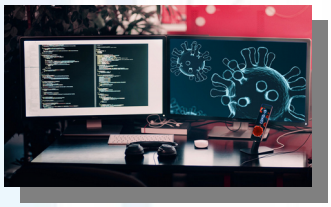
RÉGION DE GENDARMERIE AUVERGNE – RHÔNE-ALPES

Bulletin d'information Entreprises

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

Semaine 15 - Avril 2020 – N° 1

@ COVID-19 - Stop aux cybermenaces



Le coronavirus est actuellement le principal vecteur utilisé par les pirates informatiques pour attaquer les entreprises.

Ils exploitent les craintes des utilisateurs mais aussi le besoin d'informations sur les évolutions de la situation ou des dispositifs d'aides.

> **Mal protégé, le réseau informatique utilisé par une organisation ou une entreprise est vulnérable.**

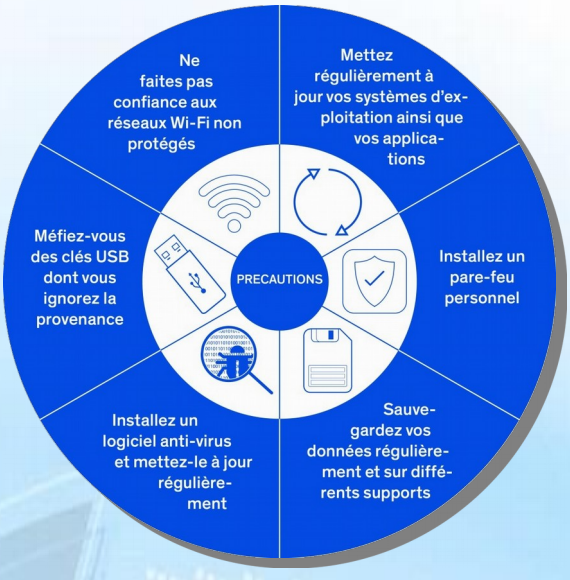
> **Mal informés, les collaborateurs en télétravail peuvent être des cibles potentielles !!!**

Recommandations pour les entreprises et les salariés

@ BILAN SÉCURITÉ ET SAUVEGARDE DES DONNÉES

● Profitez du ralentissement de l'activité pour faire un check-up complet des différentes composantes de votre réseau (*serveurs, matériel informatique, logiciels*, ...) avec votre responsable informatique.

● Sauvegardez régulièrement l'ensemble des données et réalisez périodiquement des essais de restauration pour en vérifier la viabilité. Dans la mesure du possible, privilégiez l'externalisation des sauvegardes. Toutefois, si cette démarche est réalisée sur support externe (*disque dur ou clé USB*), il conviendra alors de doubler voir de tripler le matériel et ce, afin de palier toute panne.



Sensibilisez régulièrement vos collaborateurs, les menaces étant en perpétuelle évolution.

@ LOGICIELS & MISE A JOURS

● Installez des logiciels de sécurité (*antivirus, anti-spams*, …) en vue de détecter et prévenir toute infection due à des logiciels malveillants, le vol de données, la prise de contrôle à distance du système informatique, ...

● Effectuez régulièrement les mises à jour de l'ensemble des logiciels présents dans les ordinateurs.

● En cas de mise en œuvre de mesures de télétravail, installez des logiciels permettant l'échange d'informations de manière sécurisée (*messagerie, VPN*, …).

@ 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 comme à l'extérieur.

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

Votre priorité : protéger la totalité des actifs de l'entreprise pour en assurer la pérennité.

@ DÉPLACEMENTS & TÉLÉTRAVAIL

● Invitez vos collaborateurs 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 de la Sécurité des Systèmes d'Information*** (*ANSSI*) et de ***Cybermalveillance.gouv.fr*** notamment en ce qui concerne l'utilisation d'équipements personnels pour un usage professionnel (*télétravail*).

Sécurité économique territoriale
Auvergne - Rhône-Alpes

Bureau renseignement – cellule sécurité économique
36 boulevard de l'Ouest 69580 SATHONAY-CAMP - Tél. : 04.37.85.21.15
rgra+intel-eco@gendarmerie.interieur.gouv.fr

Bulletin d'information N° 1

LES MENACES DU MOMENT

@ PHISHING

● Mails, SMS et appels téléphoniques non identifiés. Cette technique dite de « ***l'hameçonnage*** » est destinée à obtenir des données personnelles, professionnelles ou bancaires en vous orientant sur de faux sites.

@ RANSOMWARE

● Attaque informatique effectuée selon plusieurs modes : scan des ports ouverts des serveurs, mail contenant une pièce jointe infectée, lien internet frauduleux, fausse mise à jour, clé USB infectée, ...

@ ESCROQUERIES FINANCIÈRES

● Soyez vigilant lors de :

- toute sollicitation d'un virement bancaire, lequel peut s'avérer frauduleux (*escroquerie au faux président*).
- la réception de RIB semblant provenir de vos clients, fournisseurs et autres partenaires extérieurs suite à un prétendu changement de compte bancaire (*escroquerie dite au faux RIB*).

@ FAUSSES BOUTIQUES

● De nombreuses boutiques en ligne proposent à la vente divers produits médicaux (*masques, gel, gants , chloroquine, ...*) L'argent est encaissé mais la marchandise n'est jamais livrée.

@ APPELS AUX DONS

● Des escrocs profitent des chaînes de solidarité pour créer de fausses cagnottes en ligne. Ceux-ci font appel à votre générosité en sollicitant des dons destinés au financement de matériels médicaux en rapport avec la pandémie actuelle.

Entreprise / Gendarmerie
un partenariat GAGNANT - GAGNANT

@ RÉAGIR EN CAS D'ATTAQUE INFORMATIQUE

● **Isolez la machine infectée en la déconnectant du réseau.**

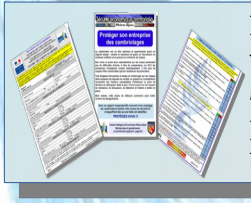
● **Faites rapidement intervenir le service informatique de l'entreprise, lequel prendra attache avec le service enquêteur pour obtenir la conduite à tenir.**

● **Déposez plainte à la gendarmerie.**

● **Alertez votre assureur** (*contrat cyber*)**.**

Pour tout renseignement, contactez la gendarmerie en privilégiant la *BRIGADE NUMÉRIQUE* *(pour toute situation non urgente - échanges par messagerie instantanée avec un gendarme 24h/24 et 7j/7)***.**

https://www.gendarmerie.interieur.gouv.fr/Brigade-numerique?service=redirection



Pour devenir acteur de votre sécurité, vous pouvez également souscrire à l'*Opération Tranquillité Entreprise*.

Pour cela, rapprochez-vous de la brigade de gendarmerie locale.

FAITS MARQUANTS

20/03/2020 : Les cyberdélinquants exploitant le rançongiciel Maze sont furieux. Leur dernière victime en date, une entreprise mondialement connue, a décidé de leur tenir tête. Disposant de sauvegardes viables, la société a pu reprendre son activité sans céder au chantage.

22/03/2020 : Une attaque par déni de service (*DDOS*) a touché un hôpital, bloquant l'ensemble des services informatiques.

30/03/2020 : Le serveur d'une mairie rhônalpine est attaqué à l'aide du ransomware *SODINOKIBI*. Ce malware est aussitôt détecté et bloqué par l'antivirus empêchant le chiffrement des données. Une rançon de plusieurs milliers d'Euros était exigée par les hackers.

INFO DE DERNIÈRE MINUTE

ALERTE ARNAQUE

Coronavirus (COVID-19)

Campagnes d'hameçonnage en cours *via* des **fausses lettres d'informations** sur le **Coronavirus** aux couleurs de **différents médias**.

Vous risquez le **blocage de votre appareil** par un support technique frauduleux !

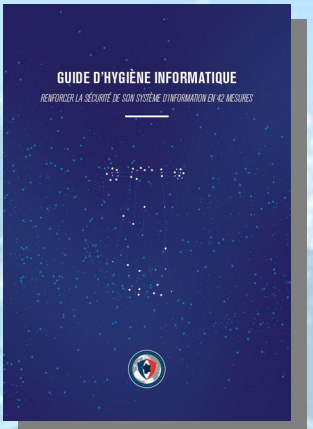
- **Méfiez-vous** des messages inattendus
- **Ne cliquez pas** sur les liens
- **N'appelez pas** le numéro indiqué
- **Si vous êtes bloqué**, redémarrez votre machine

Plus d'informations sur CYBERMALVEILLANCE.GOUV.FR Assistance et prévention du risque numérique

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/arnaques-au-faux-support-technique

POUR ALLER PLUS LOIN

(guides téléchargeables sur le site https://www.ssi.gouv.fr/)



Et consultez régulièrement le site
https://www.cybermalveillance.gouv.fr

Sécurité économique territoriale
Auvergne - Rhône-Alpes

Bureau renseignement – cellule sécurité économique
36 boulevard de l'Ouest 69580 SATHONAY-CAMP - Tél. : 04.37.85.21.15
rgra+intel-eco@gendarmerie.interieur.gouv.fr