

COMMUNIQUÉ DE PRESSE

Fort-de-France, le 2 juin 2023

Lutter contre les cyberattaques : recommandations à suivre pour se prémunir face à la menace

Ces derniers mois, plusieurs cyberattaques ont visé des collectivités locales et paralysé leur système informatique.

Ces attaques mettent en lumière les risques importants qui pèsent sur toute structure en matière de sécurité informatique et montrent à quel point nous devons tous amplifier collectivement nos efforts.

Face à ces risques, la préfecture de la Martinique s'est mobilisée pour sensibiliser les acteurs du territoire avec l'appui de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Plusieurs réunions d'informations et d'échanges ont eu lieu sur le sujet.

Aussi, il est important de rappeler les conduites à tenir pour se prémunir des attaques numériques mais également appréhender la gestion d'une crise d'origine cyber.

1. Renforcer la cybersécurité au sein des organisations, par la mise en place d'actions de :

- Sensibilisation et de formation auprès de vos collaborateurs sur les risques liés aux cyberattaques et sur les bonnes pratiques en matière de cybersécurité, notamment à travers le guide d'hygiène numérique.
- Sécurisation des systèmes informatiques en mettant en œuvre des solutions de sécurité tels que des pare-feux, des antivirus et des outils de détection des intrusions.
- Gestion des accès et des autorisations en limitant les accès aux données sensibles.
- Préparation en cas d'attaque en élaborant un plan de continuité des activités afin de faire face aux cyberattaques et aux incidents de sécurité.

2. En cas d'incident, adopter quelques réflexes simples permettant une meilleure gestion de la situation.

- Déconnectez immédiatement les équipements informatiques suspects du réseau, en retirant le câble réseau ou en éteignant les connexions sans fil (Wi-Fi ...), afin d'éviter la propagation de l'attaque ;
- Laissez les équipements suspects allumés et n'essayez pas de les modifier. Ceci permet en effet de préserver les éléments techniques nécessaires à la compréhension de l'incident puis éventuellement à l'enquête ;
- Ne connectez plus aucun appareil sur le réseau ;
- Contactez immédiatement votre service ou prestataire informatique pour qu'il puisse déclencher la mise en place d'un dispositif adéquat de gestion de l'incident.

Le dépôt de plainte est vivement recommandé. La gendarmerie nationale et la police nationale sont les interlocuteurs désignés pour le dépôt d'une plainte en matière de cybercriminalité. Si des données à caractère personnel sont impactées par l'attaque, une notification à la CNIL peut aussi être obligatoire.

L'anticipation et la préparation des entreprises et institutions face à ce type d'attaque est une nécessité absolue.

Pour en savoir davantage sur les menaces et les moyens de s'en protéger :

- Le site [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)
- Le Guide d'[hygiène informatique](#) de l'ANSSI
- Le Guide « [La cybersécurité pour les TPE/PME en treize questions](#) » de l'ANSSI
- Le Guide « [Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique](#) » de l'ANSSI
- Le Mooc [SecNumAcadémie](#) de l'ANSSI

Contact presse

Cabinet du préfet
Bureau de la communication interministérielle