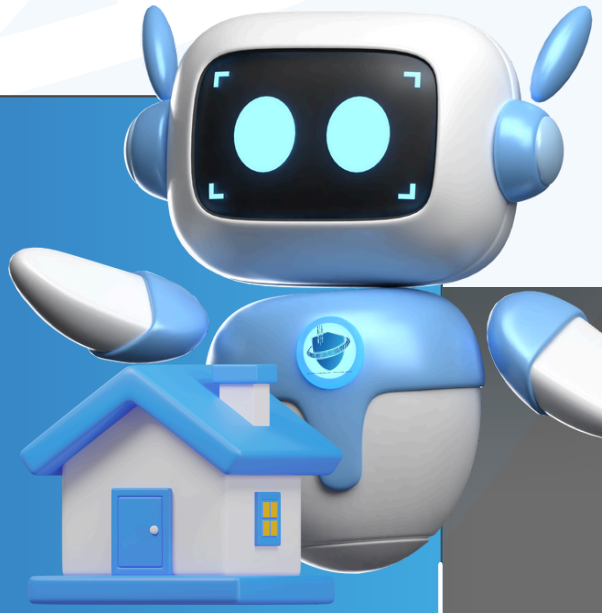
SÉCURISATION DU TÉLÉTRAVAIL

CENTRE CYBER DU PACIFIQUE

EN BREF



POURQUOI C'EST IMPORTANT ?

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
2. MAÎTRISEZ VOS ACCÈS EXTÉRIEURS
3. SÉCURISEZ VOS ACCÈS EXTÉRIEURS
4. RENFORCEZ VOTRE POLITIQUE DE GESTION DES MOTS DE PASSE
5. AYEZ UNE POLITIQUE STRICTE DE DÉPLOIEMENT DES MISES À JOUR DE SÉCURITÉ
6. DURCISSEZ LA SAUVEGARDE DE VOS DONNÉES
7. UTILISEZ DES SOLUTIONS ANTIVIRALES PROFESSIONNELLES
8. METTEZ EN PLACE UNE JOURNALISATION DE L'ACTIVITÉ DE TOUS VOS ÉQUIPEMENTS D'INFRASTRUCTURE
9. SUPERVISEZ L'ACTIVITÉ DE VOS ACCÈS EXTERNES ET SYSTÈMES SENSIBLES
10. SENSIBILISEZ ET APPORTEZ UN SOUTIEN RÉACTIF À VOS COLLABORATEURS EN TÉLÉTRAVAIL

▶ Voir détail page "10 RECOMMANDATIONS À METTRE EN ŒUVRE"

SÉCURISATION DU TÉLÉTRAVAIL

CENTRE CYBER DU PACIFIQUE

10 RECOMMANDATIONS À METTRE EN ŒUVRE

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 les accès distants aux personnes et services essentiels grâce à un pare-feu. Cloisonnez les systèmes n'ayant pas besoin d'accès distant, en particulier ceux qui gèrent des données sensibles, comme les réseaux de sauvegarde.

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

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.

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.

SÉCURISATION DU TÉLÉTRAVAIL

CENTRE CYBER DU PACIFIQUE

10 RECOMMANDATIONS À METTRE EN ŒUVRE

6. DURCISSEZ LA SAUVEGARDE DE VOS DONNÉES

Les sauvegardes régulières sont souvent le seul moyen de récupérer des données après une cyberattaque. Assurez-vous de leur bon fonctionnement et conservez des copies hors ligne pour éviter les rançongiciels. Vérifiez également la sauvegarde des données stockées à l'externe (cloud, messagerie).

7. UTILISEZ DES SOLUTIONS ANTIVIRALES PROFESSIONNELLES

Les solutions antivirus protègent contre la plupart des attaques, y compris les logiciels malveillants et le phishing. Utiliser différentes solutions pour les infrastructures et les terminaux peut renforcer la sécurité globale.

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

Conservez des journaux d'activité pour tous vos équipements (serveurs, pare-feu, proxy), afin de pouvoir retracer les événements en cas de cyberattaque. Cela permet aussi d'identifier comment l'attaque s'est produite et de limiter les dégâts.

9. SUPERVISEZ L'ACTIVITÉ DE VOS ACCÈS EXTERNES ET SYSTÈMES SENSIBLES

Surveillez en continu l'activité de vos systèmes sensibles et vos accès extérieurs pour repérer rapidement toute activité suspecte, telle que des connexions anormales ou des téléchargements inhabituels de données.

10. SENSIBILISEZ ET APPORTEZ UN SOUTIEN RÉACTIF À VOS COLLABORATEURS EN TÉLÉTRAVAIL

Formez vos collaborateurs aux bonnes pratiques de sécurité et informez-les des risques spécifiques au télétravail. Offrez un soutien rapide en cas de problème, car les utilisateurs sont souvent la première ligne de défense contre les cyberattaques.

POUR ALLER PLUS LOIN

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