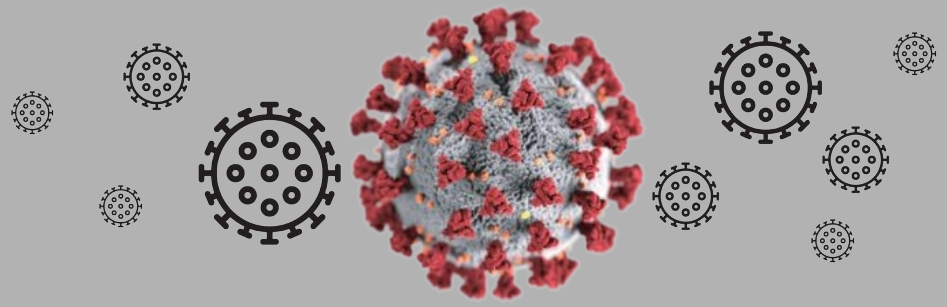
Bulletin d'information

CYBER-MENACES ET COVID-19

GROUPEMENT DE GENDARMERIE DU VAR

MESURES DE DÉCONFINEMENT

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 cyber-risques.



MESURES DE DÉCONFINEMENT : COMMENT S'ORGANISER POUR MINIMISER L'EXPOSITION AUX CYBER-RISQUES ?

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

- Veillez 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 et 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'une confirmation de commande, d'un colis en attente, d'un problème de sécurité, etc.).

- **Des escroqueries à la fausse commande** ou aux modifications de coordonnées de virement bancaire - FOVI (usurpation de l'identité d'un employé, d'un fournisseur ou d'un dirigeant sous le sceau du secret, etc.).

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

Gendarmerie nationale

307 Avenue Eole
83160 LA VALETTE DU VAR

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 à une session invitée non administrateur). Toutes les données produites depuis des ordinateurs personnels doivent être analysées puis décontaminées avant d'être intégrées au SI.

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** (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 partage de documents oubliés - Dorks).

RÉFÉRENTS GENDARMERIE

Le dispositif qui regroupe les 2 000 enquêteurs cyber de la gendarmerie (260 enquêteurs NTECH et 1 700 correspondants-NTECH) est désormais fédéré sous l'appellation« CYBERGEND ».

Ce réseau décentralisé assure un maillage sur tout le territoire national, aussi bien en métropole qu'outre-mer. Il constitue un ensemble de points de contact et de capacité d'action de proximité, doté de véritables capacités d'investigations. Il est piloté par le centre de lutte contre la cybercriminalité numérique (C3N) de Pontoise.

CONTACTS

Pour aller plus loin ou obtenir de l'information :

www.gendarmerie.interieur.gouv.fr
www.ssi.gouv.fr

Pour signaler :

- des piratages dans une entreprise : cyber@gendarmerie.interieur.gouv.fr
- des contenus illégaux sur internet : https://www.internet-signalement.gouv.fr
- des courriels ou sites d'escroquerie : https://www.internet-signalement.gouv.fr ou 0811 02 02 17
- des spams : https://www.signal-spam.fr
- des sites de phishing : https://phishing-initiative.fr
- des actes malveillants : https://www.cybermalveillance.gouv.fr
- pour les collectivités territoriales: https://www.ssi.gouv.fr/administration/guide/securite-numerique-des-collectivites-territoriales-lessentiel-de-la-reglementation/

EN CAS D'URGENCE, COMPOSEZ LE 17

Votre point de contact local : votre brigade de gendarmerie locale.
Selon la gravité de votre incident, ce point de contact local sera en mesure de faire intervenir des enquêteurs spécialisés en cybercriminalité.

En cas d'intrusion sur votre système, de campagne de dénigrement (refus de solidarité ou de don), atteinte à l'image de l'entreprise, ou toute autre tentative, alertez et déposez plainte auprès des autorités compétentes. **Conservez toutes les preuves nécessaires** à la bonne poursuite des investigations (en-tête d'email, logs de journalisation, captures écran, ordinateurs, etc.).