PRÉFET
D'ILLE-
ET-VILAINE
Liberté
Égalité
Fraternité

Fiche réflexe
à l'attention des collectivités locales
Que faire en cas de cyberattaque ?

En cas de cyberattaque ou de soupçon de cyberattaque face à un comportement anormal d'un ordinateur, le maire ou tout personnel de la mairie, doit :

➔ **Actions réflexes :**

- ☐ 1. Déconnecter les ordinateurs d'internet et du réseau informatique, en débranchant le câble réseau et/ou en désactivant la connexion Wifi ou 4/5G. L'objectif est d'éviter que l'attaque ne puisse se propager à d'autres équipements ou que des données soient exportées
- ☐ 2. Ne pas éteindre les équipements compromis pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir, certains éléments de preuve disparaissant lorsque l'on éteint l'appareil

➔ **Alerte précoce :**

- ☐ 3. Alerter au plus vite le référent informatique de la collectivité qui prendra les mesures nécessaires pour contenir les conséquences de la cyberattaque (ex : déconnexion des sauvegardes automatisées)
- ☐ 4. Alerter Breizh cyber → 0.800.200.008 et/ou → https://breizhcyber.bzh
  C'est le centre de réponse à incident du conseil régional de Bretagne. Il fournit une première aide d'urgence gratuite aux entreprises (PME et ETI), collectivités et associations du territoire, en cas de cyberattaque. Breizh cyber vous mettra en relation avec les prestataires cyber spécialisés
- ☐ 5. Prévenir les agents et élus de la collectivité. Une mauvaise manipulation de la part d'un collaborateur pourrait aggraver la situation
- ☐ 6. Prévenir l'astreinte sécurité de la préfecture : 06.77.21.94.54

➔ **Mesures de gestion de crise :**

- ☐ 7. Déclencher le plan communal de sauvegarde et constitution d'une équipe de gestion de crise afin de piloter les actions nécessaires (technique, RH, financière, communication, juridique…)
- ☐ 8. Informer avec le juste niveau de transparence vos administrés, agents, partenaires, fournisseurs, média, etc. Un plan de communication peut rassurer vos usagers
- ☐ 9. Ne pas payer la rançon - Ne jamais prendre contact avec l'attaquant
- ☐ 10. Tenir à disposition un maximum de preuves (fichiers, photos des écrans, vidéos, clés USB, disques durs, etc.)

➔ **Dépôt de plainte et judiciarisation :**

☐ 11. Déposer plainte auprès de la Police nationale ou de la Gendarmerie nationale sous 72 heures maximum, à compter du moment où vous avez eu connaissance de l'incident. Cette étape est obligatoire pour permettre une indemnisation au titre d'un contrat d'assurance cyber[1]

☐ 12. Déclaration en ligne obligatoire auprès de la CNIL dans les 72 heures en cas de violation présentant un risque pour les droits et libertés des personnes tel que la fuite de données personnelles (art.33 RGPD). Le signalement peut être complété par la suite. N'oubliez pas d'aviser également votre délégué à la protection des données (DPO).
Lien : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Contacts :

- Breizh cyber : 0.800.200.008 (lundi au jeudi de 9 h à 17h30 et le vendredi de 9 h à 17 h)
- CERT-FR (ANSSI) : 01.71.75.84.68 (permanence 7j/7, 24h/24). Cette structure nationale a vocation à traiter les attaques subies par les administrations de l'État et les structures privées les plus sensibles mais peut apporter des conseils aux collectivités en dehors des horaires d'ouverture de Breizh Cyber
- Astreinte SIDPC: 06.77.21.94.54

POUR ALLER PLUS LOIN

Sites de référence :

- https://breizhcyber.bzh
- www.cybermalveillance.gouv.fr
- https://cyber.gouv.fr/

Autres fiches réflexes :

- https://www.cybermalveillance.gouv.fr/medias/2020/10/AfficheA3_premiers-gestes-en-cas-cyberattaque.pdf
- https://www.senat.fr/rap/r21-283/r21-2832.png

1 *Art. L.12-10-1 code des assurances.*