GROUPEMENT DE GENDARMERIE DES ALPES-MARITIMES

BULLETIN D'ALERTE

Vigilance face aux cyber menaces et escroqueries en période de Covid-19

Le coronavirus est actuellement le principal appât des pirates informatiques et de personnes malveillantes qui exploitent le besoin d'information sur l'évolution de la situation ou sur les aides mises en place par l'État, les collectivités, et certaines organisations publiques ou privées

Ces atteintes à la sécurité économique se révèlent parfois difficiles à identifier pour le dirigeant d'une petite ou moyenne entreprise et par les salariés eux-mêmes contraints par un mode de travail inhabituel. Ce nouvel environnement de travail pour certains organismes comporte des risques, c'est en ce sens que l'action de la gendarmerie s'inscrit en matière de SENSIBILISATION, d'ALERTE et d'ACCOMPAGNEMENT aux entreprises et collectivités

RECOMMANDATIONS POUR LES ENTREPRISES ET LES SALARIÉS EN TÉLÉTRAVAIL

✓ Mal protégé, le réseau informatique utilisé par une organisation ou une entreprise reste très vulnérable

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

BILAN SÉCURITÉ ET SAUVEGARDE DES DONNÉES

✓ Profitez du ralentissement de l'activité pour réaliser un check-up complet de l'architecture de votre réseau informatique, avec votre responsable informatique ou par un spécialiste dont la notoriété en cybersécurité est reconnue

✓ Optimisez la protection contre le vol de données, les pertes d'exploitation liées au blocage de l'activité par rançongiciel, ou la prise de contrôle à distance de votre système informatique.

✓ Veillez à sauvegarder régulièrement vos données pour protéger les actifs de l'entreprise : données clients, techniques, stratégie d'entreprise, de secret des affaires…

VIGILANCE SUR LES DÉPLACEMENTS OU EN TÉLÉTRAVAIL

✓ Appelez vos collaborateurs et salariés à renforcer leur vigilance lors de leurs déplacements domicile/lieu de travail, en particulier quant aux règles de protection de leurs équipements mobiles

✓ Suivez les conseils de l'Agence nationale chargée de la sécurité des systèmes d'information, sur l'utilisation d'équipements personnels pour un usage professionnel, en particulier dans le cadre d'une activité en télétravail, dont la mise en oeuvre a été favorisée et étendue à la survenance de la crise sanitaire actuelle.

CHARTE INFORMATIQUE

✓ Faites un rappel sur les droits et devoirs de chacun concernant les règles d'utilisation du réseau informatique au sein de l'entreprise.

✓ Énoncez clairement les sanctions encourues en cas de non respect des règles et faites signer des clauses de confidentialité.

DONS FRAUDULEUX & FAUSSES COMMANDES

✓ Prenez garde aux escroqueries qui profitent des chaînes de solidarité de fausses cagnottes en ligne, appelant à votre générosité par un appel aux dons destinés au financement de matériels consacrés à sauver des vies en raison de la crise actuelle : masques de protection, gels hydroalcooliques, tests de dépistage…

✓ Soyez vigilant sur la sollicitation d'un virement bancaire qui peut s'avérer frauduleux, la signature de documents ou la récupération des mots de passe nécessaires au piratage de vos données d'entreprise.

ATTESTATION DE DÉPLACEMENT

✓ Facilitez la mobilité de vos salariés en éditant des attestations de déplacement dérogatoire comportant le timbre officiel de l'entreprise

FAKE NEWS

- ✓ Ne partagez pas de fausses informations ou des vidéos qui peuvent être virales et amplifier ainsi une rumeur appelée à véhiculer des peurs et des scénarios catastrophiques.
- ✓ Analysez la source d'information, prenez le temps de la réflexion et adoptez au besoin une communication de crise au sein de l'entreprise.

L'HAMEÇONNAGE

- ✓ Méfiez-vous des mails, SMS, Chat et appels téléphoniques non identifiés. Cette technique dite du phishing est destinée à soustraire des informations personnelles, professionnelles ou bancaires en vous orientant sur de faux sites.

EN CAS D'INTRUSION PHYSIQUE DE VOTRE SYSTÈME SUR LE SITE DE L'ENTREPRISE

- ✓ Contactez la gendarmerie qui pourra vous conseiller et dépêcher un enquêteur spécialisé.
- ✓ Préservez les traces et indices laissés par un cambrioleur, en attendant la réalisation des opérations de police technique par un enquêteur.

EN CAS D'ATTEINTE À L'IMAGE DE L'ENTREPRISE OU COMPORTEMENT ILLICITE

- ✓ Signalez et déposez plainte à la gendarmerie pour toute tentative de chantage, ou de dénigrement sur le net, notamment en cas de refus de solidarité de la part de votre entreprise suite à un démarchage en ligne.

RÉAGIR EN CAS D'ATTAQUE MALVEILLANTE VIA INTERNET

- ✓ Coupez l'alimentation de l'internet, identifiez les postes infectés, lancez l'anti virus…
- ✓ Signalez et déposez plainte à la gendarmerie.

POUR SIGNALER :

- **Des piratages dans une entreprise : cyber@gendarmerie.inteireur.gouv.fr**
- **Des contenus illégaux sur internet : https://www.internet-signalement.gouv.fr**
- **Des courriels ou sites d'escroqueries : https://www.internet-signalement.gouv.fr ou 0811 02 02 17**
- **Des SPAMS : htpps://www.signal-spam.fr/**
- **Des sites de phishing : htpps://www.phishing-initiative.com/**
- **Actes malveillants : htpps://www.cybermalveillance.gouv.fr**

Ayez le réflex « Brigade numérique » ! En cette période de crise sanitaire, contactez la brigade numérique pour toute question relative à la sécurité !

https://www.gendarmerie.interieur.gouv.fr/CGU_CONTACT_NUMERIQUE

Pour aller plus loin et obtenir de l'information : www.gendarmerie.interieur.gouv.fr

En cas d'urgence composer le **17**

Vous serez relayé vers votre de point de contact local selon votre zone géographique. L'incident sera en mesure d'être pris en compte rapidement par des enquêteurs spécialisés en cybercriminalité

LES RÉFÉRENTS GENDARMERIE

Le dispositif qui regroupe les 2000 enquêteurs cyber de la gendarmerie (260 **enquêteurs en Nouvelles Technologies « NTECH » et 1700 Correspondants-NTECH)** est désormais fédéré sous l'appellation « CYBERGEND ». Ce réseau décentralisé assure un maillage sur tout le territoire national. Il constitue **un ensemble de points de contact et de capacité d'action de proximité, doté de véritables capacités d'investigations.**

Déployés dans l'ensemble des départements, en métropole et en outre-mer, les 234 référents sûreté de la gendarmerie agissent quotidiennement au profit des entreprises. Les référents sûreté peuvent **conseiller sur les mesures de protection à mettre en oeuvre pour lutter contre la cyberdélinquance** et orienter les chefs d'entreprises vers les référents sécurité économique et protection des entreprises ou le cas échéant, vers les enquêteurs du réseau Cybergend.

La gendarmerie nationale dispose d'un réseau de référents Sécurité Économique et Protection des Entreprises (SEcoPE) répartis sur toute l'étendue du territoire. Présents jusqu'au niveau départemental, ces référents **agissent pour prévenir les atteintes à la sécurité économique** et **sensibiliser les acteurs territoriaux** dans une dynamique de réseau et de partenariat. Le département des Alpes-Maritimes dispose d'une cellule entièrement dédiée sur ces missions. Votre contact local :

pole-ie-sophia@gendarmerie.interieur.gouv.fr