SOLUCCIO
Les offres
CHAMBRE DE COMMERCE ET D'INDUSTRIE

REPRISE de l'activité

Fiche pratique : « Cybersécurité»

Synthèse des bonnes pratiques pour les employeurs et salariés en télétravail La crise du Coronavirus et le recours soudain au télétravail ont bousculé les habitudes de bon nombre d'entreprises. Le télétravail, bien que la meilleure solution permettant au plus grand nombre de collaborateurs de continuer à travailler, présente également quelques risques en matière de sécurité et protection des données, qu'il est facile de prévenir.

La CCI a compilé pour vous quelques recommandations que vous pourrez appliquer facilement, que vous soyez salarié ou dirigeant d'entreprise.
Sources : Cybermalveillance.gouv.fr

Employeurs

Pour faire face à la crise et au confinement imposé par l'épidémie du CORONAVIRUS – COVID-19 les employeurs, entreprises, associations, administrations, collectivités se sont vu devoir mettre en place ou développer dans l'urgence le télétravail pour maintenir, au moins a minima, leurs activités essentielles. L'ouverture vers l'extérieur du système d'information de l'entreprise peut engendrer des risques sérieux de sécurité qui pourraient mettre à mal l'entreprise, voire engager sa survie en cas de cyberattaque.

1. **Définissez et mettez en œuvre une politique d'équipement des télétravailleurs :** Privilégiez autant que possible pour le télétravail l'utilisation de moyens mis à disposition, sécurisés et maîtrisés par l'entreprise. Lorsque ce n'est pas possible, donnez des directives d'utilisation et de sécurisation claires aux employés en ayant conscience que leurs équipements personnels ne pourront jamais avoir un niveau de sécurité vérifiable (voire sont peut-être déjà compromis par leur usage personnel).

2. **Maîtrisez vos accès extérieurs :** Limitez l'ouverture de vos accès extérieurs ou distants (RDP) aux seules personnes et services indispensables, et filtrer strictement ces accès sur votre pare-feu. Cloisonnez les systèmes pour lesquels un accès à distance n'est pas nécessaire pour les préserver, surtout s'ils revêtent un caractère sensible pour l'activité de l'entreprise.

3. **Sécurisez vos accès extérieurs :** Systématisez les connexions sécurisées à vos infrastructures par l'emploi d'un « VPN » (Virtual Private Network ou « réseau privé virtuel » en français). Outre le chiffrement de vos connexions extérieures, ces dispositifs permettent également de renforcer la sécurité de vos accès distants en les limitant aux seuls équipements authentifiés. La mise en place sur ces connexions VPN d'une double authentification sera également à privilégier pour se prémunir de toute usurpation.

4. **Renforcez votre politique de gestion des mots de passe :** Qu'il s'agisse des mots de passe des utilisateurs en télétravail, mais aussi de ceux en charge du support informatique, les mots de passe doivent être suffisamment longs, complexes et uniques sur chaque équipement ou service utilisé. La majorité des attaques est due à des mots

de passe trop simples ou réutilisés. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois que cela est possible.

5. **Ayez une politique stricte de déploiement des mises à jour de sécurité :** Et ce, dès qu'elles sont disponibles et sur tous les équipements accessibles de votre système d'information (postes nomades, de bureau, tablettes, smartphones, serveurs, équipements réseaux ou de sécurité…) car les cybercriminels mettent peu de temps à exploiter les failles lorsqu'ils en ont connaissance. Un défaut de mise à jour d'un équipement est souvent la cause d'une intrusion dans le réseau des entreprises.

6. **Durcissez la sauvegarde de vos données et activités :** Les sauvegardes seront parfois le seul moyen pour l'entreprise de recouvrer ses données suite à une cyberattaque. Les sauvegardes doivent être réalisées et testées régulièrement pour s'assurer qu'elles fonctionnent. Des sauvegardes déconnectées sont souvent indispensables pour faire face à une attaque destructrice par rançongiciel (ransomware). En outre, il convient également de s'assurer du niveau de sauvegarde de ses hébergements externes (cloud, site Internet d'entreprise, service de messagerie…) pour s'assurer que le service souscrit est bien en adéquation avec les risques encourus par l'entreprise.

7. **Utilisez des solutions antivirales professionnelles :** Les solutions antivirales professionnelles permettent de protéger les entreprises de la plupart des attaques virales connues, mais également parfois des messages d'hameçonnage (phishing), voire de certains rançongiciels (ransomware). Utiliser des solutions différentes pour la protection des infrastructures et pour les terminaux peut s'avérer très complémentaire et donc démultiplier l'efficacité de la protection dans un principe de défense en profondeur.

8. **Mettez en place une journalisation de l'activité de tous vos équipements d'infrastructure :** Ayez une journalisation systématique et d'une durée de rétention suffisamment longue de tous les accès et activités de vos équipements d'infrastructure (serveurs, pare-feu, proxy…), voire des postes de travail. Cette journalisation sera souvent le seul moyen de pouvoir comprendre comment a pu se produire une cyberattaque et donc de pouvoir y remédier, ainsi que d'évaluer l'étendue de l'attaque.

9. **Supervisez l'activité de vos accès externes et systèmes sensibles :** Cette supervision doit vous permettre de pouvoir détecter toute activité anormale qui pourrait être le signe d'une cyberattaque, tels une connexion suspecte d'un utilisateur inconnu, ou d'un utilisateur connu en dehors de ses horaires habituels, ou encore un volume inhabituel de téléchargement d'informations…

10. **Sensibilisez et apportez un soutien réactif à vos collaborateurs en télétravail :** Donnez aux télétravailleurs des consignes claires sur ce qu'ils peuvent faire ou ne pas faire et sensibilisez-les aux risques de sécurité liés au télétravail. Cela doit se faire avec pédagogie pour vous assurer de leur adhésion et donc de l'efficacité des consignes. Les utilisateurs sont souvent le premier rempart pour éviter, voire détecter les cyberattaques. Ces utilisateurs coupés de leur entreprise ont également besoin d'un soutien de qualité et réactif pour éviter toute dérive.

11. **Dirigeants : impliquez-vous et montrez l'exemple !** La sécurité est toujours une contrainte qu'il faut accepter à la mesure des enjeux qui peuvent s'avérer vitaux pour les entreprises. L'implication et l'adhésion des dirigeants aux mesures de sécurité est indispensable, tout comme leur comportement qui doit se vouloir exemplaire afin de s'assurer de l'adhésion des collaborateurs.

Vous avez recours au télétravail pour maintenir votre activité. Vous ne disposez parfois pas d'équipement professionnel pour télétravailler et devez le faire avec vos moyens informatiques personnels (ordinateur, tablette, téléphone, comptes de messagerie…)
Afin de préserver au mieux la sécurité de votre entreprise et votre sécurité personnelle, appliquez les 10 recommandations suivantes :

1. **Si vous disposez d'équipements professionnels, séparez vos usages :** Séparez bien vos usages professionnels et personnels au risque de les confondre et de générer des fautes de sécurité qui pourraient être préjudiciables à votre entreprise. L'activité professionnelle doit se faire sur vos moyens professionnels et seulement sur vos moyens professionnels et l'activité personnelle doit se faire seulement sur vos moyens personnels.

2. **Appliquez strictement les consignes de sécurité de votre entreprise :** Ces mesures de sécurité visent à protéger votre entreprise, donc votre activité. Si vous rencontrez des difficultés à appliquer les mesures prescrites, l'information et demandez conseil à votre entreprise, mais ne les contournez pas de votre propre chef, car vous n'êtes probablement pas en mesure d'apprécier l'étendue des risques que vous pourriez prendre et faire prendre à votre entreprise.

3. **Ne faites pas en télétravail ce que vous ne feriez pas au bureau :** A fortiori sur vos équipements professionnels si vous en disposez. Ayez une utilisation responsable et vigilante de vos équipements et accès professionnels. Si vous utilisez vos moyens personnels en télétravail, ayez conscience que vos activités personnelles peuvent faire prendre un risque aussi à votre entreprise, redoublez donc d'attention et de prudence.

4. **Appliquez les mises à jour de sécurité sur tous vos équipements connectés (PC, tablettes, téléphones…) :** Et ce dès qu'elles vous sont proposées afin de corriger les failles de sécurité qui pourraient être utilisées par des pirates pour s'y introduire et les utiliser pour attaquer le réseau de votre entreprise au travers de vos accès.

5. **Vérifiez que vous utilisez bien un antivirus et scannez vos équipements :** Vérifiez que tous vos équipements connectés (PC, téléphones, tablettes…) sont bien protégés par un antivirus, qu'il est bien à jour, et effectuez une analyse complète (scan) de vos matériels. Si un matériel ne peut avoir d'antivirus, évitez le plus possible de l'utiliser pour accéder au réseau de votre entreprise

6. **Renforcez la sécurité de vos mots de passe :** Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipement et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est due à des mots de passe trop simples ou réutilisés. Au moindre doute ou même en prévention, changez-les et activez la double authentification chaque fois que cela est possible.

7. **Sécurisez votre connexion Wifi :** Le télétravail s'opère en général principalement sur votre connexion Wifi personnelle. Il est donc primordial de bien la sécuriser pour éviter toute intrusion sur votre réseau qui pourrait être utilisée pour attaquer votre entreprise. Utilisez un mot de passe suffisamment long et complexe (voir plus haut) et assurez-vous que vous utilisez bien le chiffrement de votre connexion en WPA2. Pensez également à mettre à jour régulièrement votre « box Internet » en la redémarrant ou depuis son interface d'administration.

8. **Sauvegardez régulièrement votre travail :** La sauvegarde est le seul moyen permettant de retrouver ses données en cas de cyberattaques, mais également en cas de panne ou de perte de son équipement. Si vous en avez la possibilité, sauvegardez régulièrement votre travail sur le réseau de l'entreprise ou les moyens qu'elle met à disposition à cet effet, mais aussi sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

9. **Méfiez-vous des messages inattendus :** Que ce soit par messagerie (email, SMS, chat…) en cas de message inattendu ou alarmiste, demandez toujours confirmation à l'émetteur par un autre moyen. Il peut s'agir d'une attaque par hameçonnage (phishing) visant à vous dérober des informations confidentielles (mots de passe), de l'envoi d'un virus par pièce-jointe ou d'un lien qui vous attirerait sur un site piégé, ou encore d'une tentative d'arnaque aux faux ordres de virement.

10. **N'installez vos applications que dans un cadre « officiel » et évitez les sites suspects :** Sur vos équipements professionnels, n'installez de nouvelles applications qu'après l'accord de votre support informatique. Sur vos équipements personnels utilisés en télétravail, n'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple : Apple App Store, Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater votre équipement. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streaming illégaux) qui pourraient également piéger vos équipements.

Cybermenaces et télétravail |

Avec l'intensification du télétravail, les cybercriminels vont chercher à mettre à profit la possible désorganisation et confusion des entreprises et organisations, ainsi que la dématérialisation des procédures qui en résulte, pour intensifier leurs attaques. Les principales cyberattaques que l'on peut envisager sont :

- **L'hameçonnage (phishing) :** Messages (email, SMS, chat…) visant à dérober des informations confidentielles (mots de passe, informations personnelles ou bancaires) en usurpant l'identité d'un tiers de confiance. Conséquences possibles : piratage de comptes professionnels de messagerie ou d'accès aux systèmes d'information de l'organisation, intrusion sur le réseau de l'entreprise, rançongiciels (ransomware), fraude aux faux ordres de virement…

- **Les rançongiciels (ransomware) :** Attaque qui consiste à chiffrer ou empêcher l'accès aux données de l'entreprise et à généralement réclamer une rançon pour les libérer. Ce type d'attaque s'accompagne de plus en plus souvent d'un vol de données et d'une destruction préalable des sauvegardes. Ces attaques sont généralement rendues possibles par une intrusion sur le réseau de l'entreprise, soit par ses accès à distance, soit par la compromission de l'équipement d'un collaborateur. Conséquence : arrêt de l'activité de l'entreprise, perte de données…

- **Le vol de données :** Attaque qui consiste à s'introduire sur le réseau de l'entreprise, ou sur ses hébergements externes (cloud), pour lui dérober des données afin de la faire « chanter », ou de les revendre, ou encore de les diffuser pour lui nuire. Comme pour les rançongiciels (cf. supra), ces attaques sont généralement possibles par une intrusion dans le réseau ou sur les systèmes hébergés de l'entreprise via ses accès à distance ou bien encore par la compromission du poste d'un collaborateur. Conséquences : atteinte à l'activité et à l'image de l'entreprise ou de l'organisation.

- **Les faux ordres de virement (FOVI/BEC) :** Escroquerie réalisée, parfois suite au piratage d'un compte de messagerie, par message et même téléphone, en usurpant l'identité d'un dirigeant ou d'un de ses mandataires, d'un fournisseur ou d'un prestataire, voire d'un collaborateur, pour demander un virement exceptionnel et confidentiel, ou un changement des coordonnées de règlement (RIB) d'une facture ou d'un salaire. Conséquence : perte financière pour l'entreprise ou l'organisation