



QUE FAIRE EN CAS DE CYBERATTAQUE ? (dirigeants)

Méthodologie synthétique de gestion des cyberattaques pour les dirigeants des entreprises, associations, collectivités, administrations.

1 PREMIERS RÉFLEXES



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 événements 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...

NE PAYEZ PAS DE 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.

2 PILOTER 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 en fonction de votre niveau de couverture assurantielle.



Alertez votre banque au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.



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



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



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



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

FAITES-VOUS ACCOMPAGNER

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

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.

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 (CNIL)
www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Police – gendarmerie : 17