INFORSUD TECHNOLOGIES
Solutions et impulsions pour l'avenir

SÉCURISATION DU TÉLÉTRAVAIL

10 bonnes pratiques !

Le développement du télétravail présente de réelles opportunités aussi bien pour les collaborateurs que pour les employeurs.
Il nécessite l'ouverture vers l'extérieur du système d'information de l'organisation, ce qui peut générer des risques d'intrusion.

1 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.

2 MAÎTRISEZ VOS ACCÈS EXTÉRIEURS

Limitez par un pare-feu l'ouverture de vos accès extérieurs ou distants aux seuls services et personnes indispensables, et filtrez strictement ces accès grâce à cet équipement de sécurité.

3 SÉCURISEZ VOS ACCÈS EXTÉRIEURS

Systématisez les connexions sécurisées à vos infrastructures par l'utilisation d'un « VPN ». Ces dispositifs chiffrent les connexions extérieures et renforcent la sécurité de vos accès distants en les limitant aux seuls équipements authentifiés.

4 RENFORCEZ VOTRE POLITIQUE DE GESTION DES MOTS DE PASSE

Les mots de passe doivent être suffisamment longs, complexes et uniques sur chaque équipement ou service utilisé. Au moindre doute 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 matériels et logiciels accessibles de votre système d'information car les cybercriminels mettent peu de temps à exploiter les failles lorsqu'ils en ont connaissance.

6 DURCISSEZ LA SAUVEGARDE DE VOS DONNÉES

Les sauvegardes seront parfois le seul moyen pour l'organisation de retrouver ses données suite à une cyberattaque ou un incident (vol, incendie, etc.). Les sauvegardes doivent être réalisées et testées régulièrement pour s'assurer qu'elles fonctionnent.

7 UTILISEZ DES ANTIVIRUS PROFESSIONNELS

Ces solutions permettent de protéger les organisations de la plupart des attaques virales connues, mais également de messages d'hameçonnage, voire de certains rançongiciels. **Astuce** : utiliser des solutions différentes pour la protection des infrastructures et pour les terminaux.

8 METTEZ EN PLACE UNE JOURNALISATION DE L'ACTIVITÉ DE TOUS VOS ÉQUIPEMENTS D'INFRASTRUCTURE

Une journalisation systématique et une durée de rétention suffisamment longue de tous les accès et activités de vos équipements seront souvent les seuls moyens de pouvoir comprendre comment a pu se produire une cyberattaque et donc de pouvoir y remédier.

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.

10 SENSIBILISEZ 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.

inforsud-technologies.com 0 811 349 609

« Cybermalveillance.gouv.fr – Données originales téléchargées sur Cybermalveillance.gouv.fr, publié le 11/2019. »