



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

## 1 PREMIERS RÉFLEXES



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

## 2 PILOTER LA CRISE



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



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



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



**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.



**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](http://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.

### 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 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](http://www.cert.ssi.gouv.fr/contact)

##### Conseils et assistance

Dispositif national de prévention et d'assistance  
aux victimes de cybermalveillance  
[www.cybermalveillance.gouv.fr](http://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](http://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles)

Police – gendarmerie : 17

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :



avi3ca



coTer  
numérique

DECLIC

**POUR PLUS D'INFORMATIONS :**  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

