PRÉFET
DES BOUCHES-
DU-RHÔNE
Liberté
Égalité
Fraternité

Fiche thématique « Cyberattaques »

1. ÉTAT DES LIEUX

Désireuses de bénéficier des nombreux atouts que proposent les outils numériques et les services en ligne, **les communes et intercommunalités s'appuient de plus en plus sur l'informatique pour mener leurs missions quotidiennes**. Par ailleurs, il est courant que les **données** traitées par ces dernières soient hébergées sur des serveurs informatiques internes ou chez des prestataires (dont des hébergeurs *Cloud* - Informatique en nuage en français).

Or, des groupes ou personnes malintentionnés profitent de cette dépendance croissante au numérique pour s'infiltrer sur ces systèmes informatiques et **mener des actions malveillantes**.

Leurs motivations sont diverses :

- **Gagner de l'argent**, au travers de cyberattaques qui bloquent les systèmes d'information et/ou exfiltrent des données pour ensuite demander une rançon à la victime, voire revendre l'information volée sur le *darkweb*. Les outils numériques peuvent également devenir le canal privilégié de certaines escroqueries (ex : usurpation d'identité, faux ordre de virement). Ces actions sont principalement portées par des groupes cybercriminels.
- **Espionner**, dans le but de récupérer des informations stratégiques ou d'un intérêt particulier pour l'attaquant (ou ses « clients »). Cette action peut être menée par des groupes cybercriminels ou des groupes d'attaquants sponsorisés par des États. À une échelle plus locale, l'espionnage informatique peut servir des intérêts individuels en soustrayant des informations politiques, administratives, financières ou personnelles pour en tirer un bénéfice personnel ou nuire à un adversaire.
- **Déstabiliser,** en rendant inopérantes certains activités-clés d'une entité, voire d'un pays. Cette action peut être menée par des groupes cybercriminels ou des groupes d'attaquants sponsorisés par des États.
- **Revendiquer** une cause politique ou sociétale, en prenant le contrôle de sites web, panneaux d'affichage, etc. pour faire passer des messages (ou les rendre indisponibles – cas du « déni de service »). Cette action est principalement menée par des groupes d'activistes.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), autorité nationale en matière de cybersécurité et cyberdéfense, constate aujourd'hui que le **nombre de cyberattaques demeure élevé**, touchant sans distinction les entreprises de toute taille et tout secteur, les collectivités territoriales et les établissements de santé.

Cette tendance s'explique de plusieurs façons :

- **Les usages numériques non maîtrisés et les faiblesses dans la sécurisation des données** continuent d'offrir de trop nombreuses opportunités aux attaquants. Si cela est vrai pour les services hébergés et administrés en interne, le recours au *Cloud* (informatique en nuage en français) et l'externalisation de services auprès d'entreprises de services numériques, lorsqu'ils ne s'accompagnent pas de clauses de cybersécurité adaptées, représentent aussi une vulnérabilité importante. Les attaquants peuvent également rebondir s'ils existent des connexions entre différents systèmes (ex : celui d'un prestataire et d'un client).

- **Par manque de sensibilisation, les utilisateurs se font piéger par du « phishing »** (hameçonnage en français), mode opératoire très souvent utilisé par les cyberattaquants pour récupérer des données personnelles ou de connexion par la tromperie (faux courriels, faux sites web), leur permettant notamment d'accéder par la suite à des systèmes d'information en exploitant les mots de passe ainsi obtenus.

- **L'amélioration des capacités des cyberattaquants** (outils, processus) leur permet de mener plus facilement des attaques ciblées ou massifiées. Concernant **les attaques massifiées, elles répondent à des logiques de rentabilité** du côté des cybercriminels : un grand nombre d'entités sont visées, puis l'attaque sera menée là où il existe des failles de sécurité facilement exploitables, par manque d'hygiène informatique (logique de la « pêche au chalut »).

En particulier, il est important de noter qu'**il n'est pas nécessaire d'être une cible pour devenir une victime** : lorsqu'un acteur malveillant envoie un million de courriels malveillants ou rebondit à partir d'un carnet d'adresses déjà piraté, les agents d'une collectivité territoriale peuvent être touchés sans ciblage initial délibéré de la part de l'attaquant.

2. MESURES PREVENTIVES

Face à ces menaces, les communes et intercommunalités doivent donc prendre en compte le risque cyber au juste niveau et adopter les bonnes mesures pour se protéger.

L'objectif est d'atteindre un niveau d'hygiène informatique minimisant la probabilité et l'impact d'attaques « opportunistes », afin de rendre le risque résiduel (celui qui subsiste après l'application des mesures retenues) acceptable. Pour cela, il est notamment important de :

- **Identifier les activités et données clés de la commune, et leurs enjeux de sécurité**
  L'identification (liste, cartographie) des activités et données critiques de la commune et la manière dont elles sont opérées (systèmes internes, externes), puis leur priorisation en matière de confidentialité et disponibilité, sont essentielles pour pouvoir mener des actions de sécurisation des systèmes jugés les plus critiques (briques de sécurité, architecture sécurisée). Elles permettent aussi de savoir quels systèmes relancer en priorité en cas d'incident.

- **Sauvegarder les données les plus importantes et vérifier la capacité à les restaurer**
  Des sauvegardes régulières des données les plus indispensables ou utiles, notamment celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques, doivent être réalisées. Il s'agit de garder à l'esprit que ces sauvegardes peuvent aussi être affectées par une attaque par rançongiciel si elles ne sont pas protégées de manière spécifique.
  À titre d'illustration, la règle *de sauvegarde 3-2-1* est une méthode recommandée (par exemple par l'ANSSI dans son guide dédié à la sauvegarde des systèmes d'information). Elle consiste à avoir 3 copies des données (l'original et 2 copies de sauvegardes), sur 2 supports de stockages différents (par exemple 1 copie sur disque dur externe et 1 copie sur système de bande) dont 1 copie hors site et hors connexion (pour éviter que

l'attaquant ne détruise ce jeu de données). Enfin, la capacité à restaurer à partir de ces sauvegardes doit être régulièrement testée pour éviter tout blocage inattendu le jour où il est critique de récupérer ces données.

- **Maintenir à jour ses logiciels et systèmes**
  Les vulnérabilités non corrigées des systèmes d'exploitation ou des logiciels présents sur le système d'information peuvent être utilisées pour infecter le système ou favoriser la propagation de l'infection. L'expérience montre que très souvent les failles exploitées par les attaquants donnaient déjà lieu à des correctifs publiés par les éditeurs, correctifs qu'il aurait suffi d'installer pour se protéger au bon niveau.

- **Sensibiliser les agents**
  Le plus souvent, l'attaque par rançongiciel commence par l'ouverture d'une pièce jointe piégée ou la consultation d'une page web malveillante, voire la saisie d'identifiants en pensant accéder à un portail légitime. Ainsi la formation des utilisateurs aux bonnes pratiques de sécurité numérique est une étape fondamentale pour lutter contre cette menace, même si elle ne constitue pas un rempart absolu.

➔ ***D'autres mesures peuvent également être mises en place en s'appuyant sur le diagnostic*** www.monaidecyber.ssi.gouv.fr

3. GERER UNE CRISE D'ORIGINE CYBER

Malgré les efforts de sécurisation déjà mené, le risque qu'une cyberattaque impacte le fonctionnement d'une commune ou intercommunalité existe. Il ne peut être totalement exclu. Dès lors, il s'avère nécessaire d'assurer un certain niveau de résilience, en établissant un plan de réponse aux cyberattaques associé au dispositif de gestion de crise, dans le but d'assurer la continuité des activités puis un retour à un état nominal.

• SPECIFICITES DE LA CRISE CYBER

Une crise « d'origine cyber » se définit par **la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation** (arrêt des activités, impossibilité de délivrer des services, impact sur l'image et la confiance, etc.) **en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques** (cyberattaques de type rançongiciel, déni de service, etc.).

C'est donc un événement à fort impact, qui ne saurait être traité par les processus habituels et dans le cadre du fonctionnement normal d'une commune.

En comparaison à d'autres scénarios de crise, les crises cyber ont **des caractéristiques propres** qu'il est important d'appréhender :

- L'existence d'une double temporalité des impacts, avec un arrêt immédiat de certaines activités et une remédiation pouvant s'étendre sur plusieurs semaines voire plusieurs mois.
- Une potentielle propagation de l'attaque à d'autres systèmes ou organisations, en raison de l'interconnexion des systèmes d'information.
- Une menace (l'attaquant) s'adaptant aux mesures d'endiguement et de remédiation.
- Une incertitude concernant le périmètre de la compromission et les raisons de l'attaque.

• PREREQUIS

La gestion d'une crise cyber nécessite donc d'être anticipée**, en apportant un focus particulier sur les actions de préparation suivantes** :

- La mise en place de **processus d'alerte** et de mobilisation du dispositif de crise.
- La **connaissance et la maîtrise des systèmes d'information** et applications métiers.
- L'identification des **activités et données essentielles** et les moyens de les faire fonctionner en mode dégradé.
- L'identification de **réseaux de soutien** (prestataires, CSIRT régional, services de l'État) et de premières actions de confinement de la menace puis de remédiation.
- La mise en place **d'outils résilients**, permettant *a minima* le pilotage et la communication (outils de communication annexes, systèmes de repli, etc.).
- La préparation d'une **stratégie de communication**.

L'objectif est de gagner en fluidité et d'adopter des automatismes, qui permettront de réagir efficacement dans l'immédiat comme sur le temps long, et de redonner confiance aux équipes et à l'écosystème concernés directement ou indirectement par les conséquences de l'incident.

• GOUVERNANCE

La particularité du scénario de crise cyber **implique de mobiliser à la fois des profils métiers, cyber et informatiques.** Il convient donc de planifier une organisation de crise en amont de tout événement et de s'accorder sur le rôle de chaque partie, afin de faciliter la mobilisation.

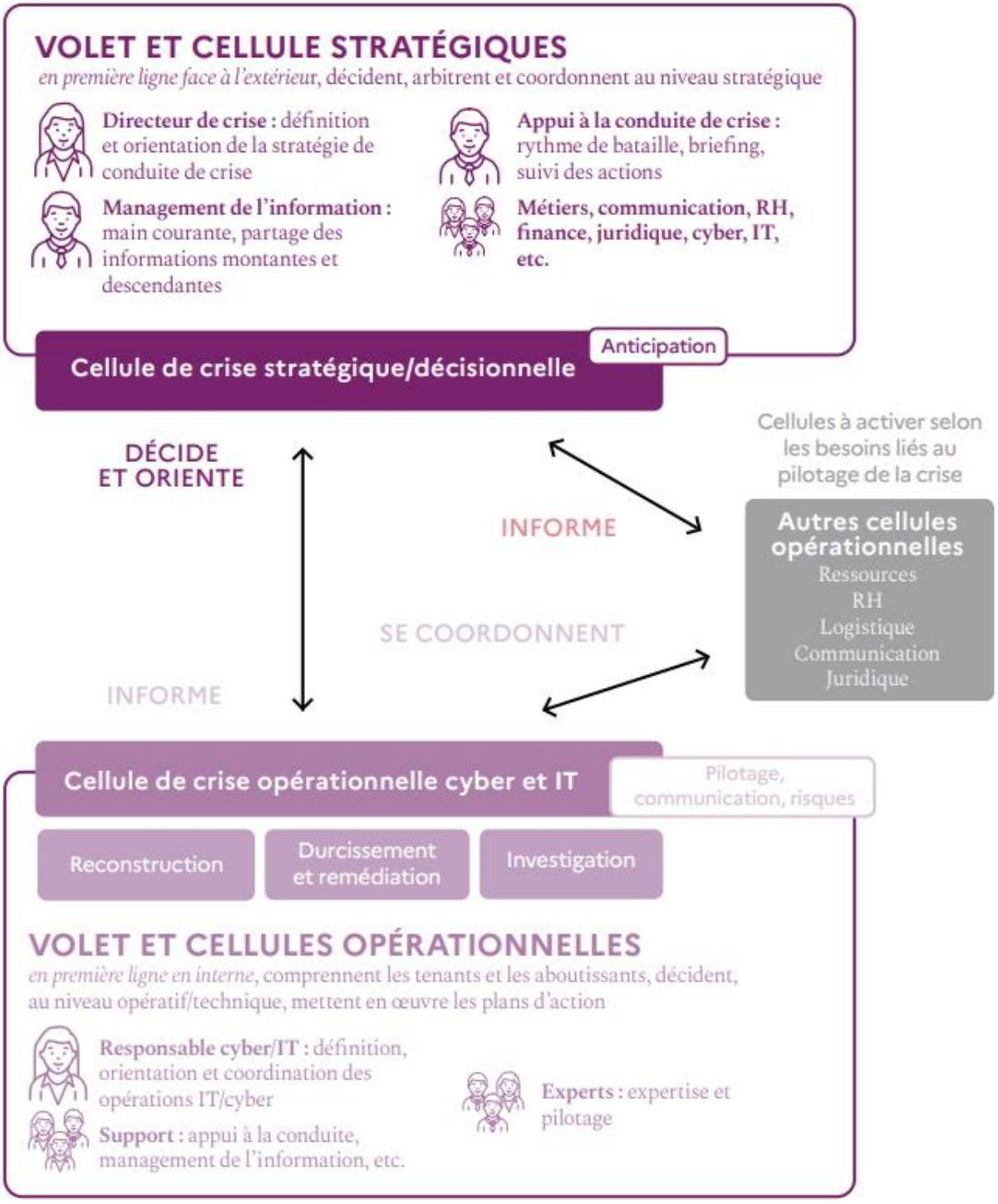
Le volet « stratégique » (ou « décisionnel ») est logiquement activé, sous la direction du maire ou du directeur général des services, avec pour **mission d'orienter et d'arbitrer la gestion de la crise.**

En parallèle, la mobilisation du **volet « opérationnel » informatique**, sous l'autorité de la direction des systèmes d'information (DSI ou RSSI) doit permettre de **piloter les actions techniques** (en particulier l'investigation, la remédiation et la reconstruction des systèmes d'information et les relations avec les prestataires) et d'exposer au volet « stratégique » **les particularités de la crise cyber** (ex : temps d'investigation long, priorisation dans la reconstruction des systèmes).

D'autres activités « opérationnelles » sont également à mener en parallèle et en cohérence, par exemple en lien avec les ressources humaines, la logistique et surtout la communication.

La coordination entre tous ces volets est bien évidemment primordiale pour permettre une compréhension mutuelle des enjeux de la crise et une conduite efficace.

Un modèle d'organisation du dispositif **est proposé ci-dessous :**



Source : Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique, ANSSI

4. RESSOURCES COMPLEMENTAIRES

- La cybersécurité pour les TPE/PME en treize questions – ANSSI : https://cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions
- Attaques par rançongiciel, comment les anticiper et réagir en cas d'incident – ANSSI : https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes
- Fiche réflexe Rançongiciel – Cybermalveillance : https://www.cybermalveillance.gouv.fr/medias/2019/11/230417_FicheReflexe_Rancongiciels.pdf
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique – ANSSI : https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique
- Anticiper et gérer sa communication de crise cyber – ANSSI : https://cyber.gouv.fr/publications/anticiper-et-gerer-sa-communication-de-crise-cyber

  Fiche sur « les mises à jour » – Cybermalveillance : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

  Fiche sur « les sauvegardes » – Cybermalveillance : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes
- Fiche sur « les rançongiciels » – Cybermalveillance : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares
- Guide « Cybersécurité : toutes les communes et intercommunalités sont concernées » – AMF / ANSSI : https://cyber.gouv.fr/publications/cybersecurite-toutes-les-communes-et-intercommunalites-sont-concernees