RÉGION DE GENDARMERIE AUVERGNE – RHÔNE-ALPES

Bulletin d'information Entreprises

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

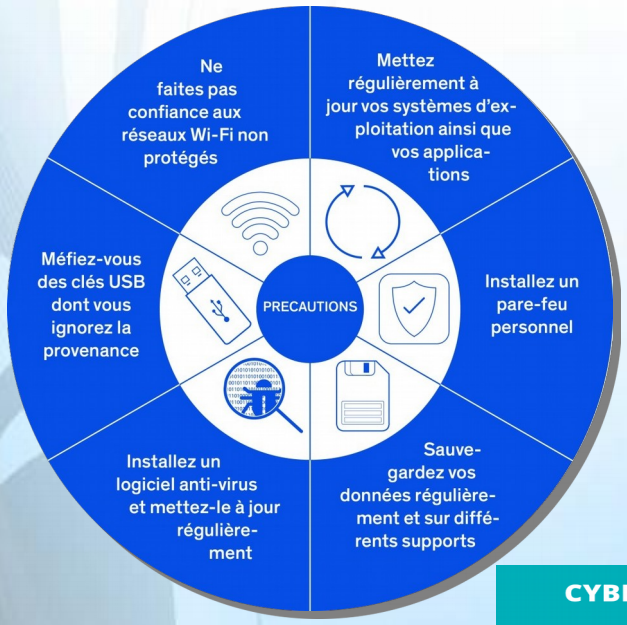
Juin 2020 – N° 4

Vacances estivales : « partez en toute *cybersérénité* » !

Déjà très affectées par la crise Covid, durant laquelle les cybercriminels n'ont pas chômé, les entreprises entrent désormais dans une nouvelle période critique pour leur sécurité, celle des vacances estivales. Leur mode de fonctionnement va une nouvelle fois être altéré (*effectifs réduits, renforts extérieurs, télétravail, fermeture totale, …****).***

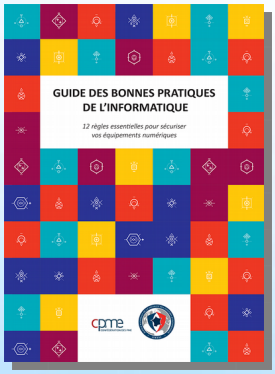
A l'approche des congés, il est toutefois essentiel de rappeler que les hackers et escrocs en tous genres, eux, ne prennent pas de vacances, bien au contraire.

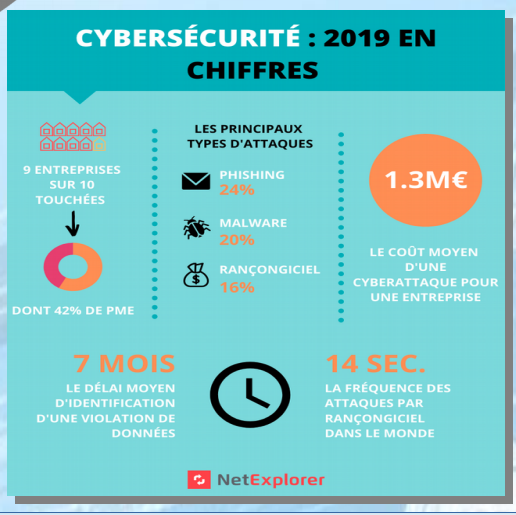
Il convient donc de procéder à des opérations de sensibilisation mais aussi d'inciter l'ensemble des salariés à appliquer de manière encore plus stricte qu'à l'accoutumée, les règles essentielles d'hygiène informatique ainsi que les procédures mises en place notamment en ce qui concerne les virements bancaires.



POUR ALLER PLUS LOIN

(Cliquer sur l'image pour télécharger le guide)





A LA UNE

Au mois de mars 2020, en pleine crise sanitaire, le réseau informatique d'une PME est chiffré à l'aide d'un ransomware. Refusant de régler la rançon exigée *(environ 50 000€)*, et n'ayant que des portions de sauvegardes viables, l'entreprise se retrouve à l'arrêt et subit un sérieux manque à gagner.

Début juin, alors qu'elle venait de redémarrer son activité en mode dégradé, et suite au non-paiement de la rançon, l'entreprise apprend que de nombreuses données exfiltrées par les hackers lors de l'attaque initiale sont désormais en vente sur le dark-web.

Sites de référence

https://www.ssi.gouv.fr/

https://www.cybermalveillance.gouv.fr

https://www.ene.fr/

https://ma-solution-numerique.fr/

Formation à la cybersécurité

https://secnumacademie.gouv.fr/

IMPORTANT

La cybersécurité n'étant qu'une des composantes de la sécurité globale de l'entreprise, il convient de s'intéresser également à la sécurité physique des locaux. Pour vous aider dans cette démarche, depuis 2012, la région de gendarmerie Auvergne – Rhône-Alpes a mis en œuvre ***l'OPÉRATION TRANQUILLITÉ ENTREPRISES (OTE).***

Pour plus d'informations ou pour vous inscrire, merci de consulter les deux pièces jointes au présent bulletin d'information.

Alerte aux rançongiciels

Vos données en otage, contre de l'argent !

Vous êtes de plus en plus nombreux à recevoir des messages douteux avec des pièces jointes et/ou des liens qui sont piégés, ***NE CLIQUEZ PAS DESSUS !***

Un virus pourrait chiffrer vos données et exiger une rançon. La payer ne garantit pas la récupération de l'intégralité de vos données.

Il est constaté de plus en plus d'**escroqueries** par des emails qui contiennent des pièces jointes et/ou des liens piégés. **Ces messages frauduleux sont maintenant plus difficiles à détecter** par les utilisateurs car ils sont bien souvent de parfaites copies, avec de vrais logos et sans faute d'orthographe.

VOICI QUELQUES RÈGLES DE BON SENS QU'IL FAUT ABSOLUMENT RESPECTER :

Ces réflexes sont indispensables et peuvent sauver votre entreprise !

N'ouvrez pas les messages dont la provenance ou la forme est douteuse.
Apprenez à distinguer des emails piégés en deux minutes sur :
https://www.hack-academy.fr/candidats/willy

Effectuez des sauvegardes régulières de vos données.
Déplacez physiquement la sauvegarde de votre réseau et placez-la en lieu sûr.
Assurez-vous aussi qu'elle fonctionne.

Mettez à jour vos principaux outils : Windows, antivirus, lecteur PDF, navigateur, etc.
Et si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera la propagation des rançongiciels via les vulnérabilités des applications.

Créer un compte « utilisateur » et n'utilisez que celui-ci, une fois votre ordinateur configuré.
Cette règle ralentira l'escroc dans ses actions malveillantes.

Bureau renseignement – cellule sécurité économique
36 boulevard de l'Ouest 69580 SATHONAY-CAMP

Bulletin d'information Entreprise N° 4

HAMEÇONNAGE

On vous incite à communiquer des informations importantes ? Ne tombez pas dans le piège.

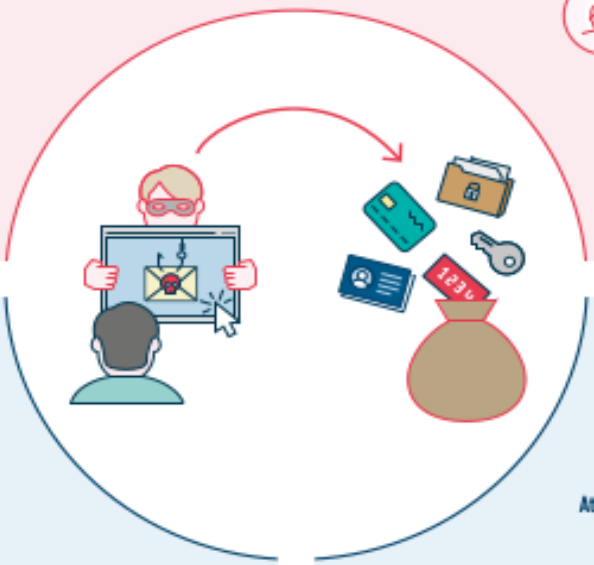
QUE SE PASSE-T-IL ?

1. Vous recevez un courriel piégé

Le courriel suspect vous invite à :
- diguer sur une pièce-jointe ou un lien piégés
- communiquer des informations personnelles

2. L'attaquant se fait passer pour une personne ou un tiers de confiance

L'attaquant est alors en mesure de :
- prendre le contrôle de votre système
- faire usage de vos informations



Impact de l'attaque

Intégrité — **Authenticité** — Disponibilité

Confidentialité

Motivations principales

Atteinte à l'image — **Appât du gain** — **Nuisance**

Revendication — **Espionnage** — **Sabotage**

COMMENT RÉAGIR ?

Vous êtes victime – Ne perdez pas un instant !

1- Renouvelez immédiatement les identifiants des comptes compromis

2- Contactez votre service informatique ou un expert (ou trouvez le vôtre sur www.cybermalveillance.gouv.fr)

3- Signalez l'incident sur PHAROS (www.internet-signalement.gouv.fr)

4- Portez plainte auprès des services compétents (www.ssi.gouv.fr/en-cas-dincident)

5- Plus de conseils avec INFO ESCROQUERIES au 0 805 805 817 (numéro gratuit)

COMMENT SE PROTÉGER ?

Ne tombez pas dans le piège

- Ne cliquez jamais sur un lien ou une pièce-jointe qui vous semblent douteux
- Ne répondez jamais à un courriel suspect. Au moindre doute, contactez l'expéditeur par un autre canal.
- Evitez l'effet boule de neige ! Disposez d'un mot de passe unique pour chaque application.
  + de conseils avec la CNIL : www.cnil.fr/fr/tag/mots-de-passe
- Vérifiez les paramètres de sécurité de votre compte de messagerie.
- Activez l'authentification à double facteur (la plupart des fournisseurs de messagerie le propose)

#CyberVigilant ! En savoir plus sur les attaques par hameçonnage :
www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001
www.cybermalveillance.gouv.fr/nos-articles/hameconnage-phishing

Sécurité économique territoriale
Auvergne - Rhône-Alpes

Bureau renseignement – cellule sécurité économique
36 boulevard de l'Ouest 69580 SATHONAY-CAMP

Bulletin d'information Entreprise N° 4

ESCROQUERIES FINANCIÈRES
Bien réagir pour s'en prémunir

Apparues en 2005, les escroqueries aux faux ordres de virement ont touché plusieurs milliers d'entreprises pour un montant total supérieur à 700 millions d'euros.

Depuis le début de la crise du coronavirus, plus d'une soixantaine d'escroqueries liées à l'achat de matériels médicaux ou de protection ont été recensées en France, pour un préjudice estimé à plus de 11 millions d'euros.

De très nombreuses autres tentatives ont heureusement échoué. Si elles avaient réussi, elles auraient rapporté 40 millions d'euros supplémentaires à leurs auteurs *(1)*.

CAS CONCRET : Un individu se présentant comme dirigeant d'une société de vente de produits médicaux contacte une PME pour lui proposer d'importantes quantités de matériels de protection contre le COVID-19 à des prix défiants toute concurrence.

Suite aux vérifications d'usage réalisées par le biais d'internet, le PDG constate que si la société existe bien, le nom du dirigeant lui, ne correspond pas. L'entreprise ne donne pas suite malgré de nombreuses relances.

MESURES DE PRÉVENTION / PROTECTION

- **Vérifier l'existence et l'application de procédures internes concernant virements et achats.**
- **Sensibiliser régulièrement les équipes financières et comptables ainsi que tout salarié exerçant une fonction «filtre»** (*secrétaire, assistante de direction, standardiste,...*).
- **Former les salariés au bon usage des moyens informatiques, aux dangers des réseaux sociaux ainsi qu'à la protection de l'information. Les responsabiliser par la mise en place de chartes.**
- **Ne pas rendre public l'organigramme de l'entreprise pour ne pas faciliter la collecte d'informations de l'escroc.**
- **Lorsqu'une demande de virement est faite hors du formalisme habituel, exiger une sollicitation écrite provenant d'une adresse mail professionnelle, ainsi qu'un numéro de téléphone fixe (et non portable) qui seront systématiquement vérifiés.**
- **Orienter l'interlocuteur vers la procédure régulière, et ne rien entreprendre sans l'aval de la hiérarchie.**
- **Ne communiquer aucun code confidentiel par téléphone, fax ou courriel.**

En cas de problème avéré ou de simple tentative : alerter immédiatement la banque pour bloquer les fonds.
Déposer rapidement plainte auprès du service de gendarmerie ou de police territorialement compétent.

Bureau renseignement – cellule sécurité économique
36 boulevard de l'Ouest 69580 SATHONAY-CAMP