TAVITA CYBERSECURITY
GARDIEN CYBER DES TERRITOIRES

À AFFICHER · À GARDER SOUS LA MAIN

CYBERATTAQUE : LES BONS RÉFLEXES POUR RÉAGIR

Ce que vous faites dans la première heure conditionne tout le reste : la reprise d'activité, l'indemnisation, la responsabilité de l'entreprise. Ce mémo vous dit quoi faire, quoi ne pas faire, et qui appeler.

RECONNAÎTRE UNE ATTAQUE

Des fichiers illisibles avec une extension inconnue et un message de rançon ; des collègues ou clients qui reçoivent des e-mails que vous n'avez pas envoyés ; une demande de changement de RIB ou un virement « urgent » ; un mot de passe qui ne fonctionne plus ; des connexions à des heures ou depuis des lieux inhabituels ; un site web défiguré ou inaccessible ; une lenteur générale inexpliquée. **Un seul de ces signaux justifie de s'arrêter et d'appeler.**

LA PREMIÈRE HEURE : 6 GESTES

1 Isoler sans éteindre
Débranchez le câble réseau ou coupez le Wi-Fi des machines suspectes. Ne les éteignez pas : la mémoire vive contient des preuves.

2 Noter l'heure et photographier
Écrans de rançon, messages d'erreur, e-mails suspects : photos avec votre téléphone, heure de chaque constat, qui a vu quoi.

3 Alerter en interne
Prévenez la direction et la personne qui gère l'informatique. Désignez un interlocuteur unique pour la suite.

4 Changer les accès critiques
Depuis un appareil sain : comptes administrateurs, messagerie, banque en ligne. Activez la double authentification.

5 Appeler la banque si un virement est en jeu
Demandez le rappel des fonds immédiatement ; passées quelques heures, l'argent est perdu.

6 Appeler un professionnel
TAVITA CYBERSECURITY : +33 6 99 63 17 11 · +689 87 30 41 25. Prise en main à distance dès l'appel.

CE QU'IL NE FAUT SURTOUT PAS FAIRE

Ne pas payer

La rançon ne garantit rien

- Aucune garantie de récupérer les données
- Finance l'attaque suivante et vous désigne comme payeur
- Position de l'ANSSI et du gouvernement

Ne pas effacer

Ni réinstaller, ni restaurer trop vite

- Vous détruisez les preuves nécessaires à la plainte et à l'assureur
- Vous risquez de réinstaller l'attaquant avec la sauvegarde
- Attendez le feu vert de l'expert

Ne pas communiquer seul

Ni avec l'attaquant, ni en public

- Pas de réponse au pirate, pas de négociation
- Rien sur les réseaux sociaux avant d'avoir cadré le message
- Clients, partenaires, presse : avec un plan

PLAINTE · 72 H
Gendarmerie ou police, avec vos photos et notes. Sans plainte sous 72 h, pas d'indemnisation par l'assureur (loi LOPMI).

CNIL · 72 H
Dès qu'une donnée personnelle (client, salarié, usager) a pu être consultée ou volée : notification sur cnil.fr, information des personnes si le risque est élevé.

ASSUREUR · ANSSI · 17CYBER
Déclaration de sinistre dans les délais du contrat ; signalement ANSSI (obligatoire sous 24 h en NIS 2) ; parcours d'assistance sur 17cyber.gouv.fr.

Choisir TAVITA CYBERSECURITY, c'est faire le choix d'un partenaire de confiance, expert, réactif et engagé pour la protection durable de votre système d'information.

SELON LE TYPE D'ATTAQUE → VERSO

SELON LE TYPE D'ATTAQUE, LES BONS RÉFLEXES

Rançongiciel (fichiers chiffrés)

Signes : fichiers illisibles, extension inconnue, note de rançon, serveurs inaccessibles.

- Isolez toutes les machines touchées, débranchez les NAS et disques de sauvegarde encore connectés
- Ne payez pas, ne négociez pas, conservez la note de rançon
- Vérifiez que vos sauvegardes hors ligne sont intactes avant toute restauration
- Considérez que les données ont aussi été volées : préparez la notification CNIL

Messagerie piratée

Signes : envois que vous n'avez pas faits, règles de transfert inconnues, contacts qui reçoivent des factures ou des RIB.

- Changez le mot de passe depuis un appareil sain et activez la double authentification
- Supprimez les règles de redirection automatique créées par l'attaquant
- Déconnectez toutes les sessions actives et révoquez les applications tierces
- Prévenez vos contacts : ils sont la prochaine cible

Fraude au virement / faux RIB

Signes : demande urgente d'un « dirigeant » ou d'un fournisseur, changement de coordonnées bancaires, pression au secret.

- Appelez la banque immédiatement pour un rappel de fonds
- Confirmez tout changement de RIB par un appel au numéro habituel du fournisseur, jamais celui du mail
- Déposez plainte sous 72 h avec l'e-mail, le RIB et l'ordre de virement
- Vérifiez si votre messagerie a été compromise en amont

Fuite ou vol de données

Signes : données de l'entreprise en vente en ligne, clients contactés par des escrocs avec vos informations, alerte d'un partenaire.

- Identifiez quelles données et combien de personnes sont concernées
- Notifiez la CNIL sous 72 h ; informez les personnes si le risque est élevé
- Changez les identifiants exposés, surveillez les usages frauduleux
- Préparez un message clair pour vos clients et partenaires

Site web défiguré ou hors ligne

Signes : page modifiée, message politique, redirection, site injoignable (DDoS).

- Mettez le site en maintenance, contactez votre hébergeur
- Changez les accès d'administration et de l'hébergement
- Restaurez depuis une sauvegarde saine après correction de la faille
- Prévenez vos clients pour éviter qu'ils saisissent des données sur le faux site

Faux support ou faux conseiller

Signes : appel « de Microsoft », « de la banque » ou « des impôts » demandant un accès à distance, un code ou un virement.

- Raccrochez, ne donnez jamais de code reçu par SMS
- Si un accès à distance a été donné : débranchez, changez tous les mots de passe
- Rappelez l'organisme au numéro officiel, pas à celui de l'appel
- Signalez sur 17cyber.gouv.fr et à votre banque si un paiement a été fait

LES JOURS SUIVANTS

Ne remettez rien en service sans savoir par où l'attaquant est entré : c'est l'objet de l'analyse. Restaurez par ordre de priorité métier, depuis des sauvegardes vérifiées, sur des systèmes réinitialisés. Gardez une chronologie écrite de tout ce qui a été fait — l'assureur et les autorités la demanderont. Une fois l'activité reprise, corrigez ce qui a permis l'attaque (double authentification, sauvegardes hors ligne, mises à jour, formation de l'équipe) et faites un retour d'expérience à froid, sans chercher de coupable.

UN PROFESSIONNEL À VOS CÔTÉS

David TOUCHE Gérant et consultant en cybersécurité, TAVITA CYBERSECURITY

Ancien des forces armées, 23 ans au Ministère des Armées, label ExpertCyber, ISO/IEC 27005 Risk Manager. 11 crises cyber gérées en cinq ans en Polynésie française et en Martinique. Il prend la main à distance dès votre appel, se déplace si nécessaire, et s'occupe des déclarations avec vous.

EN CAS DE DOUTE, APPELEZ.

Un premier échange n'engage à rien et évite les erreurs irréversibles des premières heures. Mieux vaut un appel pour rien qu'une semaine d'arrêt.

contact@tavita-cybersecurity.com
+33 6 99 63 17 11 · +689 87 30 41 25
www.tavita-cybersecurity.com
Nous suivre : linktr.ee/TAVITACYBERSECURITY
SIRET 798 544 722 00035 · N° Tahiti E31755 · RCS 211712A