HAUT-COMMISSARIAT
DE LA RÉPUBLIQUE
EN POLYNÉSIE FRANÇAISE
Liberté
Égalité
Fraternité

Cabinet
du haut-commissaire
Direction des sécurités

N° HC / 1193 / CAB / DS / sg

Papeete, le 12 juillet 2024

Note
à
destinataires *in fine*

Objet : Procédure pour faire face à une cyber attaque
Réf. : Lettre n° 1053/ANSSI/DIR/NP du 12 juin 2024.
PJ : informations Cyber malveillance

La menace cyber, souvent sous-estimée, est devenue un enjeu majeur de sécurité, majoré conjoncturellement par l'organisation des Jeux Olympiques. Aucun territoire, entreprise ou administration n'est épargné et l'actualité récente sur le Fenua en est la démonstration.

Compte tenu des préjudices importants occasionnés par les cyberattaques, il est donc primordial de maîtriser son risque cyber, d'agir rapidement pour protéger efficacement les systèmes d'information et être résilient.

A l'approche de l'ouverture des JOP 2024, et en raison du caractère toujours plus prégnant de la menace qui pèse sur le Fenua, notamment sur les communes (collectivités régulièrement ciblées dans l'Hexagone), il m'apparait nécessaire de vous rappeler au travers des documents joints les conduites à tenir au quotidien et la procédure à mettre en œuvre en cas de constatation ou de suspicion de cyber-attaque :

1/ prendre contact immédiatement avec les forces de sécurité intérieure compétentes (DTPN ou gendarmerie) qui participeront à la levée le doute sur le caractère avéré ou non de l'attaque.

2 / si l'attaque est avérée, déclarer au plus tôt l'incident au CERT-FR - centre de réponse à incident de l'ANSSI (l'agence nationale de la sécurité des systèmes d'information a été qui a été désignée comme pilote unique de la SSI pour l'organisation

59 avenue Pouvana'a a Oopa – BP 115
98713 Papeete – Tahiti – Polynésie française
Tél. : +689 / 40.468.524 – Fax : +689 / 40.468.519
stephane.gavignet@polynesie-francaise.pref.gouv.fr

des JOP 2024)- activé 24/7 (par téléphone au + 33 9 70 83 32 18 et par mail à cert-fr@ssi.gouv.fr).

Par ailleurs, je vous informe que le site de l'ANSSI dispose de supports et de ressources pédagogiques pour initier vos agents et le grand public aux enjeux et aux bonnes pratiques de la cybersécurité. Ses conseils permettent à tout participant de devenir acteur de la sécurité du numérique dans son environnement personnel et professionnel.

En vous remerciant d'avance ...

Le Haut-Commissaire

Eric SPITZ

LISTE DE DIFFUSION

DESTINATAIRES :

Pour action :

- Mesdames et messieurs les maires des communes des Iles du Vent et des Iles sous le Vent ;
- Mesdames et messieurs les maires des communes des Tuamotu-Gambier ;
- Mesdames et messieurs les maires des communes des Australes ;
- Mesdames et messieurs les maires des communes des Marquises ;
- Madame la directrice générale du syndicat pour la promotion des communes de Polynésie française.

Pour info :

- Monsieur le président de la Polynésie française,
- Madame la Procureure de la République
- Monsieur le directeur territorial de la police nationale,
- Monsieur le colonel, commandant la gendarmerie pour la Polynésie française

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES 10 MESURES ESSENTIELLES POUR ASSURER VOTRE SÉCURITÉ NUMÉRIQUE

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés... Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques. Comment se protéger au mieux face à ces risques? **Voici 10 bonnes pratiques essentielles à adopter pour assurer votre sécurité numérique.**

1 PROTÉGEZ VOS ACCÈS AVEC DES MOTS DE PASSE SOLIDES

Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est souvent due à des mots de passe trop simples ou réutilisés. Au moindre doute, ou même régulièrement en prévention, changez-les. Utilisez un gestionnaire de mots de passe et activez la double authentification chaque fois que c'est possible pour renforcer votre sécurité.

2 SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT

En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données (photos, fichiers, contacts, messages...). Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes et conservez toujours une copie de vos sauvegardes sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

3 APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS APPAREILS (PC, TABLETTES, TÉLÉPHONES...), DÈS QU'ELLES VOUS SONT PROPOSÉES

Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner (mises à jour).

4 UTILISEZ UN ANTIVIRUS

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté.

5 TÉLÉCHARGEZ VOS APPLICATIONS UNIQUEMENT SUR LES SITES OFFICIELS

N'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple: Apple App Store, Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater vos équipements. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streamings illégaux) qui pourraient également installer un virus sur vos matériels.

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

6 MÉFIEZ-VOUS DES MESSAGES INATTENDUS

En cas de réception d'un message inattendu ou alarmiste par messagerie (*e-mail*), SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime. Il peut en effet s'agir d'une attaque par hameçonnage (*phishing*) visant à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires), de l'envoi d'un virus contenu dans une pièce jointe qu'on vous incite à ouvrir, ou d'un lien qui vous attirerait sur un site malveillant.

7 VÉRIFIEZ LES SITES SUR LESQUELS VOUS FAITES DES ACHATS

Si le commerce en ligne facilite les achats et offre l'opportunité de faire de bonnes affaires, il existe malheureusement de nombreux sites de vente douteux, voire malveillants. Avant d'acheter sur Internet, vérifiez que vous n'êtes pas sur une copie frauduleuse d'un site officiel, la crédibilité de l'offre et consultez les avis. Sans cette vérification, vous prenez le risque de vous faire dérober votre numéro de carte bancaire et de ne jamais recevoir votre commande, voire de recevoir une contrefaçon ou un produit dangereux.

8 MAÎTRISEZ VOS RÉSEAUX SOCIAUX

Les réseaux sociaux sont de formidables outils de communication et d'information collaboratifs. Ils contiennent toutefois souvent de nombreuses informations personnelles qui ne doivent pas tomber dans de mauvaises mains. Sécurisez l'accès à vos réseaux sociaux avec un mot de passe solide et unique, définissez les autorisations sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour vous nuire, ne relayez pas d'informations non vérifiées (*fake news*).

9 SÉPAREZ VOS USAGES PERSONNELS ET PROFESSIONNELS

Avec l'accroissement des usages numériques, la frontière entre utilisation personnelle et professionnelle est souvent ténue. Ces utilisations peuvent même parfois s'imbriquer. Matériels, messageries, « *clouds* »... Il est important de séparer vos usages afin que le piratage d'un accès personnel ne puisse pas nuire à votre entreprise, ou inversement, que la compromission de votre entreprise ne puisse pas avoir d'impact sur la sécurité de vos données personnelles (usages personnels et professionnels).

10 ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS

En mobilité, privilégiez la connexion de votre abonnement téléphonique (3G ou 4G) aux réseaux WiFi publics. Ces réseaux WiFi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles (mots de passe, numéro de carte bancaire...). Si vous n'avez d'autre choix que d'utiliser un WiFi public, veillez à ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 1.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

QUE FAIRE EN CAS DE CYBERATTAQUE ? (élus/dirigeants de collectivités)

1 PREMIERS RÉFLEXES

ÉLU **Alertez immédiatement votre support informatique si vous en disposez** afin qu'il prenne en compte l'incident (DSI, prestataire, personne en charge).

TECHNICIEN **Isolez les systèmes attaqués** afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local.

ÉLU **Constituez une équipe de gestion de crise** afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique...).

ÉLU **Tenez un registre des évènements et actions réalisées** pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.

TECHNICIEN **Préservez les preuves de l'attaque :** messages reçus, machines touchées, journaux de connexions...

2 PILOTER LA CRISE

TECHNICIEN **Identifiez l'origine de l'attaque et son étendue** afin de pouvoir corriger ce qui doit l'être et éviter un nouvel incident.

ÉLU **Déposez plainte** avant toute action de remédiation en fournissant toutes les preuves en votre possession.

ÉLU **Notifiez l'incident à la CNIL (*)** dans les 72h si des données personnelles ont pu être consultées, modifiées ou détruites par les cybercriminels.

TECHNICIEN **Mettez en place des solutions de secours** pour pouvoir continuer d'assurer les services indispensables. Activez vos plans de continuité et de reprise d'activité (PCA-PRA) si vous en disposez.

ÉLU **Gérez votre communication** afin d'informer avec le juste niveau de transparence vos administrés, agents, partenaires, fournisseurs, médias...

NE PAYEZ PAS LA RANÇON !

Car vous encourageriez les cybercriminels à chercher à vous attaquer à nouveau et financeriez leur activité criminelle tout en n'ayant aucune garantie qu'ils tiendront leur parole.

FAITES-VOUS ACCOMPAGNER

Par des prestataires spécialisés en cybersécurité que vous pourrez trouver sur www.cybermalveillance.gouv.fr

PRENEZ EN COMPTE LES RISQUES PSYCHOLOGIQUES

Une cyberattaque peut engendrer une surcharge exceptionnelle d'activité et un sentiment de sidération, d'humiliation, d'incompétence voire de culpabilité susceptible d'entacher l'efficacité de vos équipes durant la crise et même au-delà.

(*) Le règlement général sur la protection des données européen (RGPD) oblige depuis mai 2018 à désigner un délégué à la protection des données (DPO en anglais) en charge notamment de ces notifications.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

3 SORTIR DE LA CRISE

Faites une remise en service progressive et contrôlée après vous être assuré que le système attaqué a été corrigé de ses vulnérabilités et en en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque.

Tirez les enseignements de l'attaque et définissez les plans d'action et d'investissements techniques, organisationnels, contractuels, financiers, humains à réaliser pour pouvoir éviter ou a minima pouvoir mieux gérer la prochaine crise.

CONTACTS UTILES

Support informatique

Nom du contact : _____

N° de téléphone : _____

Conseils, signalement 24h/24

Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (ANSSI/CERT-FR) www.cert.ssi.gouv.fr/contact

Conseils et assistance

Dispositif national de prévention et d'assistance aux victimes de cybermalveillance
www.cybermalveillance.gouv.fr

Notification de violation de données personnelles

Commission nationale informatique et liberté (CNIL)
www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Police – gendarmerie : 17

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

POUR PLUS D'INFORMATIONS :
www.cybermalveillance.gouv.fr