MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

LA LETTRE CYBER *en région Grand Est*

mars 2023

La thématique du mois
Que faire en cas de Cyberattaque

Qu'est-ce qu'une cyberattaque ?

Une cyberattaque est le fait de mettre en place un acte de malveillance envers des systèmes informatiques. L'attaque consiste à cibler différents dispositifs (ordinateurs ou serveurs), isolés ou en réseaux, reliés ou non à internet. Ce phénomène peut toucher les particuliers, les administrations et les entreprises.

Les premiers réflèxes !

- **Alertez immédiatement votre support informatique** si vous en disposez afin qu'il prenne en compte l'incident (service informatique, prestataire, personne en charge)
- **Isolez les systèmes attaqués** afin d'éviter une propagation sur d'autres équipements
- **Constituez une équipe de gestions** de crise afin de piloter les actions des différentes composantes concernées (Technique / R.H / Financière / Juridique….)
- **Tenez un registre d'évènements et des actions réalisées** pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident à postériori.
- **Préservez les preuves de l'attaque :** messages reçus, machines touchées, journaux de connexion, etc…

Le pilotage de la crise !

- **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.
- **Déclarez le sinistre auprès de votre assureur** qui peut vous dédommager voire vous apporter une assistance.
- **Alertez votre banque** au cas où des informations permettant des transferts de fond auraient été dérobées.
- **Déposez plainte** avant toute remédiation en fournissant les preuves récoltées.
- **Identifiez l'origine de l'attaque** et son étendue pour éviter un nouvel incident.
- **Notifiez à la CNIL** dans les 72H si des données personnelles ont été dérobées.
- **Gérez votre communication** afin d'informer au plus juste vos administrés, clients, collaborateurs, partenaires et fournisseurs.

La sortie de la crise !

Faites une remise en service progressive et contrôlée après vous être assurés que le système attaqué a été corrigé de ses vulnérabilités et 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 et humains à réaliser pour pouvoir éviter ou à minima pouvoir mieux gérer la prochaine crise.

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.

CONTACTS UTILES

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 (C.N.I.L)
Www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Police – Gendarmerie :
17

+ D'INFOS

internet-signalement.gouv.fr
Portail officiel de signalement des contenus illicites de l'Internet

FAITES-VOUS ACCOMPAGNER

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

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

Région de gendarmerie du Grand Est

LA LETTRE CYBER en région Grand Est

Directeur de la publication : GCA S. OTTAVI
Responsable éditorial : COL A. SCHWEITZER
Rédacteurs : COL A. SCHWEITZER – MDC M. KNOBLOCH
MAJ (ER) WOLFERT

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
arnaud.schweitzer@gendarmerie.interieur.gouv.fr
mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie :