MINISTÈRE
DE LA CULTURE
Liberté
Égalité
Fraternité

SG/SHFDS/FSSI

Fiche Vigilance cyber sécurité

Cette liste présente les bonnes pratiques en matière de cybersécurité recommandées par le Fonctionnaire de Sécurité des Systèmes d'Information du ministère de la Culture. Elle rappelle également les bons points de contacts en cas de compromission.

☞ Respect des règles de sécurité pour éviter une compromission :

- Maintenir à jour les logiciels et appliquer les patchs de sécurité des éditeurs sur les systèmes et les applications
- Limiter les droits des utilisateurs et des administrateurs au strict nécessaire
- Maîtriser les accès Internet
- Utiliser et maintenir à jour les logiciels antivirus
- Définir une politique de mots de passe : utiliser des mots de passe complexes, différents pour les usages personnels et professionnels. Utiliser une authentification multiple pour les accès professionnels.
- Cloisonner le système d'information pour éviter qu'un attaquant soit susceptible de prendre le contrôle d'un grand nombre de ressources et ainsi amplifier les conséquences de l'attaque
- Sauvegarder les données et disposer de copies déconnectées du réseau
- Sensibiliser le personnel avec rappel des consignes de bonnes pratiques sur la messagerie, ne pas ouvrir les courriels en cas de doute sur la légitimité ou l'origine.
- Suivre les alertes et les avis de sécurité émis par le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) : https://www.cert.ssi.gouv.fr.

☞ Conduite à tenir en cas de crise ou d'incidents cyber :

Sur le volet technique :

- Déconnecter immédiatement la ou les machines concernées du réseau et ne les éteignez pas.
- S'appuyer sur une société de sécurité informatique pour mener des actions de confinement/ investigation/ remédiation

Sur l'aspect gestion de l'incident :

- Consulter le site Cybermalveillance.gouv.fr afin d'être conseillé sur la résolution de l'incident et d'obtenir un diagnostic : https://www.cybermalveillance.gouv.fr

Sur l'aspect pilotage et gestion de la crise :

- Activer une cellule de crise cybersécurité, présidée par le responsable du service ou l'organisme.
- Mettre en œuvre les mesures prévues pour la continuité d'activité
- Anticiper sur une communication de crise.
- Déposer plainte auprès des services de police ou de gendarmerie, ou auprès du procureur de la République du tribunal judiciaire
- Notifier cette compromission à la CNIL s'il y a eu une violation de données à caractère personnel via le lien : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
- Ne jamais payer la rançon, le paiement ne garantit en rien le déchiffrement de vos données.

☞ Pour aller plus loin :

- Guide « Attaque par rançongiciel, tous concernés - comment anticiper et réagir en cas d'incident ? » : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf

- Guide hygiène et sécurité de l'ANSSI :https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

☞ Contacts :

Service	Adresse	Dans quel cas ?
CERT-FR ANSSI	cert@ssi.gouv.fr	Pour demander une assistance en cas d'incident de cybersécurité
CSIRT Culture	csirt@culture.gouv.fr	Pour informer le ministère de la Culture de l'incident