maiage
Les hommes et les entreprises de la maintenance environnementale
HEBDO

CYBERATTAQUES : UN GUIDE DESTINÉ AUX DIRIGEANTS POUR BIEN RÉAGIR

Face aux cyberattaques, il est nécessaire d'agir rapidement et efficacement pour limiter l'impact sur le fonctionnement de votre organisation. La plateforme Cybermalveillance.gouv.fr vous guide avec les bons réflexes à connaître.

Les cyberattaques concernent toutes entreprises, associations et administrations. Elles doivent être gérées rapidement et avec méthode. La plateforme Cybermalveillance.gouv.fr propose un guide pour les dirigeants pour agir en cas de cyberattaque. Il présente une liste de points essentiels à suivre pour réagir, naviguer et sortir d'une crise cyberattaque.

Réagir rapidement et agir efficacement

Le guide rappelle les bons réflexes à adopter lors des crises :

- **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 que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local.
- **Constituez une équipe de gestion de crise** afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique…).
- **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.
- **Préservez les preuves** de l'attaque : messages reçus, machines touchées, journaux de connexions…
- **Mettre 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.

- **Identifiez l'origine de l'attaque et son étendue** afin de pouvoir corriger ce qui doit l'être et éviter un nouvel incident.
- **Gérez votre communication** pour informer avec le juste niveau de transparence vos administrés, clients, collaborateurs, partenaires, fournisseurs, médias…
- **Déclarez le sinistre auprès de votre assureur** qui peut vous dédommager, voire apporter une assistance.
- **Alertez votre banque** au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.
- **Déposez plainte** en fournissant toutes les preuves en votre possession.
- **Notifiez l'incident à la CNIL** dans les 72 h si des données personnelles ont pu être consultées, modifiées ou détruites.

Signaler l'incident et sortir de la crise

Une fois sorti de la crise, le guide rappelle également de prendre en compte les **risques psychosociaux**. Une cyberattaque peut engendrer une surcharge d'activité, un sentiment d'humiliation ou de culpabilité pouvant impacter l'efficacité des équipes durant et après la crise.

Contactez les organismes qui peuvent vous soutenir en situation de cybermalveillance :

- **Déclarez le sinistre auprès de votre assureur** qui peut vous dédommager, voire apporter une assistance.
- **Alertez votre banque** au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.
- **Déposez plainte** en fournissant toutes les preuves en votre possession.
- **Notifiez l'incident à la CNIL** dans les 72 h si des données personnelles ont pu être consultées, modifiées ou détruites.

Les contacts utiles à connaître en cas de cyberattaque :

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) : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Police – gendarmerie : 17

En savoir plus : Consulter le guide.

Source : Préventica - Juillet 2025