RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

SCRUTINS 2022

COMMUNES, ASSUREZ VOTRE SÉCURITÉ NUMÉRIQUE !

UN RANÇONGICIEL PEUT METTRE EN PÉRIL L'ORGANISATION DES SCRUTINS PAR LES COMMUNES

Une cyberattaque à l'encontre d'une mairie en contexte électoral peut contribuer à désorganiser la tenue des scrutins. Les attaques par rançongiciel sont parmi les plus susceptibles d'avoir des conséquences néfastes sur les scrutins. Elles provoquent en effet le chiffrement des données et donc leur indisponibilité - les attaquants réclamant ensuite une rançon à la victime.

Les éléments suivants pourraient ainsi être inaccessibles :

- **En amont du vote** : les listes électorales et les procurations, entraînant ainsi des difficultés majeures dans la préparation des valises électorales destinées aux bureaux de vote.
- **Pendant et à l'issue du vote** : la transmission par Internet des résultats du décompte des bulletins de vote.

LES BONNES PRATIQUES À ADOPTER

Les mairies sont aujourd'hui régulièrement la cible d'attaques par rançongiciels. Afin d'assurer la bonne tenue des scrutins au sein des communes, l'ANSSI recommande d'appliquer au minimum les recommandations suivantes :

- **Sauvegarder régulièrement** les données indispensables à l'organisation du scrutin sur **des supports hors ligne** (disques durs externes, clés USB, etc.) dont l'innocuité est garantie.
- Être attentif avant d'ouvrir les pièces jointes contenues dans les courriels et ne pas cliquer sur les liens Internet qui semblent douteux.
- Protéger les accès à ses ordinateurs, aux sites Internet et aux applications par des **mots de passe complexes, uniques et secrets**.
- Mettre régulièrement à jour ses principaux logiciels (notamment anti-virus) et ses équipements informatiques.
- Privilégier l'utilisation d'un compte pourvu des seuls droits d'utilisateur (droits et accès limités sur le système d'information).

RÉAGIR EN CAS DE CYBERATTAQUE

Être victime d'un rançongiciel peut désarçonner toute organisation. Quelques gestes simples permettent d'en limiter grandement les impacts :

- Déconnectez immédiatement du réseau (câble ou Wi-Fi) les équipements piratés afin d'éviter la propagation de l'attaque et de préserver les preuves nécessaires à l'enquête.
- Ne connectez plus aucun appareil sur le réseau.
- Contactez immédiatement votre service ou votre prestataire informatique.
- Notifiez les autorités et portez plainte auprès des services compétents (Police ou Gendarmerie).
- Constituez une équipe pour gérer les conséquences de la cyberattaque et préparer une stratégie de communication.
- Déclarez l'incident à la CNIL.

Rappel : le paiement de la rançon ne garantit ni la récupération des données ni leur intégrité et finance les réseaux cybercriminels.

POUR ALLER PLUS LOIN

- **Pour se préparer et réagir aux attaques par rançongiciels :**
  - Fiche réflexe cybermalveillance.gouv.fr : *Les rançongiciels*
  - Fiche réflexe cybermalveillance.gouv.fr : *Que faire en cas de cyberattaque*
  - Guide de l'ANSSI : *Attaques par rançongiciels : tous concernés*
- **Pour sensibiliser ses équipes :**
  - Guide 2020 de l'AMF, avec le soutien de l'ANSSI : *Cybersécurité : toutes les communes et intercommunalités sont concernées*
  - Programme de cybermalveillance.gouv.fr : *Sensibilisation aux risques numériques dans les collectivités territoriales*

En cas d'incident de sécurité informatique :

ANSSI - www.ssi.gouv.fr/en-cas-dincident

Cybermalveillance.gouv.fr - www.cybermalveillance.gouv.fr/diagnostic/favoris/collectivite

COMMUNES, ASSUREZ VOTRE SÉCURITÉ NUMÉRIQUE !

Un rançongiciel peut mettre en péril l'organisation des scrutins.

En cette période électorale, faites preuve de vigilance et pensez à appliquer les bonnes pratiques recommandées par l'ANSSI et Cybermalveillance.gouv.fr.

Avec le soutien de :

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Version 1.0 – Décembre 2021

Dépôt légal : décembre 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr