COMMENT SE PRÉMUNIR D'UNE CYBERATTAQUE

« image : Freepik.com »

Mettre en places des mesures de sécurité préventives

Les menaces cybercriminelles pèsent de plus en plus sur les collectivités territoriales, établissements publics locaux et hospitaliers avec des effets collatéraux sur le comptable de la DGFiP.
En effet, au titre de la continuité de service, le comptable va devoir assurer de nombreuses dépenses et recettes sans émission préalable de pièces comptables. Autant d'actes réalisés dans des conditions dégradées de visa, avec nécessité de régularisations a posteriori avec tous les risques de doubles paiements.
Aussi, il apparaît nécessaire que la DGFiP sensibilise les ordonnateurs sur les impacts possibles d'une attaque, afin d'anticiper les mesures à prendre en cas d'attaque et s'y préparer au mieux.

CYBER ATTAQUE

CONSEILS CLASSIQUES

RÉALISER UN AUDIT

SENSIBILISER ET PRÉVOIR

> QUELQUES CONSEILS CLASSIQUES

Utiliser des **mots de passe** suffisamment **complexes** et les **changer régulièrement**

Appliquer de manière régulière et systématique les **mises à jour de sécurité du système et des applications/programmes** installés sur les postes informatiques

Tenir à jour l'antivirus et configurer le pare-feu

Faire des **sauvegardes régulières des données** pour pouvoir les réinstaller dans leur état d'origine au besoin et stocker ces sauvegardes **sur un équipement totalement déconnecté du réseau informatique**

Désinstaller les applications ou programmes dont l'éditeur n'assure plus de support (absence de mise à jour de sécurité)

N'utiliser un poste de travail en session "administrateur" que très ponctuellement et uniquement pour des opérations d'administration du poste

Ne pas ouvrir les courriels provenant d'expéditeurs inconnus ou d'un expéditeur connu mais dont la structure, la syntaxe, l'orthographe et/ou la teneur du message sont inhabituelles ou vides. Ne pas ouvrir les pièces jointes et ne pas cliquer sur les liens provenant de ces messages

Ne pas faire de **mailing avec l'ensemble des adresses mails des destinataires visibles**. Utiliser la fonction copie cachée.

Ne pas installer d'applications ou de programmes « piratés », dont l'origine ou la réputation sont douteuses

Éviter les sites non sûrs ou illicites

Il convient que l'ordonnateur s'assure de la tenue du bon niveau de sécurité de son système d'information. En cas de difficultés, l'ordonnateur pourra faire appel à son éditeur, un syndicat de mutualisation informatique ou autre prestataire. **Avoir recours à une suite logiciel en mode SaaS permet de bénéficier de l'expertise de son fournisseur / hébergeur.**

> RÉALISER UN AUDIT

Un audit réalisé par une entreprise spécialisée permet d'établir une image claire du niveau d'exposition du SI, des possibles fragilités et des moyens à mettre en œuvre (en temps et en moyens financiers) pour parvenir à être à l'état de l'art.

En fonction de la criticité du constat de l'audit, et en raison des délais administratifs il ne faut pas attendre pour lancer des consultations puis notifications de marchés de mise en sécurité du SI.

L'anticipation permet de construire un plan de remise à niveau du système d'information et de l'échelonner budgétairement. L'absence d'investissement entraînera en cas d'attaque une obligation d'investissement similaire mais concentrée sur quelques mois, sans compter les pertes strictement liées à l'attaque et la remise à niveau du système.(prestations externes et investissement supérieur du personnel interne).

L'audit ne constitue qu'une partie de la démarche de sécurité à laquelle sont soumises les collectivités. En effet **ces dernières sont tenues de respecter le RGS** (https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs) qui concerne tous les organismes proposant des services numériques au public ou échangeant avec un autre organisme public.

Chaque applicatif ou site qui rentre dans une de ces catégories doit ainsi être homologué (https://cyber.gouv.fr/lhomologation-de-securite).

Des guides sont présents sur les sites ci-dessus et l'ANSSI référence également des entreprises agrées à l'accompagnement dans cette démarche (https://cyber.gouv.fr/produits-services-qualifies).

La Gendarmerie nationale peut évaluer l'exposition des collectivités aux cyberattaques avec le pré-diagnostic cyber. Ce dispositif est accessible sur l'ensemble du territoire.
Le dispositif Diagonal (acronyme de DIAGnostique Opérationel NationaL Cyber) permet de réaliser dans les locaux de la collectivité avec l'aide d'un cyber gendarme un pré-diagnostic cyber en vue d'évaluer l'exposition aux menaces en ligne et d'identifier les actions à conduire pour sécuriser la collectivité face à la multiplication des cyberattaques.
Pour plus d'information, consulter le site FranceNum.gouv.fr

> SENSIBILISER ET PRÉVOIR

Il est difficile d'être complètement à l'abri d'une attaque.
Aussi, il est nécessaire d'envisager un tel évènement et d'en anticiper les impacts L'objet est d'être mieux armé pour répondre à une cyberattaque

Il est recommandé d'établir un plan de crise pour répondre urgemment à une attaque et un plan de continuité d'activité pour poursuivre les actions de la collectivité ou établissement en mode dégradé.

[Anticiper la création d'une cellule de crise

- Définir quels sont les acteurs à activer dès le constat de l'attaque, recenser les noms et numéros d'appel côté ordonnateur et poste comptable. Le comptable doit être immédiatement prévenu.
- Prévoir les contacts externes à activer :
  - coordonnées de l'ANSSI(1) et des relais régionaux.
  - coordonnées de l'Expert Analyse Forensique (2) auquel la structure ferait appel en cas de besoin.
- Définir quels seraient les « moyens » en gestion de crise pour les échanges mail & visio, déconnectés du SI régulier.
- Définir le fournisseur d'accès, respectueux de la souveraineté numérique. Un fournisseur gratuit peut être choisit, Proton Mail, Mailo, La Poste …
- La collectivité peut aussi recourir à l'achat d'un nom de domaine de secours et créer des boites mails.
- Il est préconisé de s'accorder sur la structure des adresses mails autorisées qui échangeront avec le comptable pour que ce dernier soit assuré de la légitimité de ses interlocuteurs : Exemple de structure nom.prenom_commune@yahoo.fr
- En cas de contamination des ordinateurs, quelles sont les solutions de secours ?
- Comment monter un réseau de secours isolé ?

DÉFINITION

(1) Contacts ANSSI : https://cyber.gouv.fr/en-cas-dincident
(2) Un expert forensique est une personne qualifiée pour conduire une analyse et une recherche méthodique et approfondie des actions réalisées sur un système informatique après incident (piratage, vol de données, etc.).

[Dresser les processus Métier et définir une Analyse des risques :

Il est recommandé pour chaque direction au sein de la collectivité ou établissement de mener les réflexions sur leur processus de travail sans informatique en dressant un tableau en 3 temps :

- **Fonction métier :**
  - Détail de la fonction métier :
    - qu'est qui ne fonctionne plus ?
    - détail de la fonctionnalité métier impactée
- **Applications concernées :**
  - Liste des applications ou outils informatiques indispensables pour réaliser ces traitements
- **Conséquences en cas d'indisponibilités des outils informatiques :**
  - Définir les conséquences à plusieurs temps après l'attaque
    - Conséquences Immédiates : depuis le début de l'attaque
    - Conséquences à 8 jours après le début de l'attaque
    - Conséquences à 1 mois après le début de l'attaque

Cet exercice permet d'évaluer les risques en cas d'attaque, de définir en regard de chacun les possibles moyens correctifs. Dans de nombreux cas, les fonctions métiers impactent la chaîne comptable et financière. Le comptable public pourra être associé et aussi éclairer l'ordonnateur pour exposer les blocages coté DGFiP si les échanges informatiques ordonnateur-comptable devaient être rompus.

[S'entraîner pour mieux se protéger :

Certaines situations, telle que la gestion d'une crise, font sortir l'organisation de ses processus de fonctionnement nominaux. Il convient donc, en complément de la formation, de développer les bons réflexes collectifs en cas de cyberattaque. Pour aborder sereinement la crise, il faut mettre régulièrement en situation au travers d'exercices l'ensemble des acteurs interne et externes à l'organisation. L'ANSSI met à disposition un kit d'exercice pour les collectivités territoriales :
https://cyber.gouv.fr/le-kit-dexercice-pour-les-collectivites-territoriales

DOCUMENTATION

- La sécurité numérique des collectivités territoriales : l'essentiel de la réglementation https://cyber.gouv.fr/publications/securite-numerique-des-collectivites-territoriales-lessentiel-de-la-reglementation
- Site gouvernemental https://www.cybermalveillance.gouv.fr/
- Le RGS s'applique aux collectivités https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs
- Homologation de sécurité : https://cyber.gouv.fr/lhomologation-de-securite
- Site internet d'auto diagnostic de cyber sécurité (Service du Haut Fonctionnaire de Défense et de Sécurité des ministères économiques et financiers) : https://ssi.economie.gouv.fr