Bulletin d'alerte

CYBER-MENACES ET COVID-19

GROUPEMENT DE GENDARMERIE DE LA GIRONDE

MESURES DE DECONFINEM

Les mesures de déconfinement vont permettre une reprise d'activité économique partielle ou totale. Toutefois, pour bien réussir cette étape sur le plan de la sécurité informatique, il convient de nouveau de rester très vigilant et d'adopter des mesures organisationnelles et techniques pour réduire les risques cyber.

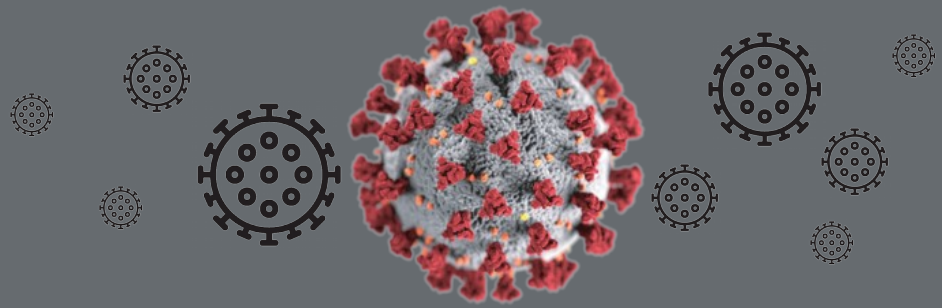
MESURES DE DECONFINEMENT : COMMENT ORGANISER SON RETOUR SUR LE SITE D'ACTIVITÉ ?

- **Procéder à un inventaire de chaque périphérique** (ordinateur, smartphone, etc.), de chaque **solution logicielle** (cloud, prise contrôle à distance, messagerie, etc.), et de toutes les **mesures de sécurité des systèmes d'information** prises dans l'urgence Afin d'apporter immédiatement un correctif pour s'assurer une reprise normale d'activité.

- Une attention toute particulière sera observée quant aux **accès ouverts des serveurs** pour faciliter les connexions de télétravail (RDP) et le recours aux logiciels (temporaires) de dépannage.

- Veiller à **accompagner chaque collaborateur** à la reprise d'activité sur site et procéder avec lui à un **inventaire de ses habitudes de travail** lors de son confinement. Identifier avec lui les **vulnérabilités** liées aux mesures prises.

- Avoir recours à la **communication, à la sensibilisation** de tous (sms, email, appels téléphoniques, …).



QUELQUES EXEMPLES DE CYBER-MENACES COVID-19 :

- **L'hameçonnage** (ou phishing) pour vous dérober des informations personnelles, professionnelles ou bancaires en vous attirant sur de faux sites officiels (promesse d'une (trop) bonne affaire, d'un remboursement, d'un colis en attente, d'un problème de sécurité, etc.).

- **Des faux ordres de virement international,** escroqueries à la fausse commande (usurpation de l'identité d'un employé, d'un fournisseur ou d'un dirigeant sous le sceau du secret, urgence, autorité, confidentialité, etc.).

- **Des demandes accompagnées de pièces jointes** qui peuvent furtivement compromettre votre ordinateur, voire chiffrer ces données afin de vous réclamer une rançon pour en retrouver l'accès (**rançongiciels**).

Gendarmerie nationale
200 Rue Judaïque, 33000 Bordeaux

10 BONNES PRATIQUES DE SÉCURITÉ INFORMATIQUE POUR RÉUSSIR SES MESURES DE DÉCONFINEMENT

1- Ne pas opérer dans la **précipitation**, **sous-estimer** les risques et **surévaluer** ses capacités. La reprise d'activité doit être menée prudemment par un sachant.

2- L'**activité générale de l'entreprise** (serveurs, postes individuels, …) doit être remise **progressivement** en fonction pour parer à toute compromission furtive.

3- Tous les **accès ouverts** pour faciliter le déploiement en télétravail doivent être **fermés et sécurisés**.

4- La principale priorité reste la **sauvegarde générale du système d'information** qui doit être testée et vérifiée. Une **deuxième copie hors réseau** est recommandée.

5- Tous les **ordinateurs** personnels ou d'entreprises **ayant servis en télétravail** doivent être **isolés et analysés** individuellement avant d'être remis sur le réseau (recours de préférence à une session invitée). Toutes les données produites depuis des ordinateurs personnels doivent être analysées puis décontaminées avant d'être intégrées au SI.

En cas d'intrusion sur votre système, **alertez (17)** et déposez plainte auprès des autorités compétentes.

Conservez toutes les preuves nécessaires à la bonne poursuite des investigations (en-tête d'émail, logs de journalisation, captures d'écran, ordinateurs, etc.).

POUR ALLER PLUS LOIN :

www.ssi.gouv.fr
www.cybermalveillance.gouv.fr
www.internet-signalement.gouv.fr

CYBERGEND NTECH INVESTIGATION & CRIMINALISTIQUE

6- Tous les **mots de passe** communiqués lors de la période de confinement (par sms, email,…) doivent être impérativement **changés**.

7- Une attention toute particulière sera portée aux diverses **applications de communication et visioconférence utilisées** par les collaborateurs lors du confinement (espaces de partage collaboratif en ligne, clouds ouverts).

8- Une fois le SI remis en état de fonctionnement « normal », faites procéder à une **analyse** (cf. scan) de **l'activité générale** et de tous les **accès restés ouverts ou récemment fermés** (identifier les tentatives d'accès légitimes ou illégitimes).

9- Une vigilance toute particulière sera observée sur **l'activité de votre réseau** dans **les jours suivants** la reprise d'activité (monitoring du réseau entre autre) et notamment les jours de non activité (week-end).

10- Une **veille sur internet** sur la « présence en ligne » de l'entreprise doit être opérée afin de déceler d'**éventuels oublis** notamment le partage de documents oubliés - cf. Dorks).