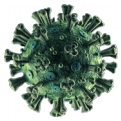
Groupement de gendarmerie du Haut Rhin

Bulletin d'alerte

Avril 2020

@ Stop aux cybermenaces en période de Covid-19



Le coronavirus est actuellement le principal appât des pirates informatiques qui exploitent le besoin d'information sur l'évolution de la situation ou sur les aides

- Mal protégé, le réseau informatique utilisé par une organisation ou une entreprise reste vulnérable
- Les salariés en télétravail qui utilisent leur équipement personnel peuvent être des cibles potentielles

Soyez vigilant / Quels sont les pièges à éviter ?

Recommandations pour les entreprises et les salariés en télétravail

@ BILAN SÉCURITÉ ET SAUVEGARDE DES DONNÉES

● PROFITEZ DU RALENTISSEMENT DE L'ACTIVITÉ POUR FAIRE UN CHECK-UP COMPLET AVEC VOTRE RESPONSABLE INFORMATIQUE OU 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.

● VEILLER À SAUVEGARDER RÉGULIÈREMENT VOS DONNÉES POUR PROTÉGER LES ACTIFS DE L'ENTREPRISE.

@ CHARTE INFORMATIQUE

● FAITE UN RAPPEL SUR LES DROITS ET DEVOIRS DE CHACUN CONCERNANT LES RÈGLES D'UTILISATION DU RÉSEAU INFORMATIQUE AU SEIN DE L'ENTREPRISE,

● ÉNONCER CLAIREMENT LES SANCTIONS ENCOURUES EN CAS DE NON RESPECT DES RÈGLES ET FAIRE SIGNER DES CLAUSES DE CONFIDENTIALITÉ.

@ VIGILANCE LORS DES 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.

● SUIVRE 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 ŒUVRE A ÉTÉ FAVORISÉE ET ÉTENDUE À L'AUNE DE LA CRISE SANITAIRE ACTUELLE.

@ DONS FRAUDULEUX

● PRENEZ GARDE AUX ESCROQUERIES QUI PROFITENT DES CHAÎNES DE SOLIDARITÉ ET FAUSSES CAGNOTTES EN LIGNE, APPELANT À VOTRE GÉNÉROSITÉ PAR UN APPEL AUX DONS DESTINÉS AU FINANCEMENT DE MATÉRIELS DESTINÉS À SAUVER DES VIES EN RAISON DE LA CRISE ACTUELLE (MASQUES, GELS HYDROALCOOLIQUES, TESTS DE DÉPISTAGES…).

Prévenez les menaces

En renforçant la cybersécurité et en diffusant des mesures de vigilance

Sensibilisez vos salariés

Sur les risques liés aux usages du numériques, renforcez les mesures de sécurité.

Protégez les actifs de votre entreprise

Pour assurer un plan de continuité et reprise d'activité

ATTESTATIONS DE DÉPLACEMENT : FACILITEZ LA MOBILITÉ DE VOS SALARIÉS EN ÉDITANT DES ATTESTATIONS DE DÉPLACEMENT DÉROGATOIRE COMPORTANT LE TIMBRE OFFICIEL DE L'ENTREPRISE.

Contactez votre brigade locale

@ FAKES NEWS

● NE PARTAGEZ PAS DE FAUSSES INFORMATIONS OU DES VIDÉOS QUI PEUVENT ÊTRE VIRALES, ET AMPLIFIER AINSI UNE RUMEUR DESTINÉE À VÉHICULER DES PEURS ET DES SCÉNARIOS CATASTROPHIQUES.

● ANALYSER LA SOURCE D'INFORMATION, PRENEZ LE TEMPS DE LA RÉFLEXION ET ADOPTER 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.

@ FAUSSES COMMANDES

● SOYEZ VIGILANT SUR LA SOLLICITATION D'UN VIREMENT BANCAIRE OU DEMANDE DE CHANGEMENT DE RIB QUI PEUT S'AVÉRER FRAUDULEUX, LA SIGNATURE DE DOCUMENTS OU LA RÉCUPÉRATION DES MOTS DE PASSE NÉCESSAIRES AU PIRATAGE DE VOS DONNÉES D'ENTREPRISE.

@ FAUX ORDRES DE VIREMENT

● SENSIBILISER L'ENSEMBLE DES EMPLOYÉS ;

● INSTAURER DES PROCÉDURES DE VÉRIFICATION ;

● ROMPRE LA CHAINE DES MAILS EN SAISISSANT SOI-MÊME L'ADRESSE HABITUELLE DU DONNEUR D'ORDRE ;

● ACCENTUER LA VIGILANCE EN CETTE PÉRIODE DE TÉLÉ-TRAVAIL

En cas de doute, la gendarmerie est à vos cotés

@ 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 LA GENDARMERIE.

@ 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 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

● COUPER L'ALIMENTATION D'INTERNET, IDENTIFIER LES POSTES INFECTÉS, LANCER L'ANTI-VIRUS…

● SIGNALEZ ET DÉPOSEZ PLAINTE À LA GENDARMERIE.

● CONSERVEZ LES MAILS ORIGINAUX SANS LES RETRANSMETTRE

Référents gendarmerie

Le dispositif qui regroupe plus de 5300 enquêteurs cyber de la gendarmerie (300 enquêteurs N'Tech et 5000 correspondants N'Tech) 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'investigation. Il est piloté par le pôle national de lutte contre les cybermenaces.

Déployés dans l'ensemble des départements, les 234 référents sûreté de la gendarmerie agissent quotidiennement au profit des entreprises. Au delà de leur expertise dans la prévention technique de la malveillance, les référents sûreté peuvent conseiller sur les mesures de protection à mettre en œuvre pour lutter contre la cybercriminalité et orienter les chefs d'entreprise vers les référents intelligence économique des régions ou le cas échéant, vers les enquêteurs du réseau « cybergend ».

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 entreprises : ***cyber@gendarmerie.interieur.gouv.fr***
- des contenus illégaux sur internet : ***https://wwwinternet-signalement.gouv.fr***
- des courriels ou sites d'escroquerie : ***https://www.internet-signalement.gouv.fr ou 0805 805 817***
- des spams : https://signal-spam.fr
- Les cybermalveillances : ***https://www.cybermelveillances.gouv.fr***

En cas d'urgence composez le 17

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

Contactez votre brigade locale