.
- Procéder épisodiquement à des essais de restauration.

G. Gérer Les prestataires de service solliciter par les salariés en télétravail

Dans le contexte actuel de crise, les alliés d'aujourd'hui peuvent devenir les ennemis de demain. Aussi, gardez toujours à l'esprit qu'ils peuvent représenter une menace potentielle pour votre activité. Les mesures à prendre dans le cadre de la protection de l'information sont identiques à celles que vous mettrez en œuvre avec vos salariés, stagiaires ou visiteurs.

- Éviter de parler au téléphone de l'entreprise et de son activité pendant le voyage.
- Éviter de travailler sur son ordinateur portable ou consulter des documents confidentiels dans les transports publics.
- Éviter de rédiger le compte-rendu de réunion dans un espace ouvert.

- Éviter d'évoquer avec un de ses collaborateurs des sujets traités lors de la réunion et/ou de la visite.
- Ne jamais laisser sans surveillance dans un lieu public (véhicule en stationnement, train, avion, etc.) les différents supports confiés durant la période de télétravail.

H. Préconisation lors de déplacement à l'étranger ou télétravail hors frontière

- Définir un cadre précis à la mission en prévoyant notamment les sujets qui peuvent être abordés et ceux qui doivent être évités.
- Ne pas être porteur d'informations stratégiques sauf impérieuses nécessitées. Le cas échéant, prendre des dispositions afin de préserver ces informations (clé USB portée en permanence).
- Observer les lois et règlements du pays (surtout en matière de cryptage des données).
- Se méfier des rencontres « amicales spontanées ».
- Éviter les conversations à caractère professionnel pendant les transports (train, avion).
- Être prudents lors des comptes-rendus téléphoniques.
- La chambre d'hôtel et son coffre de sécurité n'offrent absolument aucune garantie. En votre absence, évitez d'y laisser des documents, matériels sensibles, ou des données personnelles même dans votre valise ou attaché-case fermés à clé.
- Rendre compte rapidement à la direction de tout incident.

I. Protection du matériel nomade lors de prêt de matériel de l'entreprise au salarié en télétravail

- Avant tout déplacement, mettre à jour les systèmes d'exploitation qui seront confiés aux télétravailleurs, logiciels et antivirus.
- Désactiver partiellement ou totalement les périphériques sur les postes de travail (port USB, lecteur CD, etc.).
- Utiliser un mot de passe personnel et solide (minimum de 8 caractères et éviter les mots du dictionnaire).
- Mettre en œuvre le verrouillage automatique de la session (réduire le délai de latence au minimum).
- Lors de votre retour dans l'entreprise, ne connecter les matériels nomades au réseau qu'une fois ceux-ci passés à l'anti-virus.
- Installer un filtre de confidentialité sur les écrans des ordinateurs portables, des tablettes et des smartphones à usage professionnel.
- Éviter de transporter les données sensibles lors des déplacements quotidiens, notamment entre le domicile et le travail. Si cela est indispensable, utiliser une clé USB sécurisée et la conserver en permanence sur soi.
- En cas d'utilisation des fonctions WiFi/Bluetooth des appareils nomades dans les transports en commun, garder à l'esprit que toute liaison peut être interceptée.

- Éviter au maximum de parler de sujets professionnels dans les transports en commun : métro, bus, taxi, train, avion.
- Rester discret dans ses lectures professionnelles (rapports, notes en cours, courriels, etc.) dans un lieu public.

Les conseils préconisés et redigées par RiskAttitude dans le cadre du partenariat avec le Groupe Cadre dans la présente fiche ne sont qu'une première sensibilisation des décideurs à la sureté numérique des salariés en télétravail .

L'attention des lecteurs est attirée sur la portée générale des conseils qui ne peuvent en aucun cas être considérés comme une réponse adaptée à chaque cas particulier.