

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 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 une propagation sur d'autres équipements
-  **Constituez une équipe de gestion 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 posteriori.
-  **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.

