GROUPEMENT DE GENDARMERIE DÉPARTEMENTALE
DE MEURTHE-ET-MOSELLE

Télétravail et règles de sécurité

31 Mars 2020

La situation de crise et de confinement liée à l'épidémie du CORONAVIRUS – COVID-19 engendre une intensification du recours au télétravail.

Une mise en œuvre du télétravail peut augmenter considérablement les risques de sécurité. Elle peut mettre en danger notre activité face à une cybercriminalité qui redouble d'efforts pour profiter de cette nouvelle opportunité.

> Dans certains cas, le télétravail s'opère depuis les équipements privés des personnels, dont le niveau de sécurité ne peut pas être évalué et encore moins garanti.

> Les salariés en télétravail qui utilisent leur équipement personnel peuvent être des cibles potentielles

Soyez vigilant / Quels sont les pièges à éviter ?

Les principales cyberattaques que l'on peut envisager sont :

- L'hameçonnage (phishing) : messages visant à dérober des informations confidentielles.
- Les rançongiciels (ransomware) : attaque qui consiste à chiffrer ou empêcher l'accès aux données.
- Le vol de données.
- Les faux ordres de virements.

Si vous êtes concernés par le télétravail et afin de préserver au mieux la sécurité de votre Système d'Information, appliquez les recommandations suivantes :

1. Si vous disposez d'équipements professionnels, séparez vos usages :
- utilisez des mots de passe différents pour tous les services professionnels et personnels,
- ne mélangez pas votre messagerie professionnelle et personnelle,
- méfiez-vous des supports USB.

2. Appliquez strictement les consignes de sécurité émises par votre employeur.

3. Ne faites pas en télétravail ce que vous ne feriez pas au bureau :
- si vous utilisez vos moyens personnels en télétravail, ayez conscience que vos activités personnelles peuvent faire prendre un risque à votre collectivité. Redoublez donc d'attention et de prudence.

4. Appliquez les mises à jour de sécurité sur tous vos équipements (PC, tablettes, téléphones…) :

5. Vérifiez que vous utilisez bien un antivirus et scannez vos équipements :
- vérifiez que tous vos équipements connectés sont bien protégés par un antivirus.

6. Renforcez la sécurité de vos mots de passe :
- utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels vous accédez,
- la majorité des attaques est due à des mots de passe trop simples ou réutilisés.

7. Sécurisez votre connexion WiFi :
- le télétravail s'opère en général principalement sur votre connexion WiFi personnelle,
- il est primordial de bien la sécuriser pour éviter toute intrusion sur votre réseau,
- utilisez un mot de passe suffisamment long et complexe avec chiffrement WPA2.

8. Sauvegardez régulièrement votre travail :
- sauvegardez régulièrement votre travail sur un support externe, que vous débranchez une fois la sauvegarde effectuée.

9. Méfiez-vous des messages inattendus :
- en cas de message inattendu ou alarmiste, demandez toujours confirmation à l'émetteur par un autre moyen.

10. Evitez les sites suspects :
- évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streaming illégaux).