QUE FAIRE EN CAS DE CYBERATTAQUE ?

NE PAS PANIQUER !

Ne payez pas la rançon !

Vous encourageriez les cybercriminels à recommencer tout en n'ayant aucune garantie qu'ils tiendront leur parole

PREMIERS RÉFLEXES

ÉLU

Déposez plainte en fournissant toutes les preuves en votre possession

Notifiez l'incident à la CNIL si des données personnelles ont été touchées

Gérez votre communication afin d'informer avec le juste niveau de transparence vos administrés, agents, partenaires, fournisseurs, etc. et ainsi tous les alerter quant à l'importance de la cybersécurité

ÉQUIPE TECHNIQUE

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

Mettez en place des solutions de secours pour assurer la continuité des services indispensables

PILOTER LA CRISE

ÉLU

Alertez immédiatement votre support informatique (responsable informatique, prestataire, personne en charge…)

Constituez une équipe de gestion de crise afin de piloter les actions de tous les services impactés et alertez votre délégué à la protection des données

Tenez un registre des événements pour aider les enquêteurs et tirer les enseignements de l'incident à posteriori

ÉQUIPE TECHNIQUE

Isolez les systèmes attaqués en coupant toutes les connexions à Internet et au réseau local

Préservez les preuves de l'attaque : messages reçus, machines touchées, journaux de connexions…

SORTIR DE LA CRISE

ÉLU

Tirez les enseignements de l'attaque et définissez les plans d'actions à réaliser pour pouvoir éviter ou à minima pouvoir mieux gérer la prochaine crise

Appuyez vous sur votre délégué à la protection des données qui saura vous orienter quant aux actions à mener pour vous protéger

ÉQUIPE TECHNIQUE

Faites une remise en service progressive et contrôlée après vous être assuré que tous les risques ont été écartés et que le système attaqué a été corrigé de ses vulnérabilités

CONTACTS

Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

www.cert.ssi.gouv/contact

Dispositif de prévention et d'assistance aux victimes de cybermalveillance

www.cybermalveillance.gouv.fr

Dispositif de notification obligatoire de violations de données personnelles (CNIL)

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

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.

N'hésitez pas à prendre contact avec votre psychologue du travail pour tout conseil

Contactez immédiatement les bonnes personnes !

- Votre support informatique
- Votre délégué à la protection des données
- La gendarmerie dont vous dépendez

N'hésitez pas à noter les numéros utiles sur format papier et à les afficher