Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL D'AVANCEMENT DE GRADE DE RÉDACTEUR TERRITORIAL PRINCIPAL DE 1ère CLASSE

SESSION 2024

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS OPÉRATIONNELLES

ÉPREUVE D'ADMISSIBILITÉ :
Rédaction d'un rapport à partir des éléments d'un dossier portant sur les missions, compétences et moyens d'action des collectivités territoriales, assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 26 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir un surveillant.

Vous êtes rédacteur principal territorial de 1ère classe au sein de la commune d'Admiville qui compte 10 000 habitants et dont la directrice générale des services (DGS) est déléguée à la protection des données.

Suite aux différentes cyberattaques d'organismes publics particulièrement médiatisées, la DGS vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport sur les enjeux de la cybersécurité pour les collectivités territoriales.

10 points

Dans un deuxième temps, elle vous demande d'établir un ensemble de propositions opérationnelles permettant à la collectivité de s'engager dans une démarche de prévention des risques de cyberattaques.

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances.

10 points

Liste des documents :

Document 1 : « Guide. Obligations et responsabilités des collectivités locales en matière de cybersécurité » (extrait) - *CNIL* et *Cybermalveillance.gouv.fr* - 4 juillet 2022 - 3 pages

Document 2 : « Les petites communes mieux informées sur les cybermenaces » - *Localtis - banquedesterritoires.fr* - 8 mars 2022 - 2 pages

Document 3 : « Les collectivités territoriales face à la cybercriminalité - Fiche n°16 : Le Plan Reprise d'Activité (PRA) / Le Plan Continuité d'Activité (PCA) » - *Association nationale des directeurs et directeurs-adjoints des centres de gestion de la fonction publique territoriale* en partenariat avec *Gras Savoye* - 2016 - 3 pages

Document 4 : « Que faire en cas de cyberattaque ? (dirigeants) » (extrait) - *Cybermalveillance.gouv.fr* - 25 janvier 2022 - 1 page

Document 5 : « L'essentiel sur la cybersécurité : entreprises, collectivités territoriales : toutes concernées ! » (extraits) - *Senat.fr* - Novembre 2021 - 3 pages

Document 6 : « Cybersécurité : quelles sont les obligations et responsabilités des collectivités locales ? » - *Maire-info* - 6 juillet 2022 - 2 pages

Document 7 : « Cybersécurité : "Il reste beaucoup à faire dans les collectivités locales" » - *le Courrier des Maires* - 4 janvier 2023 - 2 pages

Document 8 : « Cybersécurité : toutes les communes et intercommunalités sont concernées » (extrait) - *Association des Maires de France et des présidents d'intercommunalité* - Novembre 2020 - 5 pages

Document 9 : « Comment Angers a fait face à sa première cyber-attaque ? » - *revue L'infocyber-risques* - 4ème trimestre 2021 - 3 pages

Dans un souci environnemental, les impressions en noir et blanc sont privilégiées. Les détails non perceptibles du fait de ce choix reprographique ne sont pas nécessaires à la compréhension du sujet, et n'empêchent pas son traitement.

DOCUMENT 1

Guide. Obligations et responsabilités des collectivités locales en matière de cybersécurité (extrait)

(...) # 1. OBLIGATIONS DES COLLECTIVITÉS LOCALES ET DE LEURS ÉTABLISSEMENTS PUBLICS EN MATIÈRE DE CYBERSÉCURITÉ

Les collectivités locales et leurs établissements publics sont tenus à plusieurs obligations en matière de cybersécurité, dans leurs relations avec les administrés et dans l'exercice de leurs compétences.

1.1 DES OBLIGATIONS LIÉES À LA PROTECTION DES DONNÉES PERSONNELLES

Qu'est-ce qu'une donnée personnelle ?

Il s'agit d'une information se rapportant à une personne physique identifiée ou identifiable, directement (ex. : avec un nom et un prénom) ou indirectement (ex. : avec un numéro de téléphone, une plaque d'immatriculation d'un véhicule, un numéro de sécurité sociale, une adresse postale, une adresse électronique, une voix, une photographie, etc.).

POUR ALLER PLUS LOIN

La notion de donnée personnelle fait l'objet de textes juridiques de référence applicables aux collectivités locales et à leurs établissements publics :

- la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « **loi Informatique et Libertés** » ;
- le règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dit « **RGPD** »
- le guide de sensibilisation au RGPD établi par la CNIL pour les collectivités locales avec des modèles de mentions légales et des fiches pratiques.

A. En quoi les collectivités locales sont-elles concernées par l'obligation de protection des données personnelles ?

Au titre de l'exercice de leurs compétences et dans leurs relations avec les administrés, les collectivités locales et leurs établissements publics sont tenus d'appliquer la réglementation relative aux données personnelles. **Ces données sont nombreuses au sein des collectivités locales, qu'il s'agisse d'une utilisation interne (ressources humaines, vidéosurveillance, etc.) ou externe (état civil, listes électorales, inscriptions scolaires, etc.).**

Les collectivités locales sont soumises aux règles relatives à la protection des données personnelles dès lors que les données considérées font l'objet de l'une des opérations suivantes : collecte, enregistrement, stockage, extraction, adaptation ou modification, communication, etc. Il est important de noter qu'un traitement n'est pas nécessairement automatisé et qu'il peut résulter d'une simple liste tenue sur un registre manuel (ex. : fichier papier des usagers de la médiathèque).

Qu'est ce qu'un traitement de données à caractère personnel ?

Un traitement de données personnelles est une opération, ou un ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation...).

B. Qui supervise les questions relatives à la protection des données personnelles au sein des collectivités locales et de leurs établissements publics ?

Toute collectivité locale ou établissement public local, **quelle que soit sa taille, est tenu(e) de désigner un délégué à la protection des données (DPO)** qui devra exercer en toute indépendance et en étant à l'abri des conflits d'intérêts.
Ce délégué peut être :

- un agent de la collectivité locale ;
- plusieurs collectivités locales peuvent également **mutualiser la désignation** d'un délégué à la protection des données, qui pourra donc être commun à un ensemble de communes ou d'établissements (ex. : organismes publics de services numériques OPSN) ;
- un conseil externe (cabinet de conseil, avocat) désigné dans le cadre d'un contrat de prestations de services.

Attention, les fonctions de Directeur Général ou bien de Responsable du Service Informatique sont susceptibles de donner lieu à un conflit d'intérêts avec la fonction de DPO.

Pour une collectivité locale, en pratique et en général, **le responsable de traitement de données à caractère personnel est son représentant légal** : maire, président d'un établissement public de coopération intercommunal (EPCI), directeur d'un établissement (ex. : centre hospitalier). **Pour chaque traitement opéré, ce dernier est responsable de la conformité de l'ensemble des traitements de sa collectivité** à l'égard des principes et obligations prévus par le RGPD (ex. : tenue du registre).

Pour aller plus loin : la fiche ***Désigner un délégué à la protection des données dans une collectivité*** *réalisée par la CNIL.*

C. Que recouvre l'obligation de protection des données personnelles par les collectivités locales ?

a/ Avant la collecte et le traitement des données

Avant toute mise en œuvre d'un traitement, le responsable définit les mesures techniques et organisationnelles appropriées afin de respecter les principes relatifs à la protection des données (finalité explicite et légitime, nécessité de l'exploitation des données, minimisation de leur recueil, définition d'une durée de conservation, respect des droits des personnes concernées, mesures de sécurité adaptées etc.).

Lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, **le responsable du traitement des données doit effectuer au préalable une analyse de l'impact des opérations envisagées,** dite « étude d'impact sur la vie privée » ou bien encore « analyse d'impact relative à la protection des données ». **Cette analyse en amont est rendue obligatoire par le RGPD** dans certaines situations particulières, à l'instar d'une collecte de données sensibles (ex. : données biométriques) ou de l'utilisation d'une nouvelle technologie.

S'agissant des collectivités locales, plusieurs traitements nécessitent ainsi une analyse d'impact en amont : système de vidéo surveillance de la voie publique sur le territoire d'une commune, instruction des demandes et gestion des logements sociaux, prise en charge des personnes par les établissements de santé ou médico-sociaux, etc.

b/ Pendant le traitement des données

Les collectivités locales et leurs établissements publics ont l'obligation de mettre en œuvre des procédures internes au plan technique et au plan organisationnel permettant de démontrer le respect des règles relatives à la protection de données et ainsi être en conformité avec le droit. S'agissant plus spécifiquement de l'obligation d'assurer la sécurité des données, **il revient aux collectivités locales de mettre en œuvre des mesures de sécurité adaptées aux éventuels risques susceptibles de peser sur les données personnelles** (destruction, perte, altération, diffusion ou accès non autorisé, piratage, fuite de données…) et appropriées à la nature des données considérées.

Les collectivités locales et leurs établissements publics sont tenus de ne collecter, d'utiliser et de stocker des données personnelles que dans la mesure où cela est strictement nécessaire, conformément au principe de minimisation.

Le traitement de données doit se fonder sur au moins une des bases légales possibles au titre du RGPD (consentement, contrat, obligation légale, mission d'intérêt public, intérêt légitime, etc.).

Les finalités poursuivies par le traitement doivent être explicitées par les collectivités locales et leurs établissements publics :

- gestion de la paie ;
- gestion des lettres d'information ;
- inscription à un service municipal ;
- inscription à une liste électorale ;
- inscription à l'école ;
- demande de permis de construire,
  etc.

*Pour aller plus loin : la fiche pratique **dédiée aux bases légales** réalisée par la CNIL.*

En cas de violation de données personnelles

Toute atteinte aux données personnelles faisant l'objet d'un traitement de données doit être signalée à la CNIL dans un délai de 72 heures si elle présente un risque pour les droits et libertés des personnes concernées (exemples : panne accidentelle d'un serveur informatique conduisant à la destruction des fichiers de demande d'inscription à un service ; cyberattaque conduisant à une fuite d'informations bancaires d'usagers ou à une perte de confidentialité des données). Les personnes concernées doivent en être informées si les risques sont élevés (en cas de doute sur le niveau de risque, la CNIL pourra être sollicitée).

*Pour aller plus loin : la fiche **Notifier une violation de données personnelles** réalisée par la CNIL.*

c/ Conservation et archivage des données

Le cycle de vie des données à caractère personnel peut se décomposer en 3 phases successives :

- **l'utilisation courante** (base active avec l'intégralité des données) ;
- **l'archivage intermédiaire** pour répondre à l'obligation légale de conservation durant une durée limitée (base avec les données indispensables) ;
- **l'archivage définitif** (pour plus de précisions, consulter le site francearchives.fr).

La durée de conservation des données doit être proportionnée, en adéquation avec les finalités du traitement et doit être inscrite dans le registre du délégué à la protection des données pour chacun des traitements concernés. Si certaines durées de conservation sont fixées par la loi (ex. : 5 ans s'agissant des bulletins de paie), la durée de conservation de nombreux types de données sera laissée à la libre appréciation du responsable de traitement en l'absence de texte spécifique.

Focus sur les mesures de sécurité à mettre en place

Les mesures de sécurité à mettre en place dépendent des situations et doivent être déterminées en conduisant une analyse des risques (ou une Analyse d'impact relative à la protection des données, AIPD). Les mesures les plus élémen-taires qui sont requises dans la quasi-totalité des cas sont :

- la sécurisation des postes de travail (antivirus, EDR, etc.) ;
- la sécurisation des éléments réseau (pare-feu, proxy, etc.) ;
- la mise à jour régulière et suivie des systèmes et logiciels utilisés ;
- la mise en place de sauvegardes régulières et régulièrement testées ;
- la mise en place d'un système d'authentification fiable et robuste des utilisateurs ;
- le chiffrement des flux réseau à travers internet (par HTTPS) et des supports de stockage (notamment les ordinateurs portables et les clés USB) ;
- la définition d'une politique d'habilitation clairement définie pour limiter les accès aux données ;
- la mise en place de journaux de connexion et leur supervision afin de détecter une compromission.

*Pour aller plus loin : la fiche **Les 10 mesures essentielles pour assurer votre sécurité numérique** réalisée par Cybermalveillance.gouv.fr.*

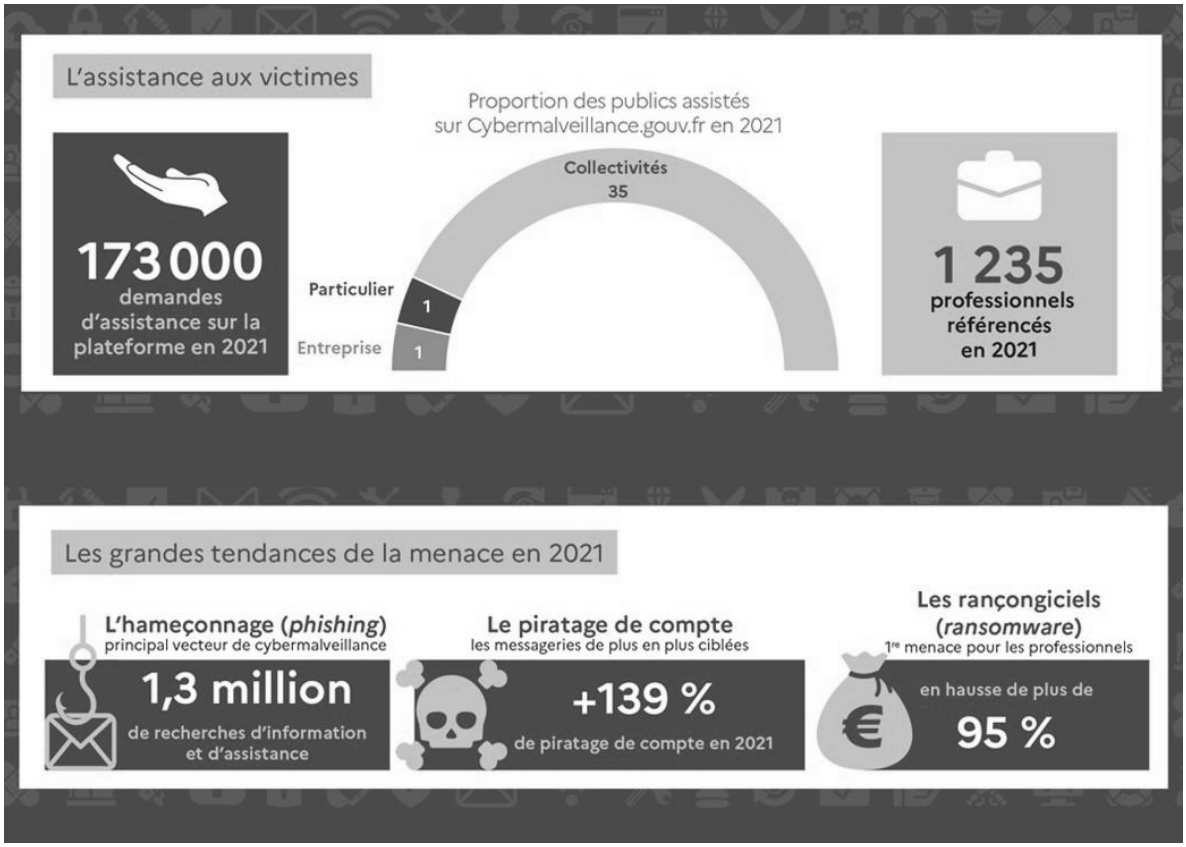
(...)

DOCUMENT 2

Les petites communes mieux informées sur les cybermenaces

Publié le 8 mars 2022 par Lucas Boncourt pour Localtis - *banquedesterritoires.fr*
Numérique, Sécurité

Quelque 3.500 petites collectivités ont fait l'objet de cyberattaques selon le rapport annuel du GIP Cybermalveillance (Acyma). Quatre associations de collectivités font désormais partie d'Acyma. Une participation qui leur permet notamment de relayer les alertes de sécurité du GIP.



© cybermalveillance.gouv

En 2021, les collectivités territoriales ne représentaient que 2% des entités assistées par le GIP Acyma, très loin derrière les particuliers (90%) et les entreprises ou associations (8%). Si le chiffre est stable par rapport à 2020 – année de forte augmentation des risques cyber - il faut se garder de le minimiser. En valeur, il représente près de 3.500 structures publiques et, rapporté à la place des collectivités dans la société française, cela fait "un particulier pour 35 collectivités", note le rapport annuel du GIP Acyma.

Les rançongiciels toujours en tête

Les collectivités restent principalement victimes de rançongiciels (20%), cybermenace qui truste le podium devant l'hameçonnage (16%), le piratage de comptes mail (16%) et la violation de données (7%). Ces attaques ont souvent des liens entre elles, l'hameçonnage tenant le rôle de "mère de toutes les attaques selon Jean-Jacques Latour, en charge du suivi de la menace à Acyma, car il précède le plus souvent un vol de données personnelles, une usurpation d'identité, l'installation d'un rançongiciel ou encore un débit frauduleux sur une carte bancaire". Les fuites de données personnelles imputables à des failles de sécurité, telles

que celle subie par l'AP-HP en octobre 2021, sont également très préoccupantes. Les données personnelles, revendues sur le darknet, provoquent des vagues d'attaques par hameçonnage, avec de faux mails, faux SMS et ou encore des tentatives de fraude au support technique. Un scenario susceptible d'arriver aux collectivités laissant fuiter des données de leurs usagers.

L'AMF relaie les cyberalertes

Beaucoup d'attaques pourraient cependant être évitées par des pratiques d'hygiène informatique assez basiques. Parmi celles-ci la mise en place de correctifs dès qu'une faille de sécurité est repérée. Ce volet prévention fait partie des nouveaux services mis en place par le GIP. "Alerte cyber vise à informer les professionnels des failles de sécurité majeures pouvant affecter leur activité. L'AMF, qui a rejoint le GIP en 2021, a demandé à en être destinataire pour la relayer auprès des communes", a expliqué Jérôme Notin, directeur d'Acyma. Trois alertes cyber ont ainsi été relayées en 2021. L'Association des maires de France a par ailleurs été étroitement associée à la réalisation de vidéos de sensibilisation ciblant les maires ainsi qu'à la réalisation du questionnaire d'autoévaluation "immunité cyber" conçu en partenariat avec l'Anssi et l'unité cyber de la gendarmerie. L'AMF rejoint ainsi Régions de France, l'Avicca et l'association Déclic (fédération des structures de mutualisation numériques) pour porter la voix des petites collectivités. On rappellera que celles-ci ne bénéficient pas de l'appui de l'Anssi en cas de cyberattaque et sont invitées à se tourner vers Acyma et les gendarmes. Autre arrivée marquante au sein du GIP, celle de la Cnil qui trouve avec la cybersécurité un levier supplémentaire pour faire appliquer le RGPD.

Au moins un prestataire labellisé par région

Côté prestataires, le GIP a poursuivi en 2021 sa politique de labellisation des professionnels de la cybersécurité et "en particulier les prestataires adaptés aux besoins des petites structures". Le nombre de labellisés est passé de 50 à 161, sur les quelque 1.200 prestataires répertoriés par Acyma. L'objectif de proposer un interlocuteur cyber de proximité à chaque victime est cependant encore très théorique avec à peine un prestataire labellisé en (ex)région Centre, à la Martinique et la Guadeloupe et 5 dans le Grand Est. Autant dire qu'en cas de cyberpandémie, ceux-ci risqueront fort d'être débordés.

Ukraine : une menace cyber surestimée ?

"On s'attendait tous à des impacts cyber avec le conflit ukrainien mais pour le moment on ne voit rien", a indiqué Jérôme Notin. Une affirmation qui corrobore l'analyse du chef d'état-major Thierry Burkhard dans son interview au Monde du 6 mars. Néanmoins, la vigilance reste de mise comme le rappelle une note du Cert mise à jour le 7 mars. La note détaille notamment les cyberattaques dont ont été victimes les infrastructures numériques ukrainiennes. Si les attaques par déni de service ou défigurations de sites sont peu préoccupantes, il en va tout autrement des "wipers", des logiciels semblables aux rançongiciels mais dont la particularité est d'effacer définitivement les données des machines infectées. Le Cert alerte en outre sur le risque d'exploitation du conflit armé par des cyberdélinquants.

Les collectivités territoriales face à la cybercriminalité

Fiche n° 16
LE PLAN REPRISE D'ACTIVITÉ (PRA) / LE PLAN CONTINUITÉ D'ACTIVITÉ (PCA)

Préambule

L'incident de sécurité majeur et impactant lourdement le système d'information est, de nos jours et ce malgré l'ensemble des solutions de sécurité existantes, quasiment inévitable. Il est donc nécessaire de prévoir cet incident et surtout de mettre en place des mécanismes pour pallier les dégâts infligés à l'infrastructure. Un des moyens les plus sûrs est de se doter de procédures de reprise d'activité et de restauration de données. Ces différents éléments sont à mettre en place en fonction du besoin exprimé par la collectivité sur les éléments fonctionnels critiques du système préalablement identifiés.

Un Plan de Reprise d'Activité permet d'assurer, en cas de crise majeure ou importante d'un système informatique, la reconstruction de son infrastructure et la remise en route des applications vitales au fonctionnement d'une entité.

Le Plan de Reprise d'Activité doit permettre, en cas de sinistre, de basculer sur un système de substitution capable de prendre en charge les besoins informatiques nécessaires au fonctionnement minimal de la collectivité. Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par les élus en charge de la question.

Le Plan de Reprise d'Activité (PRA) est à distinguer du Plan de Continuité d'Activité (PCA) : ce dernier a pour objectif de poursuivre l'activité du service sans interruption et d'assurer la disponibilité des informations quels que soient les problèmes rencontrés. Le PRA en est un sous-ensemble qui décrit les mesures qui doivent être déclenchées à la survenue d'un sinistre ou incident majeur ayant entraîné une interruption de l'activité.

Pour être efficace, ce plan de reprise doit être validé par les utilisateurs des différentes solutions et testé de manière régulière en fonction de l'évolution du système d'information. La mise en fonction de manière unique d'un plan lors d'une panne majeure d'un système est vouée à l'échec. Elle peut même, au pire, être contre-productive et faire perdre un temps précieux dans la remise en route des éléments de production.

Le Plan de Reprise parfait et standard n'existe pas. Chacune des collectivités mettant en place ce type de procédure devra le faire de manière unique. Cette procédure est, en effet, fortement liée à l'organisation de son entité et à son système d'information souvent propre à une collectivité et ce, quelle que soit sa taille.

Ces procédures dans leur ensemble sont très peu mises en place en collectivité de manière rigoureuse car très coûteuses et pas toujours pertinentes. La perte d'exploitation, si elle n'est pas trop importante, reste plus possible pour une administration que pour une société dont l'économie repose essentiellement sur son Système d'information.

Cependant, cette perte d'exploitation doit être minimisée au maximum pour éviter tout arrêt de l'activité préjudiciable en termes d'image et en termes fi-nanciers.

Etapes de la mise en place d'un plan de reprise /continuité

Pour qu'un plan de reprise/continuité soit réellement adapté aux exigences de la collectivité, il doit reposer sur une analyse de risque et une analyse d'impact :
L'analyse de risque débute par une identification des menaces sur l'informatique. Les menaces peuvent être d'origine humaine ou « naturelle ». Elles peuvent être internes à l'entreprise ou externes.
On déduit ensuite le risque qui découle des menaces identifiées, on en mesure l'impact possible. Enfin, on décide de mettre en œuvre des mesures d'atténuation des risques en se concentrant sur ceux qui ont un impact significatif.

L'analyse d'impact consiste à évaluer quel est l'impact d'un risque qui se matérialise, et à déterminer à partir de quand cet impact est intolérable, généralement parce qu'il met en danger les processus essentiels de la collectivité.

Une analyse de risque réussie est le résultat d'une action collective impliquant tous les acteurs du système d'information: techniciens, utilisateurs et managers.

Choix de la stratégie de sécurisation

Il existe plusieurs méthodes pour assurer la continuité de service d'un système d'information. Les méthodes se distinguent entre préventives et curatives. Les méthodes préventives sont souvent privilégiées, mais décrire les méthodes curatives est une nécessité car aucun système n'est fiable à 100 %.

Pour une mise en œuvre dans de bonnes conditions, il faut établir les procédures suivantes :

Les procédures qui mettent la stratégie en œuvre. Ceci inclut les procédures d'intervention immédiate (qui prévenir ? qui peut démarrer le plan et sur quels critères ? où les équipes doivent-elles se réunir ? etc.).

Les procédures pour rétablir les services essentiels, y compris le rôle des prestataires externes.

Toutes ces procédures doivent être accessibles aux membres des équipes de pilotage, même en cas d'indisponibilité des bâtiments.

Mesures préventives

La sauvegarde des données

Voir la fiche n° 3 page 25

Les systèmes de secours

Il s'agit de disposer d'un système informatique équivalent à celui pour lequel on veut limiter l'indisponibilité : ordinateurs, périphériques, systèmes d'exploitation, programmes particuliers, etc. Une des solutions consiste à créer et main-tenir un site de secours, contenant un système en ordre de marche capable de prendre le relais du système défaillant. Selon que le système de secours sera implanté sur le site d'exploitation ou sur un lieu géographiquement diffé-rent, on parlera d'un secours in situ ou d'un secours déporté.

Pour répondre aux problématiques de recouvrement de désastre, on utilise de plus en plus fréquemment des sites délocalisés. Ces solutions sont de plus en plus proposées par les éditeurs de logiciels métiers. Elles restent toutefois très dépendantes de la bande passante disponible sur la zone d'exploitation.

Les sites de secours (in situ ou déportés) se classent selon les types suivants :

• Salle blanche (une salle machine protégée par des procédures d'accès particulières, généralement secourue électriquement). Par extension, on parle de salle noire pour une salle blanche entièrement pilotée à distance, sans aucun opérateur à l'intérieur.

• Site chaud : site de secours où l'ensemble des serveurs et autres systèmes sont allumés, à jour, interconnectés, paramétrés, alimentés à partir des données sauvegardées et prêts à fonctionner.

• Site froid : site de secours qui peut avoir une autre utilisation en temps normal. Les serveurs et autres systèmes sont stockés mais non installés, connectés, etc. Lors d'un sinistre, un important travail doit être effectué pour mettre en service le site, ce qui conduit à des temps de reprise longs (quelques jours). Mais son coût de fonctionnement, hors période d'activation, est faible, voire nul.

• Site tiède : site de secours intermédiaire. En général, on trouve des machines installées (mise à jour décalée par rapport au site de production) avec les données sur bande mais non importées dans les systèmes de données.

Plus les temps de rétablissement garantis sont courts, plus la stratégie est coûteuse. Il faut donc choisir la stratégie qui offre le meilleur équilibre entre le coût et la rapidité de reprise.

Mesures curatives

Selon la gravité du sinistre et la criticité du système en panne, les mesures de rétablissement seront différentes.

La reprise des données

Dans cette hypothèse, seules des données ont été perdues. L'utilisation des sauvegardes est nécessaire et la méthode, pour simplifier, consiste à réimplanter le dernier jeu de sauvegardes. Cela peut se faire dans un laps de temps court (quelques heures), si l'on a bien identifié les données à reprendre et si les méthodes et outils de réimplantation sont accessibles et connus.

Le redémarrage des applications

A un seuil de panne, plus important, une ou des applications sont indisponi-bles. L'utilisation d'un site de secours est envisageable, le temps de rendre disponible l'application en cause.

Le redémarrage des machines

•Provisoire : utilisation des sites de secours
•Définitif : après dépannage de la machine d'exploitation habituelle, y re-basculer les utilisateurs, en s'assurant de ne pas perdre de données et si possible de ne pas déconnecter les utilisateurs.

Exercices et maintenance

Le but de l'exercice est multiple :

•Vérifier que les procédures permettent d'assurer la reprise/continuité d'activité
•Vérifier que le plan est complet et réalisable
•Maintenir un niveau de compétence suffisant parmi les équipes de pilotage
•Évaluer la résistance au stress des équipes de pilotage

Un plan doit aussi être revu et mis à jour régulièrement (au moins une fois par an) pour tenir compte de l'évolution de la technologie et des objectifs de la collectivité.

QUE FAIRE EN CAS DE CYBERATTAQUE ? (dirigeants)

(extrait)

Méthodologie synthétique de gestion des cyberattaques pour les dirigeants des entreprises, associations, collectivités, administrations.

1 PREMIERS RÉFLEXES

Alertez immédiatement votre support informatique si vous en disposez afin qu'il prenne en compte l'incident (service informatique, prestataire, personne en charge).

Isolez les systèmes attaqués afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local.

Constituez une équipe de gestion de crise afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique…).

NE PAYEZ PAS DE RANÇON !

Car vous encourageriez les cybercriminels à chercher à vous attaquer à nouveau et financeriez leur activité criminelle tout en n'ayant aucune garantie qu'ils tiendront leur parole.

Tenez un registre des évènements et actions réalisées pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.

Préservez les preuves de l'attaque : messages reçus, machines touchées, journaux de connexions…

2 PILOTER LA CRISE

Mettez en place des solutions de secours pour pouvoir continuer d'assurer les services indispensables. Activez vos plans de continuité et de reprise d'activité (PCA-PRA) si vous en disposez.

Déclarez le sinistre auprès de votre assureur qui peut vous dédommager voire vous apporter une assistance en fonction de votre niveau de couverture assurantielle.

FAITES-VOUS ACCOMPAGNER

Par des prestataires spécialisés en cybersécurité que vous pourrez trouver sur **www.cybermalveillance.gouv.fr.**

Alertez votre banque au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.

Déposez plainte avant toute action de remédiation en fournissant toutes les preuves en votre possession.

Identifiez l'origine de l'attaque et son étendue afin de pouvoir corriger ce qui doit l'être et éviter un nouvel incident.

Notifiez l'incident à la CNIL dans les 72h si des données personnelles ont pu être consultées, modifiées ou détruites par les cybercriminels.

Gérez votre communication afin d'informer avec le juste niveau de transparence vos administrés, clients, collaborateurs, partenaires, fournisseurs, médias…

(…)

L'ESSENTIEL SUR LA CYBERSÉCURITÉ : ENTREPRISES, COLLECTIVITÉS TERRITORIALES : TOUTES CONCERNÉES ! (extraits)

Le rapport de la délégation sénatoriale aux entreprises établi par Sébastien Meurant et Rémi Cardon a souligné **l'ampleur du risque cyber** pour les entreprises, en particulier les PME, mais aussi pour toutes les organisations territoriales. Ce sujet a été à nouveau largement évoqué lors de la 5ème Journée des entreprises qui s'est déroulée au Sénat le 21 octobre 2021, puis lors de la table-ronde, organisée avec la délégation aux collectivités territoriales le 28 octobre. Suite à ces travaux, il est apparu que **les entités publiques, à savoir les** collectivités territoriales, établissements de santé et établissements publics, **sont également concernées par cette menace qui peut paralyser le fonctionnement du service public**. La réponse appropriée pour réduire cette menace nécessite une synergie des actions publiques et privées.

1. UNE PRISE DE CONSCIENCE TARDIVE ET INSUFFISANTE DE L'AMPLEUR DES CYBERMENACES

En 2020, près de 30 % des collectivités territoriales ont été victimes d'une attaque au rançongiciel selon une étude du Clusif[1]. En effet, cette même année a vu le nombre de cyberattaques contre des collectivités territoriales **augmenter de 50 %** par rapport à 2019[2].
En mai 2020, Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'est déclaré « ***inquiet*** »[3] pour la cybersécurité des collectivités territoriales. Pourtant, la cybersécurité était, en 2018, **loin d'être une préoccupation centrale des collectivités territoriales**. Selon un sondage Ifop[4] pour l'Observatoire des Politiques Publiques, en janvier 2020 encore seuls 33 % des fonctionnaires territoriaux interrogés déclaraient que leur organisation avait mis en place un programme de cybersécurité. Le manque de budget et de personnes qualifiées justifie en partie les difficultés des collectivités territoriales en matière de cyberprotection de leurs outils et données numériques.
Les élus locaux prennent désormais, et de manière croissante, la pleine mesure de ce risque. Les associations d'élus accompagnent la prise de conscience des collectivités territoriales, qui demeure inégale sur le territoire. Ainsi, l'Association des maires de France (AMF) a édité en novembre 2020 un **guide** intitulé « *Cybersécurité : toutes les communes et les intercommunalités sont concernées* ».
Faute de temps mais également de compétences et de ressources humaines qualifiées, les petites communes se contentent parfois d'installer ponctuellement un anti-virus, alors que la cybersécurité doit être **mise à jour en permanence**. Or, la pénurie de compétences est telle que l'ANSSI a lancé un « observatoire des métiers de la cybersécurité » afin d'aider les acteurs concernés dans leur politique de recrutement et de formation. Dans ce contexte, la **mutualisation au plus près des collectivités concernées** s'avère être un choix judicieux pour mettre en commun les efforts, affronter les pénuries de professionnels qualifiés et ainsi mettre en place **une protection collective**.

2. LE DISPOSITIF DE CYBERPROTECTION PUBLIQUE

Le bouclier

Il s'articule autour de **l'Agence nationale de la sécurité des systèmes d'information (ANSSI)** et d'un **réseau de CERT (*Computer Emergency Response Team*)**, organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces CERT sont des centres d'alerte et de réaction aux attaques informatiques, dont les informations sont accessibles à tous. L'objectif du **volet cybersécurité de France Relance**, lancé en septembre 2020

et dont le pilotage a été confié à l'ANSSI, doit renforcer la sécurité des administrations, des collectivités, des établissements de santé et autres organismes publics, tout en dynamisant l'écosystème industriel français.

Doté d'un fonds de **136 millions d'euros**, il comprend :

- **un parcours de cybersécurité** ayant pour objectif de renforcer la sécurité des systèmes d'information des bénéficiaires en proposant un pré-diagnostic et un accompagnement par des prestataires compétents, de la maîtrise d'ouvrage jusqu'à la mise en œuvre ;
- **des appels à projets**, pour certaines collectivités territoriales dont le niveau de cybersécurité est suffisamment mature et le besoin assez clair pour que le projet soit mené hors du cadre des « Parcours de cybersécurité ». Basés sur le cofinancement et destinés à sécuriser des systèmes d'information existants, ces projets peuvent être des prestations d'audit, d'analyse de risque, d'acquisition et de déploiement de produits... ;
- **le réseau des CSIRT régionaux** (*Computer Security Incident Response Team*), centres de réponse aux incidents cyber au profit des entités implantées sur le territoire régional, devra traiter des demandes d'assistance des acteurs de taille intermédiaire, dont les collectivités territoriales, et les mettre en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques.

La prévention et l'assistance aux victimes

Depuis 2017, la plateforme Cybermalveillance.gouv.fr, du GIP ACYMA, dispositif national de **sensibilisation, prévention et assistance** aux victimes d'actes de cybermalveillance pour les particuliers, entreprises et collectivités territoriales, est porté par un **partenariat public-privé**. Outre l'ANSSI et les principaux ministères, cette plateforme rassemble de nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des éditeurs de logiciels…

Face à la recrudescence des cyberattaques contre les collectivités territoriales, Cybermalveillance.gouv.fr a créé un groupe de travail dédié à ce public composé de l'ANSSI, l'AVICCA, la Banque des Territoires, le CoTer Numérique et Déclic, et lancé un **programme de sensibilisation** à destination des élus.

Il comporte **trois étapes** :

- Étape une : Menaces et réflexes essentiels pour la sécurité numérique des collectivités
- Étape deux : Vigilance face aux cyberattaques : les collectivités sont toutes concernées !
- Étape trois : Sensibilisation aux risques numériques : les collectivités se mobilisent

Les **ressources documentaires** destinées aux collectivités territoriales sont les suivantes :

- Vidéos de sensibilisation sur les risques numériques
- Campagne de sensibilisation inter-régions sur la cybersécurité
- Supports pour résumer les premiers gestes en cas d'attaque
- I.M.M.U.N.I.T.É.Cyber : questionnaire pour sensibiliser les élus à la cybersécurité

(...)

[1] *https://clusif.fr/newspaper/le-risque-associe-aux-rancongiciels-demeure-sous-evalue-dans-les-collectivites-territoriales-clusif/*

Le Clusif est l'association de référence de la sécurité du numérique en France.

[2] *https://www.lesechos.fr/tech-medias/hightech/flambee-dattaques-informatiques-contre-les-mairies-en-france-1284537*

[3] *Face aux membres de la commission de la défense nationale et des forces armées de l'Assemblée nationale : https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/cion_def/l15cion_def1920054_compte-rendu.pdf*

[4] *https://2020.forum-fic.com/Data/ElFinder/s23/PDF/20200206-note-cyber-et-territoires.pdf?_t=1581012131*

#CYBERATTAQUE

Délégation aux collectivités **TERRITORIALES**

Délégation aux **ENTREPRISES**

QUE FAIRE EN CAS DE CYBERATTAQUE ?

1 **Déconnectez du réseau** tous les ordinateurs infectés, ainsi que les disques externes et autres terminaux reliés.

2 **Contactez des prestataires externes expérimentés en neutralisation des attaques informatiques.** Vous pouvez faire appel à **votre assurance.** L'ANSSI propose également une liste de prestataires habilités.

3 **Portez plainte** auprès de la gendarmerie ou du commissariat de proximité.
Vous pouvez aussi adresser un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.
Des services spécialisés se chargent ensuite de l'enquête.

4 Si des **données à caractère personnel** ont été dérobées, **avertissez la Cnil** dans les 72h.

5 Si vous êtes un **opérateur d'importance vitale, prévenez l'ANSSI** dans les meilleurs délais.

6 Vous pouvez également **signaler les faits** via la plateforme de signalement **« Pharos »** ou le numéro dédié : 0811 02 02 17

7 En parallèle, si nécessaire, vous pouvez élaborer un plan de communication pour rassurer vos usagers.

ET APRÈS ?

Consultez le site **CYBERMALVEILLANCE.GOUV.FR**. Il peut **vous mettre en relation avec des prestataires de services informatiques de proximité agréés (cyber-experts) pour remettre votre système en état de fonctionnement et le sécuriser.**
Une fois l'incident terminé, **prenez des précautions** :

- sauvegardes et mises à jour régulières des logiciels
- sécurisation de la borne d'accès internet
- souscription d'un contrat d'assurance spécifique

NOVEMBRE 2021

www.senat.fr

MAIRE info

Cybersécurité : quelles sont les obligations et responsabilités des collectivités locales ?

06/07/2022
Cybermalveillance

Cybermalveillance.gouv.fr et la Commission nationale de l'informatique et des libertés (Cnil) ont publié le 1er juillet un guide à destination des élus locaux et des agents territoriaux. Ce dernier est un résumé de leurs obligations et responsabilités en matière de cybersécurité.

Une enquête publiée en début d'année par Cybermalveillance.gouv.fr a montré que les élus de nombreuses communes de moins de 3 500 habitants estimaient que le risque de cyberattaques pour leur commune était faible voire inexistant. 65 % de ces collectivités locales ne prennent pas en compte le risque de cyberattaque.

Pourtant, *« les collectivités de toutes tailles sont la cible d'actes de cybermalveillance de plus en plus nombreux et dont les conséquences ne sont pas négligeables : systèmes d'information bloqués, vol de données personnelles, missions de service public interrompues, etc. »*. C'est ce qui est rappelé dans le nouveau guide de Cybermalveillance.gouv.fr et de la Commission nationale de l'informatique et des libertés (Cnil) intitulé *Obligations et responsabilités des collectivités locales en matière de cybersécurité.*

Cette publication sert de piqûre de rappel aux élus et agents quant au cadre juridique en vigueur. Les collectivités locales ont en effet trois obligations liées à la cybersécurité : la protection des données personnelles, la mise en œuvre des téléservices locaux et l'hébergement des données de santé. Il est d'autant plus important d'avoir conscience de cela qu'en cas de cyberattaque *« la responsabilité des collectivités locales et/ou de leurs agents peut être engagée, sur le plan administratif, civil ou pénal. »*

Trois grandes obligations

Le guide est synthétique et ses auteurs font le point sur les trois obligations qui concernent les collectivités en matière de cyberprotection. D'abord, une collectivité locale doit protéger les données personnelles de ses administrés, qu'il s'agisse d'une utilisation interne (ressources humaines, vidéosurveillance...) ou externe (état civil, inscriptions scolaires...). C'est le délégué à la protection des données (DPO) qui supervise la gestion des données.

Pour ce faire, et assurer une protection optimale, plusieurs mesures sont à mettre en place comme *« la sécurisation des postes de travail (antivirus, etc.) »*, *« la sécurisation des éléments réseau (pare-feu, proxy, etc.) », « la mise à jour régulière et suivie des systèmes et logiciels »* ou encore *« la mise en place d'un système d'authentification fiable et robuste des utilisateurs. »*

Deuxième obligation : sécuriser les téléservices locaux. Les auteurs du guide rappellent que *« la mise en œuvre de téléservices locaux impose des obligations aux collectivités locales et à leurs établissements publics »*. Cela concerne les démarches comme la demande de permis de construire, demande de logement social, demande de pièces extraites de l'état civil, inscription à la cantine scolaire, etc. L'ensemble de ces téléservices doit satisfaire aux exigences du Référentiel général de sécurité, dit RGS, qui sont des règles de sécurité applicables aux collectivités et prestataires.

Enfin, une collectivité se doit d'assurer la sécurisation de l'hébergement des données de santé. Ce type de données *« est recueilli à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social: radios, résultats de laboratoire, comptes rendus médicaux, etc. »* Les données sont utilisées, par les collectivités locales, pour les départements au titre de la gestion des aides sociales et pour les communes au titre des centres communaux d'action

sociale. Les collectivités se doivent d'être conformes à la réglementation de la protection des données personnelles et à la réglementation spécifique s'appliquant aux activités consistant à héberger des données de santé, lorsqu'elles sont externalisées auprès d'un tiers.

Des risques de sanctions

En cas de cyberattaque, s'il est constaté un manquement à ces trois obligations, la responsabilité des collectivités locales et/ou de leurs agents peut être engagée. « *Lorsqu'il est constaté (…) que des dispositions relatives à la loi dite Informatique et libertés et/ou au RGPD ont été méconnues, la Cnil a la faculté de prononcer des sanctions administratives »* **avec des sanctions pécuniaires pouvant aller jusqu'à 20 millions d'euros.**

Les citoyens peuvent aussi *« engager la responsabilité de l'administration pour faute lorsque cette dernière a manqué à ses obligations et que le manquement leur a causé un préjudice. »*

Concrètement, des entreprises ou des administrés peuvent réclamer à une collectivité locale une indemnisation des préjudices subis du fait des conséquences d'une cyberattaque. Le système d'inhumation d'une ville peut être stoppé net par une cyberattaque pendant plusieurs jours et, dans ce cas, les familles peuvent par exemple demander un remboursement des frais de chambre mortuaire. Répétons qu'une telle procédure ne peut être engagée que si la collectivité locale est en tort et qu'elle n'a pas respecté les obligations de prévention.

Un élu ou un agent peut aussi faire l'objet de sanctions pénales en cas d'atteinte grave aux règles du RGPD. *« Par exemple, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures destinées à garantir la sécurité des données ou de ne pas tenir de registre des traitements. »* **Il est aussi expliqué dans le guide qu'un maire ou un agent peut aussi être condamné pour des fautes d'imprudence et de négligence** *« en cas de faute caractérisée exposant autrui à un risque grave et immédiat »*. **Une barrière de parking peut faire l'objet d'un dysfonctionnement à cause d'une cyberattaque et blesser un citoyen. Le responsable peut être pénalement puni** *« s'il s'avère que des manquements graves à la sécurité des systèmes d'information les ont rendus particulièrement vulnérables à une cyberattaque. »*

Un besoin de sensibilisation

La publication de ce nouveau guide s'inscrit dans un contexte où le nombre de collectivités touchées par des cyberattaques ne cesse d'augmenter. En fin d'année 2021, le Sénat insistait déjà sur le besoin de faire de la pédagogie et de la sensibilisation autour de ces sujets avec les élus et agents. (lire *Maire info* **du 3 novembre) Françoise Gatel avait alors rappelé que l'AMF et l'Agence nationale de la sécurité des systèmes d'information ont réalisé des guides pour les collectivités sur la cybersécurité,** *« qui sont des outils indispensables. »*

Ce guide est une ressource supplémentaire qui encourage les élus, dirigeants et agents publics dans les collectivités locales et leurs établissements publics, à s'investir dans ces questions de cybersécurité en respectant notamment strictement les différentes réglementations présentées dans le guide.

LE COURRIER DES MAIRES
et des élus locaux

Cybersécurité : « Il reste beaucoup à faire dans les collectivités locales »

AURÉLIEN HÉLIAS

Publié le 04/01/2023 à 11h32

2022 a vu les cyberattaques se multiplier contre les collectivités locales, paralysant l'action de leurs administrations et de leurs services publics pendant plusieurs jours voire semaines. Sous-directeur stratégie de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Yves Verhoeven dresse le bilan de l'année écoulée et détaille les moyens mis en œuvre par l'agence pour prévenir les futures attaques contre le secteur public local et accompagner élus et agents dans leur politique de cybersécurité.

De nombreuses collectivités ou hôpitaux publics locaux ont été visés par des cyber-attaques en 2022 ; quels sont les derniers chiffres en votre possession ? Comment expliquer ce phénomène croissant ?

Yves Verhoeven : À ce stade, nous n'avons pas encore de chiffres consolidés pour 2022. Mais la menace ne faiblit pas, notamment vis-à-vis des collectivités territoriales. En 2021, plus de 1 000 intrusions avérées ont été relevées et le phénomène des rançongiciels reste significatif, avec près de 200 cas. Sur les 1 000 attaques répertoriées, 19 % visaient des collectivités, 7 % des établissements de santé. S'y ajoutent bien sûr les cas dont nous n'avons pas connaissance...

Le secteur public local est-il particulièrement vulnérable à la cybermalveillance ? Aux rançongiciels ?

Au cours de l'année 2022, il y a effectivement eu des vagues d'attaques par rançongiciels contre des collectivités, notamment des conseils départementaux. Mais c'est un phénomène qui touche l'ensemble des catégories d'acteurs.

Les élus locaux et agents des administrations locales sont-ils insuffisamment conscients des risques ? Suffisamment formés à la cybersécurité ?

Il reste beaucoup à faire, notamment pour sensibiliser. Mais pas uniquement les élus locaux, c'est la société en général qui doit progresser. Au sein des collectivités locales, des efforts ont été faits qui devront être poursuivis pour former les agents et mettre en place une organisation adaptée aux enjeux de cybersécurité.

Comment l'ANSSI peut-elle les aider ? Toutes les collectivités, quel que soit leur statut, leur strate, peuvent-elles solliciter l'agence ?

Les délégués de l'ANSSI sur le terrain sont capables de mener des actions de sensibilisation et de formation. La gendarmerie et le GIP Action contre la Cybermalveillance ACYMA, via la plateforme cybermalveillance.gouv.fr, fruit d'un partenariat avec le ministère de l'Intérieur, prodiguent également des conseils tant de prévention qu'en réponse à un incident cyber.

Le ministère a depuis quelque mois mandaté les préfets pour mener une politique au niveau local sur la sécurité numérique des collectivités. L'initiative menée par le préfet du Morbihan avec les associations de maires et de présidents EPCI fait de ce territoire un département d'excellence en matière de cybersécurité, avec un plan en cinq actions qui s'adresse aux collectivités, toutes

catégories confondues. Ce plan pourrait servir d'inspiration pour une généralisation à l'ensemble des départements.

Comment l'Anssi couvre-t-elle le territoire ?

Depuis peu, chacune des régions métropolitaines a un à deux délégués par région – s'y ajoute un délégué responsable des outre-mer - à même de mener des opérations structurantes. En appui des autres réseaux de l'État, ces délégués peuvent aussi réaliser des actions de sensibilisation.

Au cours des derniers mois, des initiatives ont été menées au sein des territoires à l'image des parcours de cybersécurité financés par le plan de relance et qui ont bénéficié à 750 collectivités locales. L'ANSSI soutient également la création de centres régionaux de réponse aux incidents cyber – les CSIRT, Computer Security Incident Response Team - qui fourniront assistance et conseil en cas de cyberattaques.

En quoi consiste « MonServiceSécurisé » proposé par l'ANSSI ? Quelles sont ses fonctionnalités ?

C'est un service développé en partant du constat que l'ensemble des collectivités, de même que leurs administrations, sont soumises à des exigences réglementaires dont certaines sont difficiles d'accès, pour nombre d'entités concernées, notamment les petites collectivités. L'objectif est de réussir un accompagnement, clé en main, de la cybersécurité des services web, smartphones, API. Cette application est le fruit d'une démarche innovante, celle du laboratoire d'innovation publique qui fait l'objet d'une start-up d'État soutenue par la Dinum (la direction interministérielle du numérique, ndlr), et est développée de manière collaborative. C'est une vraie évolution du service de l'ANSSI, au-delà des exigences normatives, que de fournir des outils accessibles. La plateforme est accessible depuis le 13 décembre à tous les agents publics.

Votre agence doit voir ses ressources humaines étoffées en 2023 : quelles seront ses nouvelles tâches, son action en faveur de la cybersécurité du secteur public local ?

On demeure sur une courbe de croissance relativement régulière avec quelques dizaines d'agents, ce qui permet de consolider le dispositif des délégués territoriaux et notre capacité de « cyberpompier » pour aider les collectivités. Nous allons aussi préparer la mise en œuvre de la directive NIS 2 qui nous permet de réguler un certain nombre d'entités. L'ANSSI est le régulateur des opérateurs de service d'importance vitale et de services essentiels, principalement des entreprises et quelques autres entités publiques. Ces entités doivent nous déclarer leur SI, mettre en œuvre une politique de cybersécurité, se soumettre aux contrôles et nous signaler leurs incidents de cybersécurité. Or ce champ des opérateurs va être élargi par cette directive à certaines collectivités.

Quels sont vos partenaires pour amplifier la cybersécurité du secteur public local ?

Il faut souligner le rôle important d'un certain nombre d'acteurs qui accompagnent la transformation numérique des acteurs publics : opérateurs publics de services numériques (OPSN), centres de gestion départementaux, syndicats mixtes chargés du numérique... Ils peuvent avoir une action en profondeur sur la cybersécurité, on les a identifiés comme des relais importants et ils facilitent la mutualisation, un atout sur ce sujet où les ressources sont rares et chères.

Les élections, organisées par les communes qui transmettent les résultats aux préfectures, sont-elles l'un des points de vigilance majeurs pour la cybersécurité de demain en France ?

La transmission des résultats des élections et leur consolidation sont des sujets qui ont été identifiés et qui font l'objet de travaux. La sécurité du processus électoral au niveau cyber est un dossier sur lequel nous soutenons le ministère de l'Intérieur.

DOCUMENT 8

CYBERSÉCURITÉ : TOUTES LES COMMUNES ET INTERCOMMUNALITÉS SONT CONCERNÉES

(extrait)

(...)

RELATIONS AVEC DES TIERS

Recommandations	
15	Formaliser les exigences de sécurité puis vérifier l'adéquation des mesures proposées par les prestataires notamment à travers un « plan d'assurance sécurité » (cf. guide de l'ANSSI « Maîtriser les risques de l'infogérance »).
16	Inclure systématiquement un chapitre contractuel sur la sécurité numérique pour les prestations, qu'elles soient ou non informatiques.
17	Inclure dans les cahiers des charges des conventions de délégation de service public, des clauses explicites et express précisant la répartition des responsabilités et des obligations entre le délégant et le délégataire.
18	Inclure systématiquement la clause de réversibilité dans les documents contractuels liant la commune ou l'intercommunalité au prestataire/partenaire privé. Faire préciser aux prestataires les moyens qu'ils mettront en œuvre pour assurer cette réversibilité.

1. Quels sont les menaces et les points de vulnérabilité dans les communes et les intercommunalités ?

Les communes et les intercommunalités, quelle que soit leur taille, peuvent être la cible d'attaques informatiques. Ces cyberattaques peuvent être d'origine externe (site internet, téléphone mobile, cybercriminels...) ou interne (élus, agents, prestataires, clés USB, mots de passe faibles...) et utiliser des vulnérabilités techniques, juridiques, organisationnelles ou humaines.

1. Les menaces : tendance et typologie des incidents numériques

Le panorama qui suit n'est pas une représentation exhaustive de la réalité des évènements cyber affectant les communes et les intercommunalités. Ce tableau est dressé sur la base des faits portés à la connaissance de l'ANSSI. Ainsi, la vision qui en résulte n'en est que partielle et repose sur le besoin d'aide exprimé par les bénéficiaires et leur volonté de signaler ces évènements à l'ANSSI.

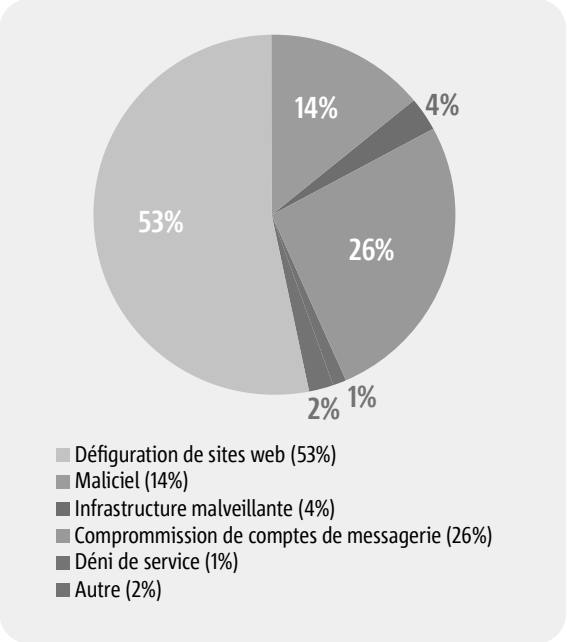
Le périmètre retenu pour cette étude comprend tous les incidents de sécurité d'origine cyber affectant les communes, les communautés de communes, d'agglomération, urbaines ainsi que les métropoles françaises traités par l'ANSSI tout au long de l'année 2019.

Les incidents correspondent aux signalements relevant d'une compromission* avérée de l'entité victime ou d'une attaque réussie. Dans le cas de compromissions dont la gravité et l'impact requièrent un engagement renforcé de l'agence, les incidents peuvent alors évoluer en incident majeur voire en opération de cyberdéfense.

A - Panorama de la situation cyber

Au cours de l'année 2019, l'ANSSI a recensé et traité 92 incidents de sécurité d'origine cyber affectant les communes et les intercommunalités, soit près de 25% des incidents totaux traités par l'agence sur cette période. Cette proportion conséquente reste toutefois à nuancer au regard de la gravité relative des compromissions détectées sur le système d'information des entités concernées. Ces dernières n'ont pas fait l'objet en 2019, ni même les années précédentes, d'incident majeur ou d'opération de cyberdéfense.

Comme représenté ci-après, on dénombre trois grandes catégories de compromission affectant les systèmes d'information des collectivités, objet de cette étude :



Si les deux premières catégories, malgré leur nombre, relèvent de compromissions d'impact et de gravité mineures, la troisième, quant à elle, couve une réalité non négligeable et aux impacts forts pour ces entités. En effet, sur 12 cas de compromission de système d'information avec dépôt de code malveillant, 9 d'entre eux sont relatifs à des rançongiciels* paralysant tout ou partie du parc informatique infecté.

Du fait d'une maturité à la sécurité numérique encore à développer, les communes et intercommunalités sont des cibles accessibles aux yeux d'acteurs malveillants pour qui l'attaque par rançongiciel est devenue une source de revenu efficace. Cette tendance s'inscrit dans une tendance globale qui a vu le nombre d'attaques par rançongiciel augmenter de manière drastique au cours de l'année 2019.

Panorama détaillé : la défiguration* de sites internet

La majorité (88%) des défigurations de sites Internet de communes et intercommunalités françaises est portée à la connaissance de l'ANSSI via le site ZONE-H qui recense et archive les défigurations de pages web en tout genre depuis 2002. À noter que les auteurs de défigurations sont parfois eux-mêmes susceptibles d'y soumettre ce qu'ils voient comme leurs « exploits ». Pour le restant, les signalements proviennent de particuliers, de partenaires nationaux mais rarement des victimes elles-mêmes concernées.

Lorsqu'une défiguration est portée à la connaissance de l'ANSSI, cette dernière constate la véracité des faits et, le cas échéant, transmet le signalement à l'entité concernée pour prise d'action. Dans la majeure partie des cas, l'incident est clos dans les jours qui suivent. Ainsi, le vecteur initial de compromission n'est généralement pas connu de l'ANSSI.

Panorama détaillé : la compromission de comptes de messagerie

Sur les 24 cas de compromission de comptes de messagerie signalés à l'ANSSI, 17 proviennent d'une même intercommunalité. L'actualité de cette dernière, quasi exhaustivement portée à la connaissance de l'agence, est loin d'être un lieu d'exception cyber et permet donc, par extension, d'entrevoir les problématiques opérationnelles rencontrées par les autres entités du périmètre. Les incidents ne sont, en effet, pas systématiquement détectés ni remontés à l'ANSSI.

CYBERSÉCURITÉ : TOUTES LES COMMUNES ET INTERCOMMUNALITÉS SONT CONCERNÉES

La prise de conscience récente des enjeux liés à l'hygiène informatique et le développement nouveau de la culture de la sécurité numérique des personnels des communes et des intercommunalités laissent encore ces dernières être des cibles privilégiées et faciles d'accès pour la distribution d'hameçonnage à des fins cybercriminelles. À titre d'exemple, il est courant que des couples d'identifiants et mots de passe de comptes de messagerie des personnels des communes et intercommunalités se retrouvent dans des divulgations, facilitant ainsi leur compromission ultérieure.

Panorama détaillé : la compromission avec attaque de maliciels*

C'est sans nul doute la catégorie d'incidents dans laquelle se situent les attaques ayant eu l'impact le plus marquant pour le périmètre étudié. Outre les cas de dépôt opportuniste de codes malveillants, notamment à des fins de cryptominage*, neuf cas sur douze ont trait à une attaque par rançongiciel. Si, pour l'une de ces attaques seulement, le périmètre de compromission s'est restreint à un seul poste utilisateur, les autres ont affecté fortement le fonctionnement du système d'information infecté allant, parfois, jusqu'à sa nécessaire reconstruction complète. L'impact opérationnel et le coût associé de ces attaques sont autant d'arguments qui doivent amener les communes et les intercommunalités à se saisir du sujet et renforcer leur sécurité informatique.

Fait intéressant, sur ces huit incidents notables, quatre ont été portés à la connaissance de l'ANSSI par voie de presse. Une fois le contact pris, une assistance a donc pu leur être proposée.

Panorama détaillé : autres types d'incidents

D'autres incidents mineurs, de par leur nombre et leur gravité, ont affecté des communes françaises. On dénombre, ainsi, un cas d'attaque par déni de service* et plusieurs cas de compromission de serveurs pour héberger des activités malveillantes comme des pages d'hameçonnage*.

B - Exemples d'incidents notables

Exemple 1 : site internet d'une commune aspiré par un nom de domaine en .tk

En août 2017, le responsable de la sécurité informatique d'une mairie informe l'ANSSI d'un incident concernant le site Internet de sa commune. En effet, le contenu du site Internet a été aspiré et publié sous un autre nom de domaine en .tk. Ce faisant, les attaquants auraient modifié les pages du site cloné et ajouté du contenu pornographique. De plus, des résultats de recherche liés au site Internet de cette commune pointent vers le site malveillant.

Face à cette situation préoccupante, le responsable contacte l'hébergeur du site et obtient le déréférencement du site malveillant en 24 heures par les moteurs de recherche. Il porte également plainte auprès des services de police. La réaction prompte du responsable aura permis de faire cesser cette atteinte à l'image dans de brefs délais.

Exemple 2 : présence d'un mineur de cryptomonnaie sur le site internet d'une commune

En janvier 2018, un agent de l'ANSSI effectue un signalement avisant de la présence d'un cryptomineur* sur une page du site Internet d'une commune. Ce signalement provient du résultat d'un moteur de recherche spécialisé (publicwww) qui indexe le code source des sites Internet. Bien que ce cryptomineur soit disponible en source libre et que son utilisation puisse être légitime, il peut être surprenant d'en faire la découverte sur un site « institutionnel ».
L'ANSSI transmet ce signalement à la commune qui fait le nécessaire pour le supprimer.

Exemple 3 : une attaque par rançongiciel sur le site d'une commune

En juillet 2019, une commune fait part à l'ANSSI de la compromission de son système d'information par un rançongiciel. Les fonctions critiques de la mairie ne sont plus fonctionnelles durant l'incident. Il apparaît que les sauvegardes sont compromises et que leur réinstallation réactive un processus

de chiffrement des données les rendant inexploitables. Cet incident nécessitera une réinstallation complète des machines virtuelles de la commune.

Après analyse, il semble que le système d'information était fragilisé par une politique de mots de passe faibles et une prolifération de comptes avec des privilèges administrateurs non connus des services de la mairie, ce qui a facilité l'attaque via un des comptes administrateur.

Lien vers le guide *Attaques par rançongiciels, tous concernés :* **https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/**

Exemple 4 : typosquattage de noms de domaine d'une métropole

En novembre 2019, les services informatiques d'une métropole informent l'ANSSI de la réservation de plusieurs noms de domaine usurpant son identité. Après des investigations, il s'avère qu'une entreprise étrangère a réservé ces noms de domaine, sans les rendre actifs, prétextant une utilisation professionnelle. L'ANSSI émet des recommandations à l'attention de la métropole suggérant un rapprochement avec l'AFNIC (organisme qui gère les noms de domaine). Une surveillance accrue des noms de domaine similaire est également conseillée.

En effet, la réservation de noms de domaine proches sémantiquement du nom officiel d'une organisation (typosquattage) peut entraîner différents risques pour cette dernière. Ces noms peuvent être utilisés pour envoyer des courriels d'hameçonnage. Profitant de la confiance que peuvent suggérer ces adresses, la propagation de maliciels ou la récupération de données d'identification ou de données personnelles peuvent s'en trouver facilitées, autant envers les agents de la métropole qu'envers les citoyens.

Exemple 5 : exploitation d'une vulnérabilité informatique rendue publique

En décembre 2019, un avis de vulnérabilité (exécution de codes arbitraires à distance) concernant les applicatifs CITRIX a été publié par l'éditeur.
En janvier 2020, une métropole et un département font part à l'ANSSI de la compromission d'équipement CITRIX de leurs systèmes d'information respectifs.

Concernant plus particulièrement la métropole, qui n'avait pas appliqué la solution de contournement proposée par l'éditeur, il a été constaté des modifications dans les tâches planifiées sur son serveur CITRIX ainsi que des connexions sortantes vers un serveur en Russie.

Suite à des échanges avec l'ANSSI, la métropole a pris diverses mesures de remédiation, en appliquant notamment le correctif proposé fin janvier par l'éditeur et en changeant les identifiants du serveur.

Exemple 6 : compromission par un cheval de Troie (type de logiciel malveillant)

En février 2020, une communauté d'agglomération fait part de la compromission d'un poste de travail par le cheval de Troie EMOTET suite à l'ouverture d'une pièce jointe au contenu malveillant.

La communauté d'agglomération a notamment constaté des modifications de fichiers PDF et JSE sur un serveur distant. Deux postes de travail auraient également été compromis par l'ouverture de ces fichiers modifiés par l'attaquant.

Le cheval de Troie EMOTET, initialement utilisé pour dérober des identifiants bancaires, sert également aujourd'hui de première étape d'infection pour nombre de maliciels, parmi lesquels des rançongiciels.

2. Les points de vigilance

Les sites Internet ne doivent pas être l'unique point d'attention, les vulnérabilités sont multiples. Une attention particulière doit notamment être portée sur le wifi public, les capteurs, l'hébergement des données... *(cf. - Quelques bonnes pratiques pour prévenir le risque de malveillance numérique - page 24)*

Sites Internet

- Les sites Internet des collectivités devraient disposer d'une gestion des mots de passe conforme aux bonnes pratiques (mots de passe de qualité).

CYBERSÉCURITÉ : TOUTES LES COMMUNES ET INTERCOMMUNALITÉS SONT CONCERNÉES

- Le socle technique *(système d'exploitation)* des serveurs sur lesquels reposent les sites internet devraient être régulièrement mis à jour.
- Les logiciels de gestion de contenu *(CMS)* sur lesquels reposent les sites internet devraient être régulièrement mis à jour.

Wifi

- Les mots de passe wifi devraient être régulièrement changés.
- Le cloisonnement entre utilisateurs visiteurs et internes devrait toujours être mis en place.
- Les connexions devraient être opérées via un portail captif*.

Capteurs

- Les données de capteurs devraient être envoyées dans une offre d'information « nuagique » européenne.

Cloud

- Les modalités de réversibilité *(récupération des données)* devraient être définies avant la signature du contrat.

Mobiles

- Les équipements mobiles *(tablettes ou ordiphones)* devraient disposer d'un antivirus, si possible administré pour vérifier ses mises à jour.
- Les équipements mobiles devraient être administrés afin de disposer d'un verrouillage/effacement automatique en cas de vol.

Messageries

- Les messageries devraient systématiquement utiliser les versions chiffrées des protocoles d'envoi et de réception.
- Les comptes de messagerie et les adresses de courrier éléctronique des élus et agents quittant la collectivité devraient être supprimés sans délai après leur départ.

Serveurs et postes de travail

- Les sauvegardes et les mises à jours applicatives sont indispensables.

FOCUS

Usages personnels et professionnels

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone, etc.) personnels et professionnels. Très répandues, les pratiques qui mélangent les deux sphères posent des problèmes en matière de sécurité des données : vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur.

Dans ce contexte, il est recommandé de séparer les usages personnels des usages professionnels, à savoir :
• ne pas faire pas suivre les messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
• ne pas héberger de données professionnelles sur les équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne ;
• de la même façon, éviter de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de la commune ou de l'intercommunalité.

Si ces bonnes pratiques ne sont pas appliquées, il y a le risque que des personnes malveillantes volent des informations sensibles de la commune ou de l'intercommunalité, après avoir réussi à prendre le contrôle de la machine personnelle.

https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

(...)

Comment Angers a fait face à sa **première cyber-attaque ?**

Revue L'info cyber-risques - 4ème trimestre 2021

Début 2021, la capitale de l'Anjou subissait une cyber-attaque sans précédents via le rançongiciel Ryuk. Pendant plus d'une semaine, la ville et sa métropole sont retournées au fax et au papier. Une attaque endiguée, qui a forcé cette administration locale à fonctionner en mode dégradé durant plusieurs mois. L'incident a cependant accéléré un plan d'actions visant à renforcer la cybersécurité du SI, engagé juste avant l'attaque.

« *N'ouvrez pas vos ordinateurs ce lundi matin. Une cyber-attaque a eu lieu ce week-end et endommage tout notre système d'information. Tous les documents, applications, messagerie, accès internet ... sont indisponibles. Les équipes de la DSIN ont pris des mesures d'urgence pour éviter une aggravation de la situation. Merci de respecter cette consigne jusqu'à nouvel ordre* ». Ce texte était placardé dans les ascenseurs de l'hôtel de ville d'Angers le lundi 18 janvier 2021 au matin. Environ 48 heures auparavant, la capitale de l'Anjou, connue pour son célèbre château mais aussi ses entreprises d'électronique, venait de subir sa première cyber-attaque de grande ampleur. Un incident qui s'ajoutait à une longue liste de collectivités territoriales françaises prises pour cibles par des cybercriminels, avec également des cas emblématiques comme la région Grand-Est (lire *L'Info Cyber-Risques N°1*), Évreux, Bayonne ou La Rochelle.

Spécificité de l'attaque d'Angers : elle n'a jamais été revendiquée. L'enquête est toujours en cours. Et pour l'heure, la collectivité n'a pas été informée d'une éventuelle piste permettant d'identifier ses attaquants. Il semble qu'Angers soit juste tombée dans les mailles du filet de cybercriminels faisant de « *la pêche au gros* ». Ils n'avaient donc pas ciblé initialement cette administration locale pour la rançonner. Leurs logiciels de ransomware avaient simplement repéré une « *opportunité d'attaque* » sur le SI de la ville et d'Angers Loire Métropole (ALM). « *Il s'agit d'un scénario classique d'intrusion via un identifiant et un mot de passe. Nous ne savons pas comment il a été récupéré, mais il a servi de point d'entrée pour les cyber-attaquants* », résume Jacques Pouvreau, DSI d'Angers Loire Métropole. « *Ils ont ensuite augmenté leurs privilèges pour se déplacer dans le SI et chiffrer des données* ».

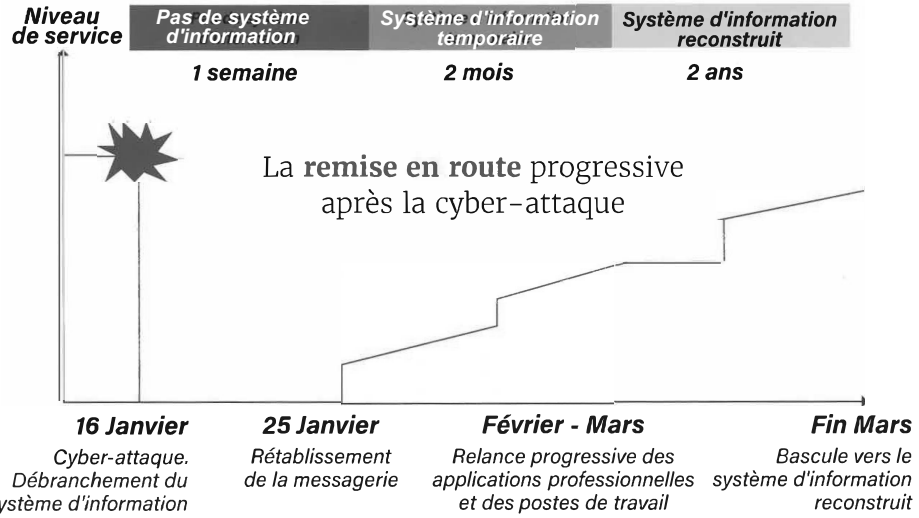
Les premières traces de l'attaque remontent à la nuit du vendredi 15 au samedi 16. Toujours très classiquement, les cybercriminels ont ainsi choisi de lancer l'opération juste avant le week-end, en espérant que les équipes informatiques soient moins réactives qu'en semaine. Ce qui ne fut pas le cas. « *Le samedi matin, les agents d'astreintes de la DSIN (Direction du Système d'Information et du développement numérique) ont été alertés d'un dysfonctionnement des applications de gestion des bibliothèques. Cela nous a conduit à mener immédiatement des investigations. Elles se sont rapidement orientées vers une cyberattaque de type rançongiciel, car nous avons découvert des fichiers chiffrés sur nos serveurs* », poursuit le DSI.

Pour bien comprendre le contexte de l'attaque, rappelons qu'Angers et sa métropole forment un territoire de 29 communes, rassemblant près de 300 000 habitants. Les services administratifs, répartis sur une cinquantaine de gros sites, sont assurés par près de 5000 agents, dont 3000 ont un accès régulier au SI. Les autres sont quotidiennement sur le terrain et n'y accèdent que ponctuellement. Le SI accueille plus de 200 applications métiers, dont la grande majorité est hébergée en local. Microsoft Office 365 est l'un des rares applicatifs à exploiter le cloud. Quant à la DSI, elle est mutualisée depuis 2003 entre la ville et la métropole, et compte une soixantaine d'agents. Le niveau de sécurité du SI lors de l'attaque était « *classique* », mais avec déjà un projet en cours de renforcement de sa protection. « *Depuis la mi-2020 nous avions engagé une démarche pour augmenter notre niveau de cyberprotection. Début 2021, lors de l'attaque, nous avions déjà réalisé le diagnostic, l'analyse de risques et nous travaillions sur le plan d'actions, notamment le déploiement d'un EDR. L'attaque a donc devancé de peu la mise en place des premières mesures* », poursuit-on à la DSI.

« Je n'aurais pas cru qu'on serait amené à réactiver le fax »

Dès le samedi 16 janvier, le RSSI (nommé un an plus tôt) ainsi que les équipes de la DSI décident de prendre des premières actions pour éviter la propagation du rançongiciel. Tous les liens Internet sont coupés. Les routeurs réseaux sont bloqués et les récentes sauvegardes du SI sont isolées. L'ANSSI est prévenue ainsi que le cabinet de conseil Wavestone avec qui Angers travaille déjà sur le renfort du SI. « *L'ANSSI nous a accompagné à distance, via le CERT-FR, et les équipes de Wavestone sont intervenues sur site dès le lundi pour nous aider à analyser et gérer la situation* », souligne Jacques Pouvreau.

Parallèlement, un comité de crise est constitué dès le samedi. Outre les équipes informatiques, il réunit également le maire, Christophe Béchu qui vient lui-même de subir une attaque sur son compte Twitter. Le vendredi, une main tatouée



N'ouvrez pas vos ordinateurs ce lundi matin.

Une cyber-attaque a eu lieu ce week-end et endommage tout notre système d'information.

Tous les documents, applications, messagerie, accès internet... sont indisponibles.

Les équipes de la DSIN ont pris des mesures d'urgence afin d'éviter une aggravation de la situation.

Veillez à respecter cette consigne jusqu'à nouvel ordre.

Lundi 18 janvier, des affiches placardées dans la mairie demandant aux agents de ne pas utiliser leurs ordinateurs.

Christophe Béchu a communiqué sur la cyberattaque auprès du grand public via le média en ligne Brut, ainsi que les réseaux sociaux Twitter et Facebook.

avait ainsi remplacé son portrait sur le réseau social. Les deux incidents ne semblent cependant pas liés.

Concrètement, tous les services de la ville fonctionnent alors en mode dégradé, en travaillant par téléphone, sur Office 365 (via des PC portables déconnectés du SI) et en ressortant les supports papiers. La bibliothèque est ponctuellement fermée le samedi de l'attaque, car sans système de réservation des livres, elle ne pouvait tout simplement plus fonctionner. La police municipale a également vu son système impacté en ne pouvant plus émettre de PV. Le contrôle d'accès des bâtiments communaux était assuré « à la main », c'est-à-dire sans badges. Quant aux sites internet de la ville et de la métropole, ils ont également été mis hors ligne.

Dans une vidéo, postée le 21 janvier sur le média en ligne « Brut », Christophe Béchu explique qu'il n'aurait pas cru que « *l'on serait amené potentiellement à réactiver le fax* ». Et de poursuivre : « *Voilà ce qui nous relie à l'extérieur à l'heure qu'il est* (le fax du premier sous-sol, NDLR). *On avait pourtant eu un débat pour savoir si ça valait le coup de conserver ce fax et puis on s'était dit que l'on ne sait jamais, que ça pouvait toujours servir. Mais je ne pensais pas que l'on en aurait l'usage en ce début d'année 2021 !* » Ce fax sera notamment utilisé durant l'attaque pour envoyer le dépôt de plainte la concernant au procureur de la République.

« *La plupart des services concrets se poursuivent* », a tenu à préciser l'élu. « *On n'a pas arrêté la collecte des ordures ménagères, on continue à alimenter d'eau les robinets des 300 000 habitants de l'agglomération ! En revanche, nous n'avons plus depuis ce week-end la capacité à pouvoir produire de manière normale le suivi de nos missions administratives. En clair, on ne peut pas délivrer par exemple un extrait d'acte de naissance à quelqu'un qui viendrait le chercher en mairie puisque l'on n'allume pas les ordinateurs, donc on n'a pas accès à ces fichiers* », confie également Christophe Béchu dans cette vidéo. Elle fera d'ailleurs office de communication officielle auprès de la population, aux côtés d'informations publiées sur Twitter et sur Facebook.

Pas de traces d'extraction de données

Dès le lundi matin, une communication est diffusée auprès des agents via des affiches et des documents papiers. Les différentes directions métiers sont, quant à elles, tenues informées via WhatsApp. En complément du comité de crise, dédiée plutôt à la stratégie de gestion de crise, une cellule plus décisionnelle est créée. Dédiée au pilotage des actions, elle intègre notamment la DRH, la direction de la Communication, le DSI et le RSSI. Une troisième cellule, cette fois spécifique à la DSIN, vient également compléter le dispositif pour la partie opérationnelle.

Les premières investigations montrent que les cybercriminels ont réussi à chiffrer des données hébergées sur les serveurs Windows et sur 200 postes de travail avant que le SI ne soit déconnecté. Si des données ont bien été chiffrées, « *nous n'avons pas identifié de traces d'extractions de données* », poursuit Jacques Pouvreau. Aucune demande de rançon n'a non plus été envoyée. « *Les cybercriminels nous ont simplement adressé une demande de prise de contact en ligne, que nous avons bien entendu ignorée* ».

Ces premières analyses permettent d'identifier le ransomware utilisé pour l'attaque qui n'est autre que Ryuk. En octobre 2020, Ryuk avait déjà été exploité dans le cadre de la cyberattaque visant Sopra Steria (lire *L'Info Cyber-Risques* N°2). Pour rappel ce rançongiciel a servi, depuis 2018, à mener plusieurs campagnes d'attaques, dont la plus importante a pris pour cible la chaîne d'hôpitaux américaine Universal Health Services (UHS), en septembre 2020. Selon sa fiche ANSSI, il génère pour chaque fichier ciblé une clé de 128 bits et chiffre son contenu en AES avec le mode CTR. C'est un des rançongiciels les plus utilisés par les cybercriminels. D'après un classement du FBI, paru en mars 2020, Ryuk serait ainsi le ransomware le plus lucratif pour les cyberattaquants avec 61 millions de dollars rançonnés rien qu'entre février 2018 et octobre 2019.

Deux mois de mode dégradé

Durant la première semaine suivant l'attaque, le blocage du SI a été complet. Les sauvegardes ayant été déconnectées, et leur fiabilité validée, une réouverture progressive des services est intervenue durant les semaines suivantes. Mais globalement la plupart des services sont restés dégradés durant environ deux mois.

Le SIRH a été l'un des premiers services à être relancés. « *L'attaque est survenue en milieu de mois, juste quand la paye était en cours de traitement* », indique la DSI. Le site internet a également été de nouveau mis en ligne mais en restant déconnecté du SI et avec seulement une partie de ses fonctions d'e-administration. Les autres services (finances, scolaire, état civil, vidéosécurité ...) ont été réactivés très progressivement. En avril dernier, près de 70% des applications étaient de nouveau accessibles. « *En cette fin d'année, il n'y a pas de retour complet à la normale, même si nous avons récupéré plus de 90% des applications métiers. Ceci car nous en profitons pour revoir notre plan d'actions de cyberprotection. Par exemple, le portail « A'tout », dédié à la vie quotidienne des habitants (bibliothèque, transport..), ne sera de nouveau en ligne que prochainement, mais avec une cybersécurité renforcée* ». La DSI table sur un retour complet à la normale début 2022.

« Le poids de l'informatique dans la vie quotidienne des services publics n'a cessé d'augmenter. »

Christophe Béchu, maire d'Angers.

Un impact considérable

Jacques Pouvreau préfère ne pas détailler l'ensemble des mesures prises pour renforcer le SI. Il évoque cependant la mise en place d'un EDR managé, d'un SOC et une segmentation améliorée du réseau. Les agents vont également être formés aux bonnes pratiques de cybersécurité. « *Il faut une approche globale, à la fois technique et humaine, sans oublier la nécessité de prévoir un plan de gestion d'incident au cas où ce type d'attaque survienne. La meilleure parade reste l'anticipation* », estime Jacques Pouvreau.

Cette attaque sans précédent pour la ville et sa métropole a clairement laissé des traces dans les esprits, confie la DSI. Mais il n'y a pas que du négatif. « *L'attaque a éveillé les consciences et a notamment accéléré la mise en place des actions de cybersécurité que nous avions prévues. Nous avons également démontré notre capacité à réagir à une attaque de grande ampleur grâce à la mobilisation de nos équipes, à celle de nos partenaires, et au soutien de nos élus. Christophe Béchu a ainsi soutenu la DSI durant toute la crise et c'est toujours le cas aujourd'hui* », tient à souligner Jacques Pouvreau.

Le coût financier de l'incident n'a pas encore été déterminé. Mais il devrait se chiffrer en plusieurs centaines de milliers d'euros, principalement à cause des pertes de productivité. En termes d'image pour la collectivité territoriale, les conséquences restent difficiles à évaluer. « *Nous avons largement communiqué auprès des Angevins et tenté, autant que cela était possible, de compenser les blocages informatiques par de l'humain* », souligne la DSI.

Reste que l'attaque est survenue alors qu'Angers s'est engagée dans un vaste projet de territoire connecté. De par son ampleur, il s'agit même du plus large projet de Smart city français.

Doté d'un budget de plus de 120 millions d'euros, il vise notamment à réduire la consommation énergétique du territoire (éclairage passé au LED, chauffage intelligent, arrosage optimisé des espaces verts ...). Il doit également « *améliorer la qualité de vie des habitants* » en proposant des services de Smart parking (guidage vers des places de stationnement disponibles), un renfort de la vidéoprotection (outils d'analyse d'images), une gestion intelligente de la régulation du trafic routier, *etc.* Des services qui seront connectés à un « hyperviseur », plateforme capable de gérer tous les systèmes de manière centralisée. La cyberattaque a-t-elle mis à mal ce projet de premier ordre pour le territoire ? « *Elle ne l'a pas interrompu mais l'a complexifié. Nous avons bien entendu accentué l'attention portée à la dimension cybersécurité du projet* », indique Jacques Pouvreau.

Dans sa vidéo publiée sur Brut, Christophe Béchu salue les apports de l'IT dans la gestion des administrations locales. Mais il en souligne aussi les limites. « *Le poids de l'informatique dans la vie quotidienne des services publics n'a cessé d'augmenter, et on nous encourage à le faire. [...] On s'est beaucoup plus concentré sur le fait d'augmenter les services que l'on offrait à la population via le numérique, qu'au fait de protéger l'architecture de ces systèmes. Cela ne veut pas dire que l'on n'a rien fait. Cela veut dire que l'on n'a pas mis assez d'intensité et assez d'efforts là-dessus* », conclut l'élu.

CHRISTOPHE GUILLEMIN