INFORMATIQUE
09.51.40.21.64
06.75.94.21.64
contact@bpc-informatique.fr
www.bpc-informatique.fr

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

ADOPTER LES BONNES PRATIQUES

SÉCURISATION DU **TÉLÉTRAVAIL**

Le développement du télétravail présente de réelles opportunités tant pour les collaborateurs que pour les employeurs. Il nécessite toutefois généralement l'ouverture vers l'extérieur du système d'information de l'organisation (entreprise, collectivité, association), ce qui peut engendrer de sérieux risques de sécurité susceptibles de mettre à mal votre organisation, voire d'engager sa survie en cas de cyberattaque (rançongiciel, vol de données, faux ordres de virement...). **Voici 10 recommandations à mettre en œuvre pour limiter au mieux les risques.**

1 DÉFINISSEZ ET METTEZ EN ŒUVRE UNE POLITIQUE D'ÉQUIPEMENT DES TÉLÉTRAVAILLEURS

Privilégiez autant que possible l'utilisation de moyens mis à disposition, sécurisés et maîtrisés par votre organisation. 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 par un pare-feu l'ouverture de vos accès extérieurs ou distants (RDP par exemple) aux seules personnes et services indispensables, et filtrez strictement ces accès grâce à cet équipement de sécurité. Une attention toute particulière sera portée sur les éventuels accès de télémaintenance qui peuvent présenter une vulnérabilité importante s'ils sont compromis. Cloisonnez également 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 votre organisation (comme les réseaux de sauvegardes et les réseaux d'administration informatique par exemple).

3 SÉCURISEZ VOS ACCÈS EXTÉRIEURS

Systématisez les connexions sécurisées à vos infrastructures par l'utilisation 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 d'une double authentification sur ces connexions VPN 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 régulièrement en prévention, changez-les et activez la double authentification chaque fois que cela est possible. En savoir plus sur les mots de passe.

5 AYEZ UNE POLITIQUE STRICTE DE DÉPLOIEMENT DES MISES À JOUR DE SÉCURITÉ

Et ce, dès qu'elles sont disponibles et sur tous les matériels et logiciels 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 organisations. En savoir plus sur les mises à jour.

bpc INFORMATIQUE

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

6 DURCISSEZ LA SAUVEGARDE DE VOS DONNÉES

Les sauvegardes seront parfois le seul moyen pour l'organisation 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 **des données des postes nomades des collaborateurs et de celles de ses hébergements externes** (*cloud*, site Internet de l'organisation, service de messagerie…) pour vérifier que le service souscrit est bien en adéquation avec les risques encourus par votre organisation. En savoir plus sur les sauvegardes.

7 UTILISEZ DES SOLUTIONS ANTIVIRALES PROFESSIONNELLES

Ces solutions permettent de protéger les organisations 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 complémentaire et démultiplier ainsi l'efficacité de la protection dans un principe de défense en profondeur.

POUR ALLER PLUS LOIN

PAR L'ANSSI : Recommandations pour le nomadisme numérique
https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique

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 le plus rapidement possible 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 et formalisées sur ce qu'ils peuvent faire ou ne pas faire et sensibilisez-les aux risques de sécurité liés au télétravail. Cela, 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. Utilisez au besoin nos supports et notre kit de sensibilisation. Ces utilisateurs coupés de leur organisation ont également besoin d'un soutien de qualité et réactif pour éviter toute dérive.