Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL
DE PROMOTION INTERNE ET D'AVANCEMENT DE GRADE
DE TECHNICIEN PRINCIPAL TERRITORIAL DE 2ème CLASSE

SESSION 2023

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS OPÉRATIONNELLES

ÉPREUVE D'ADMISSIBILITÉ :

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION

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 29 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.

S'il est incomplet, en avertir le surveillant.

Vous êtes technicien principal territorial de 2ème classe, en poste en qualité de responsable sécurité des systèmes d'information (R.S.S.I.), en charge de la direction informatique de la commune de Techniville (10 000 habitants).

Des communes voisines ont récemment été victimes de cyberattaques. Dans ce contexte, les élus sont préoccupés par l'étendue des menaces actuelles et souhaitent renforcer la sécurité informatique de la collectivité.

Dans un premier temps, la directrice générale des services (D.G.S.) vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur les cyberattaques.

10 points

Dans un deuxième temps, elle vous demande d'établir un ensemble de propositions opérationnelles visant à se prémunir de celles-ci.

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances

10 points

Liste des documents :

Document 1 : Comment lutter contre les cyberattaques ? - Zuzana - *logpoint.com* - novembre 2020 - 4 pages.

Document 2 : Cyberattaques : comment se prémunir du pire - Olivier Devillers - *mairesdefrance.com* - septembre 2021 - 3 pages.

Document 3 : Comment se prémunir d'une cyberattaque ? - g*ouvernement.fr* - mars 2022 - 2 pages.

Document 4 : Cybersécurité : les collectivités qui montrent l'exemple - *weka.fr* - juin 2021 - 2 pages.

Document 5 : Les régions, soutenues par l'Anssi, déploient des centres régionaux de réponse aux incidents cyber - *francenum.gouv.fr* - juin 2022 - 1 page.

Document 6 : Former et sensibiliser les agents à la sécurité informatique pour réduire les risques - Pierre Alexandre Conte - *lagazettedescommunes.com* - septembre 2016 - 2 pages.

Document 7 : Cyberattaque au Département de Seine-et-Marne : Le point sur la situation - *seine-et-marne.fr* - novembre 2022 - 3 pages.

Document 8 : Cyberattaques dans les hôpitaux : « Le paiement de rançon n'est pas une solution, sinon, ça devient le Far West » - Julien Lemaignen et Manon Romain - *leMonde.fr* - décembre 2022 - 3 pages.

Document 9 : Pour sécuriser les petites communes, faut-il mutualiser les RSSI ? - Louis Adam - *zdnet.fr* - juin 2021 - 2 pages.

Document 10 : Cybercriminalité : « Nous ne voulons plus qu'un élu nous dise qu'il ne savait pas » - Hélène Lerivrain - *lagazettedescommunes.com* - décembre 2021 - 2 pages.

Document 11 : Cyberattaques : la négligence des collectivités pourrait leur coûter cher - Lucas Boncourt - *banquedesterritoires.fr* - juillet 2022 - 2 pages.

Dans le cadre de sa politique environnementale, la cellule pédagogique nationale privilégie des impressions en noir et blanc. Les détails non perceptibles du fait de ce choix reprographique ne sont pas nécessaires à la compréhension du sujet, et n'empêchent passon traitement.

DOCUMENT 1

Comment lutter contre les cyberattaques ?

Zuzana - *logpoint.com* - novembre 2020.

Quiconque entreprend une activité en ligne doit être conscient qu'il s'expose à une cyberattaque potentielle. Ce risque peut s'avérer particulièrement néfaste pour les entreprises car les enjeux sont plus importants, comme par exemple la sécurité de leurs clients. Découvrir l'univers des cyberattaques de manière approfondie, notamment ce qu'elles sont et comment les prévenir, peut considérablement améliorer votre sécurité en ligne.

Qu'est-ce qu'une cyberattaque ?

Une cyberattaque désigne toute action entreprise par des cybercriminels avec à l'esprit des objectifs malveillants. Les cybercriminels lancent leurs attaques en utilisant un ou plusieurs ordinateurs afin de frapper d'autres ordinateurs, réseaux ou systèmes d'information.

Diverses méthodes peuvent être utilisées pour lancer une cyberattaque, mais les objectifs sont généralement de :

- Voler des données.
- Détruire des informations ou des données.
- Modifier des données.
- Désactiver des ordinateurs.
- Obtenir un gain financier.
- Espionner.

Pourquoi les cyberattaques se produisent-elles ?

Les cyberattaques sont généralement motivées par des objectifs criminels ou politiques.
Les adversaires peuvent être une personne privée, un acteur étatique ou une organisation criminelle. Mais la principale réponse à la question concernant la raison pour laquelle ces attaques se produisent est de regarder les objectifs se cachant derrière chacune d'entre elles. Les cybercriminels ne veulent pas toujours la même chose, c'est pourquoi il n'existe pas une réponse simple à cette question.

Certains cybercriminels veulent de l'argent ou des informations, tandis que d'autres cherchent simplement à causer des problèmes. Ensuite, il y a ceux qui attaquent les systèmes dans le but de les détruire pour des raisons personnelles, comme c'est le cas parfois d'anciens employés mécontents.

Les types de cyberattaques les plus courantes

Il existe de nombreux types de cyberattaques, mais certaines actions malveillantes sont plus courantes que d'autres. Les actions malveillantes les plus courantes incluent divers types de malwares, de ransomwares, de déni de service et de phishing.

Attaques actives / passives

Avant d'explorer les types d'attaques de cybersécurité spécifiques, il faut prendre en compte les deux principales catégories, passive et active. Les attaques passives n'affecteront pas les ressources du système et viseront plutôt la découverte d'informations.
En revanche, les attaques actives cherchent à avoir un impact sur la vie privée, l'intégrité ou la disponibilité d'un système.

Cryptojacking

Ce type de cyberattaque survient lorsqu'un cybercriminel utilise l'ordinateur de la victime pour miner de la cryptomonnaie.

Ce type d'attaque est mis en oeuvre généralement via des malwares de cryptomining ou par le biais de code JavaScript via des navigateurs Web.

Déni de Service Distribué (DDoS)

Les attaques DDoS (Distributed Denial of Service) se produisent lorsque des pirates tentent d'empêcher l'accès à un site Web ou à un serveur.

Pour atteindre cet objectif, les cybercriminels utilisent de nombreux systèmes et surchargent le système ciblé, le rendant ainsi indisponible pour les véritables utilisateurs.

Man in the middle

Dans ce type de cyberattaque, le cybercriminel se place entre le service Web et l'utilisateur.
Un exemple serait un attaquant créant une page de connexion Wi-Fi au niveau d'un réseau public pour imiter le vrai. Une fois que la victime s'est connectée, le cybercriminel peut avoir accès aux informations qu'il saisit, notamment les mots de passe importants.

Phishing

Le phishing est un type courant d'attaque de cybersécurité. Cette technique implique généralement l'envoi d'emails qui semblent authentiques mais qui proviennent en réalité de cybercriminels, demandant généralement des données personnelles.

Malheureusement, même si les filtres anti-spam progressent, les cybercriminels continuent de développer des moyens de les contourner.

Ransomware

Le ransomware est un type de malware ou d'attaque syntaxique qui chiffre les fichiers présents sur l'appareil ciblé. Ensuite, les cybercriminels demandent de l'argent en échange du déchiffrement des fichiers.

Attaque de la Supply chain

Les attaques de la chaîne d'approvisionnement logiciel sont un type de cyberattaque qui compromet le code d'un logiciel commun, dans le but de fournir aux attaquants un accès aux applications installées par les utilisateurs. C'est le résultat d'une autre attaque ciblant l'éditeur du logiciel et débouchant sur une attaque syntaxique.

Certaines de ces cyberattaques ont pour objectif de toucher le maximum de victimes.
L'attaque PrismWeb, qui a touché plus de 200 boutiques en ligne au niveau des campus universitaires, en est un bon exemple.

Ce type de cyberattaque peut également viser des cibles spécifiques. Dans ce cas, les cybercriminels ont une cible et choisissent un programme ou un logiciel qui peut leur donner un accès. Les cybercriminels peuvent aussi profiter d'autres personnes également touchées par cette attaque, en fonction de leurs objectifs.

Injection SQL

Le nom de cette attaque vient de l'utilisation des commandes SQL. SQL est une abréviation de Structured Query Language, et lorsque vous utilisez une injection SQL comme moyen de lancer une cyberattaque, vous essayez de prendre le contrôle d'une base de données et éventuellement de la voler. En insérant un code malveillant dans une base de données, les cybercriminels exploitent les vulnérabilités des applications basées sur les données à partir desquelles ils ont accès à des données sensibles.

Attaques syntaxiques ou malwares

Les attaques syntaxiques font référence à des malwares comme les chevaux de Troie (trojans), les vers (worms) et les virus qui infectent un ordinateur. Les virus s'auto-répliquent et s'attachent à d'autres fichiers. Les vers sont similaires mais ne reposent pas sur un autre fichier, car ils s'exécutent automatiquement. Les chevaux de Troie introduisent des malwares sur les appareils en se faisant passer pour des logiciels légitimes, comme un enregistreur de frappe par exemple.

Exploits zero-day

Ces cyberattaques font référence au moment où les attaquants exploitent les vulnérabilités des logiciels que les développeurs n'ont pas encore corrigées.

Exemples de cyberattaques

Pour montrer la gravité des attaques de cybersécurité, il est bon de se remémorer certaines cyberattaques ayant eu lieu ces dernières années.

Attaque par déni de service Mafiaboy en 2000

Le 7 février 2000, l'une des premières attaques DDoS à faire la Une des journaux vient d'avoir lieu. L'attaque a été lancée par un pirate âgé de 15 ans et se faisant appeler « Mafiaboy », qui a réussi à réduire le trafic sur eBay, CNN, Amazon, Buy.com et d'autres sites importants. Le FBI a estimé que les sites affectés avaient subi un préjudice d'environ 1,7 milliard de dollars.

WannaCry en 2017

Cette attaque de ransomware chiffre les ordinateurs, exigeant ensuite des Bitcoins pour déverrouiller les fichiers. Il a ciblé des organisations critiques telles que le NHS au Royaume-Uni. La particularité de cette faille, qui la rend critique, était qu'elle se propageait via une vulnérabilité dans Windows découverte par la NSA (National Security Agency) américaine. Les cybercriminels ont utilisé cette vulnérabilité pour orchestrer cette attaque dévastatrice.

NotPetya en 2017

Petya désignait une attaque de ransomware similaire à d'autres attaques en 2016, mais en juin 2017, elle a été utilisée plus massivement avec une nouvelle version, appelée NotPetya. Elle a utilisé le même exploit que WannaCry.

Faille Citrix en 2019

En mars 2019, Citrix a été victime d'une attaque de type 'password spraying'. Ce type d'attaque désigne des pirates qui tentent d'obtenir un accès en exploitant des mots de passe faibles.

La faille de Capital en 2019

En juillet 2019, Capital One a découvert que des centaines de milliers de cartes de crédit avaient été compromises, incluant notamment une fuite de numéros de sécurité sociale et de dates de naissance. Curieusement, il n'existe aucune preuve que les informations et les données concernées aient été utilisées à des fins frauduleuses ou même partagées par l'attaquant qui avait obtenu l'accès.

Conseils de cybersécurité pour vous protéger contre les cyberattaques

La bonne nouvelle est que si les cyberattaques représentent un risque important, il existe également de nombreuses stratégies pour s'en protéger. En apprenant ce qu'est une cyberattaque

et les méthodes et tactiques les plus couramment utilisées, vous pourrez prendre les précautions appropriées.

Sauvegarde des données : les sauvegardes peuvent aider dans plusieurs situations. Elles minimiseront les dommages causés si un cybercriminel supprime ou modifie les données de votre système et atténuera les effets d'une attaque de ransomware.

Contrôle de l'accès au système : vous pouvez également réduire le risque de cyberattaques en faisant preuve de rigueur au niveau de l'accès au système, notamment en révoquant l'accès dès qu'une personne quitte l'entreprise et en mettant en place un contrôle d'accès strict basé sur les rôles. Une telle précaution empêchera d'anciens employés mécontents d'agir de manière malveillante en vous assurant que seules les bonnes personnes disposent des autorisations appropriées.

Obtenez une assistance professionnelle : il est important d'être en mesure de se tenir au courant des dernières menaces et stratégies de cybersécurité afin de détecter rapidement les attaques. Cette détection peut être mise en oeuvre grâce à un outil de surveillance de la sécurité tel qu'une solution SIEM.

Authentification multifacteur : l'utilisation de l'authentification multifacteur permet d'empêcher les pirates d'accéder à votre réseau ou à vos appareils s'ils ont réussi à mettre la main sur vos mots de passe. Cette précaution est particulièrement importante pour les entreprises, au niveau desquelles un risque élevé de phishing par emails existe.

Sensibilisez et formez aux employés : assurez-vous que vos employés soient conscients de l'importance de la cybersécurité et de la manière d'éviter les cyberattaques, notamment les risques liés aux malwares et au phishing.

Mettre à jour les systèmes : quel que soit le système ou le programme que vous utilisez, il doit toujours être mis à jour. Cette précaution vous permettra de tirer parti des derniers correctifs de sécurité qui traiteront les vulnérabilités connues.

Utilisez des pare-feu et un antivirus : tous les appareils connectés au réseau de votre entreprise doivent disposer d'un logiciel antivirus et d'un pare-feu opérationnels. Cette précaution offrira une couche de protection supplémentaire en détectant les malwares et en atténuant les autres risques.

DOCUMENT 2

Cyberattaques : comment se prémunir du pire

Olivier Devillers - *mairesdefrance.com* - septembre 2021.

Si le nombre précis de collectivités victimes de cyberattaques est inconnu de l'Agence nationale de la sécurité des systèmes d'information (Anssi), les quelques chiffres disponibles indiquent qu'ils «explosent » : 192 attaques par rançongiciels ont été notifiées à l'Anssi en 2020, soit un nombre multiplié par quatre par rapport à 2019 avec, pour premières victimes, des hôpitaux publics et des collectivités.

Les plus petites parmi ces dernières ne sont pas épargnées par un phénomène qui prend un caractère «industriel », touchant absolument tout le monde, comme le relève le rapport annuel de l'agence.

Identifier les risques

Parmi les attaques particulièrement dommageables pour les communes, on mentionnera tout d'abord la fraude à l'identité. Le groupement d'intérêt public (GIP) Cybermalveillance mentionne le cas d'un maire dont l'adresse Gmail a été piratée. À partir de ce compte de messagerie, le criminel a pu contacter tout le carnet d'adresses de l'élu pour solliciter un don invoquant la crise du Covid-19. Mais le RIB joint était bien évidemment celui du criminel.

Autre exemple cité : un mail se faisant passer pour un prestataire de la collectivité sollicitant le paiement d'une facture prétendument impayée. Ce type d'attaque a des conséquences financières réelles mais peut être contré par un logiciel de filtrage et des actions de sensibilisation au risque d'« hameçonnage ».

Rançongiciels

Les attaques par rançongiciel sont beaucoup plus destructrices. Ces cryptovirus paralysent totalement le fonctionnement de la commune en empêchant l'accès à l'informatique. Tous les fichiers sont cryptés par une clé que les pirates cherchent à monnayer selon un montant calculé en fonction des moyens financiers de la collectivité. «Une rançon qu'il ne faut payer en aucun cas », rappelle l'Anssi car «leur paiement encourage les attaques sans pour autant garantir que la collectivité retrouvera ses données et ne sera pas à nouveau attaquée. »

Ces rançongiciels, comme le rappelle Cybermalveillance (lire l'avis d'expert ci-contre) peuvent paralyser durablement les services à la population (état civil, affaires scolaires, cimetières…), le fonctionnement des services (retards dans le paiement des agents, dossiers à l'arrêt) et l'encaissement de recettes (stationnement, marchés, cantines…).

Colmater les failles
Contrairement à une idée reçue, ces attaques ne sont que rarement liées à un clic malencontreux sur un courriel ou sur sa pièce jointe. Dans 80 % des cas, selon Cybermalveillance, les pirates exploitent des failles du système d'information – ordinateurs, logiciels, équipements réseaux ou serveurs… –, et les humains qui peuvent aussi être manipulés ! Ces failles sont «autant de portes » vers les données et les infrastructures numériques de la collectivité. Colmater ces failles de sécurité des logiciels passe par la mise à jour des applications, sans oublier celles du site internet, de l'imprimante ou les applications installées sur les smartphones.

Droits restreints de paramétrage des ordinateurs et logiciels
Par ailleurs, les droits d'administration pour paramétrer un ordinateur ou un logiciel doivent être restreints. De même, la signature électronique du maire ne doit pas être utilisée par plusieurs personnes. Le mélange des activités professionnelles et personnelles doit être également limité. On ne peut ainsi qu'inciter les communes à se doter d'un nom de domaine et d'un compte de messagerie officiel (mairie-nom-de-la-commune.fr) pour faciliter cette séparation des usages.

Enfin, des règles doivent être imposées sur les mots de passe. Ceux-ci doivent faire au minimum huit caractères, utiliser des lettres, des chiffres et des caractères spéciaux. Ils doivent surtout être spécifiques à un seul usage, ne jamais être affichés ou partagés, et être renouvelés régulièrement. Toutes ces règles peuvent être transcrites dans une charte informatique et se traduire par des actions de sensibilisation.

Multiplier les sauvegardes
La sauvegarde des données et logiciels de la collectivité est stratégique car c'est elle (et sa récence) qui déterminera le temps nécessaire à la restauration du système d'information en cas d'attaque par rançongiciel. Au Grand Cognac (Charente, 56 communes) par exemple, il a fallu que la collectivité aille rechercher des pièces jointes à des mails pour reconstituer des dossiers cryptés… Ces sauvegardes doivent être multiples, en ligne (cloud) et hors ligne.

« Désormais, explique l'Anssi, les cyberattaquants cherchent à repérer les sauvegardes avant de lancer leur attaque. » Le syndicat Seine-et-Marne numérique, comme l'agglomération de La Rochelle (Charente-Maritime, 28 communes), tous deux victimes d'un rançongiciel en 2020, ont décidé de ressortir la sauvegarde sur bande, plus difficile d'accès pour un hacker. Les collectivités pouvant aussi être victimes de vol ou d'incendie dans leurs locaux, une sauvegarde en dehors de la mairie est vivement recommandée.

Se faire accompagner
Si quelques règles «d'hygiène informatique » peuvent aider les communes à éviter le pire, la sécurité des systèmes d'information doit être planifiée et pilotée dans la durée. Cela pose bien évidemment la question des moyens, financiers comme humains.

260 collectivités étaient accompagnées, en juin 2021, par l'Anssi pour un «parcours cyber ». Il s'agit de les aider à identifier les failles de leur système d'information et à établir un plan d'action.

Bien que de plus en plus dépendantes du numérique, la majorité des petites communes n'ont pas de responsable informatique.

Mutualisation des expertises
Elles peuvent cependant s'appuyer sur une structure de mutualisation (syndicat informatique) proposant une expertise cyber et des solutions mutualisées comme en Charente-Maritime (Soluris), dans les Landes (Alpi) ou encore dans l'Oise (Adico). La commune de Longueil-Sainte-Marie (Oise) a, par exemple, été accompagnée en 2020 par l'Association pour le développement et l'innovation numérique des collectivités (Adico) pour cartographier son système d'information, évaluer les risques et établir un plan d'action.

Appui de la plateforme Cybermalveillance
Que faire là où ces appuis locaux font défaut ? Les communes peuvent s'adresser à la plateforme « cybermalveillance ». Celle-ci propose des guides, un outil de diagnostic en cas de cyberattaque

et une liste de prestataires de confiance. Des relais de terrain sont par ailleurs en cours de mise en place sous l'impulsion de l'État. Tout d'abord, des centres réponse aux incidents informatiques vont voir le jour en 2022 sous la houlette des conseils régionaux et de l'Anssi, pour mettre en place un accompagnement local, ciblant entreprises et collectivités.

Commandement Cyber de la gendarmerie nationale
Par ailleurs, le commandement Cyber de la gendarmerie nationale va être mobilisé pour aider les petites communes à prendre conscience des risques. Et en cas d'attaques, ces quelque 7 000 gendarmes spécialisés aideront les communes à prévenir les autorités – notamment l'Anssi et la Cnil, en cas de fuite de données personnelles – et à porter plainte. Car pour mettre fin au fléau des cyberattaques, il est essentiel que les forces de l'ordre puissent enquêter.

60 millions d'euros affectés à la cybersécurité

Le plan de relance a dévolu 60 millions d'euros à la sécurisation des collectivités, notamment pour financer des «parcours cybersécurité ». Ces aides sont cependant réservées aux (grandes) collectivités dotées d'un responsable de la sécurité des systèmes d'information (RSSI). Ceux-ci peuvent cependant être mutualisés au niveau d'un EPCI. En parallèle, des appels à projets ont été lancés pour faire émerger des solutions cybermutualisées.

JEAN-JACQUES LATOUR, RESPONSABLE DE L'EXPERTISE DU DISPOSITIF CYBERMALVEILLANCE.GOUV.FR

« Il faut anticiper les risques »
« J'ai pu entendre des collectivités dire : "Nous sommes une petite structure, un servicepublic et nous ne nous sentons pas menacés." C'est une grave erreur car la question n'est pas de savoir si la collectivité va subir une attaque informatique mais quand ! Il est donc urgent de s'y préparer car les conséquences peuvent être très graves.

Les services publics peuvent être paralysés pendant plusieurs semaines. La collectivité peut subir un manque à gagner en étant incapable d'encaisser des recettes dépendant d'installations informatiques. Elle peut également être sanctionnée au titre du RGPD pour avoir failli à protéger les données confidentielles de ses administrés. La responsabilité personnelle des élus peut enfin être engagée.

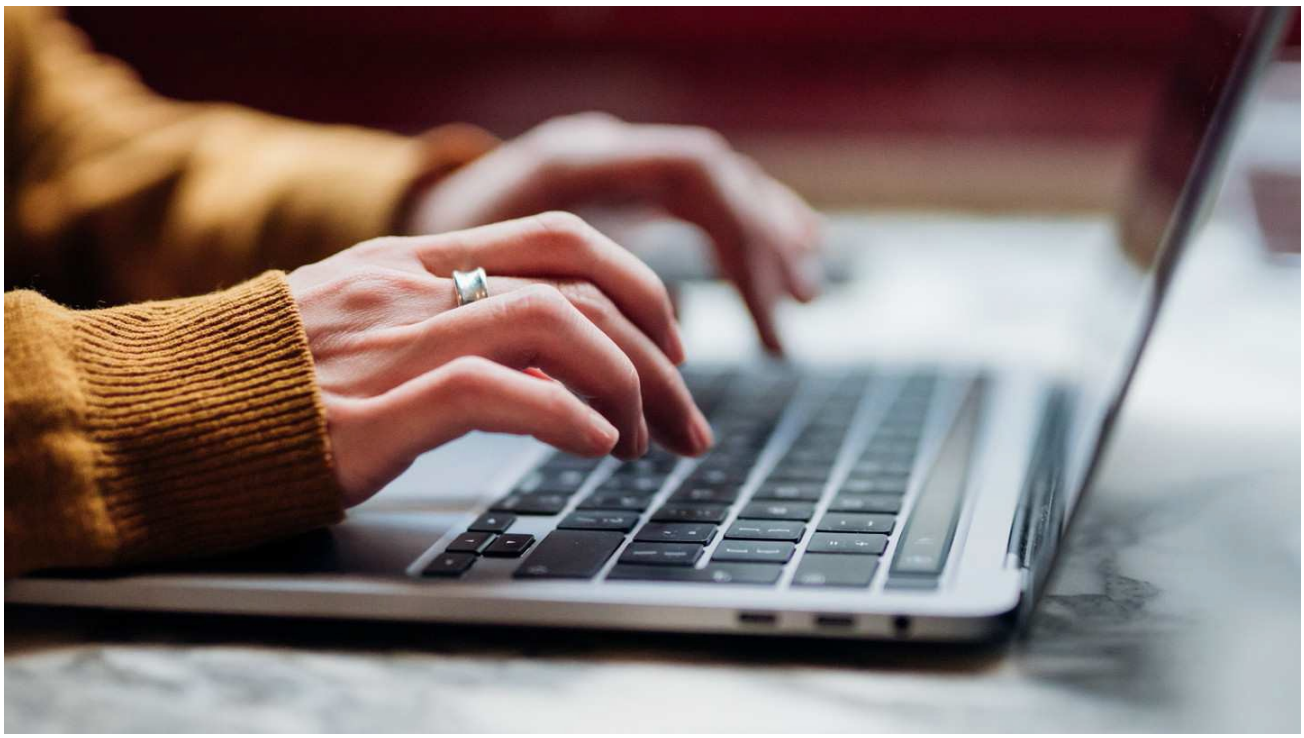
Trop souvent, les investissements en matière de sécurité sont réalisés à l'issue d'une cyberattaque. Leur coût est alors beaucoup plus élevé que s'ils avaient été anticipés. Un audit du système d'information – par un prestataire spécialisé référencé sur Cybermalveillance – pourra aider à repérer les principales failles et à les colmater.

Nous sommes là pour les aider à promouvoir les règles de base de l'hygiène informatique qui permettront aux élus d'éviter des attaques. Nous leur apportons aussi un premier niveau d'assistance quand les attaques se produisent. »

DOCUMENT 3

Comment se prémunir d'une cyberattaque ?

Gouvernement.fr - mars 2022.



Depuis quelques années, les cyberattaques se multiplient, en particulier en temps de crise, qu'elle soit sanitaire ou sécuritaire. L'occasion de faire le point sur les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour vous protéger en ligne.

Vous recevez un courriel estampillé Trésor public vous demandant de fournir vos coordonnées bancaires pour procéder à un remboursement ?

Un service de transport vous demande par *sms* de cliquer sur un lien pour régler les taxes douanières d'un colis ?

Vous recevez un courriel de la part de la gendarmerie nationale vous accusant d'un délit et vous demandant de répondre sous peine de poursuites ?

Soyez vigilant : les demandes adressées de manière autoritaire ou intimidante, par courriel ou par *SMS*, dissimulent parfois des tentatives d'arnaques.

L'un des premiers réflexes consiste à définir des mots de passe robustes, à la fois difficiles à trouver par un système automatisé et à deviner pour une tierce personne.

Privilégiez des **mots de passe longs, complexes et composés de différents types de caractères** (des chiffres, des lettres majuscules, des lettres minuscules et des caractères spéciaux).

Préservez votre identité numérique en vous **montrant vigilant en ligne et sur les réseaux sociaux** : prenez soin de vos données personnelles et ne communiquez pas vos informations sensibles (numéro de téléphone, adresse ou numéro de carte bleue).

Si vous recevez un message d'une personne que vous connaissez bien, mais que le **contenu est étonnant** (un titre en anglais ou dans une autre langue, une demande inhabituelle), faites preuve de prudence !

Vous devez garder en mémoire que **l'identité de l'expéditeur peut être usurpée**. Soyez attentif à tout indice mettant en doute l'origine réelle d'un courriel : incohérence de forme ou de fond entre le message reçu et ceux que votre interlocuteur légitime vous envoie habituellement.

Dans le même sens, ne répondez pas aux demandes suspectes d'expéditeurs inconnus.

Les demandes d'informations confidentielles sont rarement faites par courriel. Soyez donc attentifs à ces tentatives dites d'hameçonnage, aussi appelées *phishing*. Par exemple, le règlement de vos impôts passe uniquement par votre profil de contribuable sur le site impots.gouv.fr : le Trésor public ne vous demandera jamais vos coordonnées bancaires par courriel.

Assurez-vous également qu'en passant la souris au-dessus du lien proposé, **l'adresse du site soit conforme à l'expéditeur annoncé**. Souvent, le contenu des sites frauduleux comporte des fautes de français, mais de plus en plus, les tentatives d'hameçonnage emploient un français correct.

Enfin, **soyez vigilant avant d'ouvrir les pièces jointes**. Elles constituent le principal vecteur d'attaque et peuvent véhiculer des programmes malveillants.

Les hackers ciblent les ordinateurs utilisant des logiciels qui ne sont pas à jour pour exploiter les vulnérabilités non corrigées.

Évitez aussi les réseaux publics ou inconnus. Privilégiez la connexion de votreabonnement téléphonique (3G ou 4G) lorsque vous êtes en déplacement.

Les réseaux wi-fi publics sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles (mots de passe, numéro de carte bancaire...).

Si vous n'avez d'autre choix que d'utiliser un wi-fi public, veillez à ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).

Enfin, il faut penser à **sauvegarder vos fichiers régulièrement sur un support externe à votre équipement** (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée. En cas de piratage de votre ordinateur, vous risquez de perdre des données (photos, fichiers, contacts, messages…).

Si vous êtes victime d'une cyberattaque Prévenez vos contacts, changez vos mots de passe, obtenez de l'assistance auprès de cybermalveillance.gouv.fr, déposez plainte.

DOCUMENT 4

Cybersécurité : les collectivités qui montrent l'exemple

weka.fr - juin 2021.

De plus en plus souvent ciblées par les pirates informatiques (hackers), surtout depuis la crise sanitaire, les collectivités doivent prendre en compte la cybersécurité en amont, sans attendre qu'une attaque se produise. Avec, au-delà du coût, des conséquences désastreuses : interruption du service rendu, atteinte à l'image de la collectivité, piratage de données…

Trois collectivités sur dix auraient été victimes d'un rançongiciel ou ransomware (demande de rançon) en 2019, selon une étude 2020 du Clusif. Année où plus de 1 200 collectivités ont demandé de l'aide au GIP Cybermalveillance.gouv.fr, qui accompagne les victimes et leur fournit un diagnostic personnalisé. Les collectivités subissent également des piratages de comptes en ligne, du hameçonnage (vol de données personnelles ou d'informations sensibles) ou encore du déni de service.

Les tendances observées en 2019 se sont confirmées en 2020*. L'année a été marquée par une recrudescence des attaques par rançongiciels. Le nombre de signalements liés à des rançongiciels a été multiplié par quatre par rapport à l'année 2019. Les victimes de rançongiciels sont principalement des collectivités territoriales, des établissements de santé et des entreprises du secteur de l'industrie.

Cybermalveillance.gouv.fr leur propose des outils pour apprendre à renforcer la sécurité informatique des systèmes d'information (SI) et à inculquer aux agents et aux élus des comportements moins risqués. Son site rapporte aussi des témoignages d'élus très instructifs.

Ainsi, Longueil-Sainte-Marie (Oise, 1 924 habitants) a tout d'abord vérifié le niveau de sécurité de son SI. Accompagnée par l'Association pour le développement et l'innovation numérique des collectivités (Adico), la commune a préparé un dossier d'homologation au RGS (référentiel général de sécurité), ce qui l'a conduite à effectuer une analyse de risques globale du SI pour définir un plan d'action – de la sensibilisation essentiellement.

Des faux mails d'hameçonnage devraient être envoyés aux agents et aux élus, dans le but d'accroître leur vigilance. À Vannes (Morbihan, 55 411 habitants), qui a lancé une telle campagne de faux mails sans information préalable, 23 % des agents ont manqué de vigilance et cliqué… Après une formation en ligne sur les pièges des mails malveillants, le taux de clics est passé à 6 % en un an.

La Rochelle (Charente-Maritime, 171 811 habitants) prépare pour les utilisateurs des SI de la ville et de la communauté d'agglomération (élus, agents, personnel non permanent…), une charte comportant les valeurs à protéger : disponibilité et qualité du service public, respect des obligations légales, confidentialité et intégrité des données sensibles… Les nouveaux arrivants devraient bénéficier d'un parcours de sensibilisation d'une demi-journée.

Outre des informations très pratiques (Où stocker les données pour qu'elles soient sauvegardées ? Pourquoi éteindre ses équipements le soir ? Comment déclarer un incident ?), ils recevront des conseils sur la gestion des mots de passe, les mails malveillants, les usages pro-perso, la protection de la vie privée… Les agents traitant des données sensibles participent à une formation spécifique d'une journée avec des exercices et une évaluation.

Rochefort Habitat Océan (office qui gère 2 631 logements en Charente-Maritime) met aussi l'accent sur la sensibilisation de son personnel. Les collaborateurs ont été impliqués, en 2018/2019, autour des pratiques essentielles de sécurité à appliquer au quotidien, en vue de créer une charte informatique opposable. Leur travail a conduit à élaborer une affiche, distribuée et expliquée au personnel lors d'un petit déjeuner, et diffusée aux nouveaux arrivants. Chaque trimestre, une newsletter rappelle une bonne pratique ou attire l'attention sur un risque informatique, comme en septembre 2020 : « Les mots de passe, c'est un peu comme les brosses à dents ».

Chaque année, une réunion de sensibilisation est organisée avec le soutien du syndicat mixte Soluris ; en 2020, ce sont les agents de proximité et les responsables d'immeubles dotés de téléphones portables qui ont découvert les cybermenaces et les moyens de sécuriser les smartphones.

Depuis 2017, un groupe de travail de quatre collaborateurs et du référent sécurité de l'office suit les plans d'actions annuels sur la sécurité informatique et la protection des données. Il rédige les newsletters et s'assure auprès du personnel de l'acceptabilité et de la mise en oeuvre des règles de sécurité. Dans les petites communes, également cibles de cyberattaques, il est indispensable de faire connaître largement la plateforme de prévention et d'assistance Cybermalveillance.gouv.fr, comme l'a fait Tillières-sur-Avre (Eure, 1 098 habitants). Les agents sauront ainsi vers qui se tourner en cas d'attaque.

** L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié le 10 juin son rapport d'activité. Lors de l'attaque des sites institutionnels de la ville de et de la métropole de Toulouse, en mai 2020, Toulouse Métropole (486 828 habitants) a mis en place une cellule de gestion de crise. Mieux préparée, la collectivité a ainsi pu réagir, six mois plus tard, face au virus Emotet (extrêmement dangereux). Après accompagnement de deux semaines d'Orange CyberDefense (organisation, prises de décisions et management des opérations techniques et de communication…), la métropole a consolidé son dispositif et identifié comment l'améliorer. En parallèle, elle a renforcé ses infrastructures et outils de détection et d'analyse. Toulouse prépare un guide sur la gestion de crise et prévoit d'organiser un exercice de gestion de crise cyber pour entraîner les agents.*

DOCUMENT 5

Les régions, soutenues par l'Anssi, déploient des centres régionaux de réponse aux incidents cyber

francenum.gouv.fr - juin 2022.

Pour faire face aux menaces cyber croissantes, l'État, dans le cadre du plan de Relance, finance la création de centres régionaux de réponse aux incidents cybers : les CSIRT régionaux. Subventionné à hauteur de 1 million d'euros pour trois ans, et incubé par l'Anssi, partenaire de France Num, chaque centre régional offrira un soutien de proximité, adapté aux besoins et aux conditions économiques et sociales locales des petites et moyennes entreprises (TPE, PME) et aux entreprises de tailles intermédiaires (ETI).

Les CSIRT régionaux au service de la cybersécurité des TPE, PME et ETI

Un CSIRT régional (Computer Security Incident Response Team) est un centre de réponse aux incidents cyber au profit des entités (notamment les TPE, PME, ETI et associations) implantées sur le territoire régional.

Le CSIRT vient compléter l'offre existante en matière de cybersécurité sur son territoire : tandis que Cybermalveillance.gouv.fr s'adresse aux particuliers et aux petites structures et que l'Anssi est focaliseée sur les administrations, les opérateurs critiques et les plus grosses entreprises, les CSIRT se positionnent sur les acteurs intermédiaires.

Chaque centre doit permettre d'apporter une réponse concrète et immédiate aux victimes de cyberattaques. Sensibilisation, mise en relation avec des prestataires locaux ou encore incitation à déposer une plainte : ces structures doivent fonctionner comme des services de veille et d'urgence en cas de problème.

Ils répondent à plusieurs missions :

- centraliser les déclarations d'incidents cyber ;
- les qualifier et transmettre les premiers bons réflexes aux bénéficiaires ;
- mettre les victimes en relation avec les organisations chargées de les accompagner dans la résolution (prestataires ; police et gendarmerie) ;
- effectuer une veille des vulnérabilités et des correctifs de sécurité ;
- analyser l'état de la menace cyber visant les bénéficiaires ;
- partager les connaissances en la matière au sein du réseau des CSIRT.

Les premières régions à disposer d'un CSIRT régional :

- Bourgogne - Franche-Comté
- Centre - Val de Loire (recia.fr)
- Corse
- Grand Est
- Normandie
- Nouvelle - Aquitaine
- Provence - Alpes - Côte d'Azur (C2RCsud.org)

Les régions restantes devraient intégrer le dispositif d'ici décembre 2022 :

- Occitanie (cyberocc.com)
- Auvergne - Rhône - Alpes
- Hauts de France
- Bretagne
- Pays de la Loire
- Île de France

DOCUMENT 6

Former et sensibiliser les agents à la sécurité informatique pour réduire les risques

Pierre Alexandre Conte - *lagazettedescommunes.com* - septembre 2016.

Les acteurs du monde de la sécurité informatique s'accordent à le dire : une grande partie des incidents sont liés à une faille humaine. Une étude de l'Université Friedrich-Alexander d'Erlangen-Nuremberg menée par le professeur Zinaida Benenson et publiée mi-août a d'ailleurs révélé que 56% des personnes cliquent sur des liens présents dans des mails envoyés par des inconnus. Et ce, même si celles-ci ont conscience du danger qu'elles encourent. La curiosité est la principale raison de cette prise de risque.

Ce test effectué auprès de 1700 étudiants, Laurent Charveriat l'a relayé au cours d'un colloque organisé le 15 septembre à Puteaux par la Mission Ecoter. Le thème de celui-ci : « Sécurité des lieux, sécurité des usagers. » Le directeur d'I-Tracing, une société notamment spécialisée dans la sécurité des systèmes d'information, souhaitait par ce biais faire comprendre aux collectivités territoriales qu'elles sont d'abord rendues vulnérables par le comportement de leurs agents.

Les agents en première ligne

Contrairement à ce que beaucoup d'entre elles pensent encore, comme l'a révélé en 2015 une étude de Primo France, les collectivités territoriales sont des cibles, à l'instar des particuliers ou des entreprises. Et elles le seront d'autant plus à l'avenir avec la place croissante prise par le numérique.

De l'atteinte à la vie privée au vol de données sensibles en passant par l'altération de la réputation ou les pertes financières, les conséquences d'un piratage peuvent être multiples, comme l'a rappelé Jean-Philippe Collignon, directeur de développement chez Engie Ineo Cybersécurité.

Pour diminuer le risque, la seule véritable réponse à apporter, c'est la formation. Il est devenu indispensable de sensibiliser les agents à ces questions pour les pousser à adopter un comportement responsable tout en leur faisant prendre conscience des pratiques frauduleuses existantes. Car ces derniers sont plus que jamais en première ligne.

Début juin, la société PhishMe a publié un rapport établissant que 93% des attaques via phishing contenaient des ransomwares, soit des logiciels malveillants visant à prendre en otage des données en les cryptant et réclamer une rançon en échange de leur restitution.

Un simple clic peut ainsi conduire un système d'information à être paralysé. C'est ce qui est arrivé à un hôpital de Los Angeles, en février 2016.

Pour retrouver au plus vite un fonctionnement normal, la direction de ce dernier a dû débourser 17000 dollars. L'idée reçue veut que les hackers visent des cibles qui auraient des moyens financiers importants. Mais Laurent Charveriat rappelle qu'ils n'adoptent généralement pas cette stratégie-là : « Le maire a tendance à se dire que sa commune n'est la cible de rien, de personne. Mais la logique des hackers, c'est d'inonder partout. Statistiquement, il y a un nombre d'utilisateurs qui vont cliquer. »

De l'importance de connaître son système d'information

Si la faille humaine ne doit pas être négligée, il ne faut pas pour autant mettre de côté les autres portes d'entrée vers les systèmes d'information des collectivités territoriales. A commencer les lieux en eux-mêmes, dont la sécurité physique doit être assurée. Veiller à ce que les sous-traitants respectent les règles fixées est également indispensable.

Concernant le volet numérique, « cela ne sert à rien de tout sécuriser, cela n'a pas de sens », affirme le directeur général d'I-Tracing. Avant de préciser sa pensée : « On met des agents de police devant

les écoles, pas partout. Et on ne commence pas par la technique. Il faut faire un ‘Connais-toi toi-même’. Quelles sont les données sensibles et qui sont les consommateurs de ces données ? Uniquement des personnes en interne ou la population y a-t-elle accès ? Derrière, il faut les mesures qui s’imposent. »

Ces mesures dépendent donc essentiellement de ce qui est menacé. Certaine solutions permettent un retour rapide à un fonctionnement normal tandis que d’autres garantissent une perte minimale de données en cas de panne. Reste à savoir si l’outil met en cause le fonctionnement de la collectivité territoriale ou non. Par ailleurs, Audrey Paris, expert SSI chez Engie Ineo a pris soin de préciser qu’un « simple bilan ponctuel de la sécurité ne suffisait pas » mais qu’il fallait un « suivi en continu ».

Évidemment, cette sécurité a un coût. Mais elle est aujourd’hui devenue un enjeu central. Pour ceux qui se refusent encore à penser dans ce sens, le nouveau règlement européen sur la protection des données personnelles qui entrera en application en 2018 devrait achever de les convaincre. Les sanctions seront ainsi renforcées.

Certes, une marge de manoeuvre est laissée aux États par rapport au secteur privé mais les amendes encourues par les entreprises – jusqu’à 20 millions d’euros ou de 2 à 4% du chiffre d’affaire – en cas de non respect des règles donnent un ordre d’idée des sanctions envisageables.

Avant d’en arriver là, mieux vaut donc anticiper. Et appliquer dans un premier temps ce que préconise l’ANSSI dans son référentiel général de sécurité.

DOCUMENT 7

Cyberattaque au Département de Seine-et-Marne : Le point sur la situation

seine-et-marne.fr - novembre 2022.

Depuis le 6 novembre, le Département est victime d'une attaque informatique de grande ampleur. Tous les réseaux informatiques de la collectivité ont été coupés par mesure de sécurité. Le Département est pleinement mobilisé pour évaluer les préjudices, limiter les conséquences et rétablir les systèmes au plus vite. Le point au 26 décembre 2022.

Dans un contexte de cyberattaque, le Département de Seine-et-Marne s'adapte pour le maintien du service public. Le paiement des prestations sociales, dont la PCH est bien maintenu.

Pour les personnes dont les droits venaient à échéance entre octobre et décembre 2022, leurs droits ont été automatiquement reconduits par les services du Département.

Pour les personnes dont les droits devaient s'ouvrir à compter de novembre ou de décembre 2022, nous ne prenons en compte qu'uniquement les situations urgentes qui nous sont signalées.

Malgré la situation, nous restons pleinement mobilisés pour assurer la continuité des services et des prestations sociales.

Une mobilisation globale

Face à une attaque ciblant l'ensemble de ses réseaux informatiques, le Département de Seine-et-Marne a été contraint de couper ses réseaux afin de protéger les données et isoler son système informatif. En parallèle, une plainte a été déposée le 7 novembre et une notification a été envoyée à la CNIL.

La Direction des systèmes d'information et du numérique (DSIN) est mobilisée en collaboration avec Orange cyberdéfense et avec l'aide de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Un diagnostic est en cours afin d'évaluer les préjudices et limiter les conséquences de cette cyberattaque.

Plan de continuité du service public

Le Département de Seine-et-Marne est pleinement mobilisé pour continuer à assurer ses missions de service public. Les services publics (MDS, PAT, MDPH, PMI, etc.) sont ouverts au public et opérationnels.

La collectivité déploie des numéros de téléphones utiles afin de permettre aux usagers de joindre les différents services départementaux. Les lignes téléphoniques habituelles reviennent progressivement.

Comment contacter les services ?

Maisons départementales des solidarités (MDS)

Les 14 Maisons Départementales des Solidarités de Seine-et-Marne continuent d'accueillir du public. La prise de rendez-vous est opérationnelle sur le site rdv-solidarites.fr.

Pour tout renseignement, les usagers peuvent désormais contacter les MDS en consultant l'annuaire des MDS.

Maison départementale des personnes handicapées (MDPH)

La MDPH continue d'accueillir du public aux jours et horaires habituels. Pour contacter la MDPH, trois lignes téléphoniques sont mises en place pour les usagers :

- 06.30.33.22.31 - 06.70.21.57.69 - 06.07.85.53.39

La MDPH est joignable également par mail à l'adresse : contact@mdph77.fr.

Points Autonomie territoriaux (PAT)

Les 6 PAT et leurs antennes continuent d'accueillir du public. Les lignes téléphoniques fixes et les mails sont opérationnels.

Prestations sociales

Les droits en cours seront automatiquement renouvelés afin d'éviter toute rupture de droit d'accompagnement. La CAF assure le versement des allocations aux bénéficiaires du RSA. Il n'y aura donc aucun impact sur les allocataires du RSA, les droits sont bien maintenus.

Protection de l'enfance

Pour les informations préoccupantes, les inspecteurs d'éducation doivent contacter l'adresse suivante : cripsetm@gmail.com

Musées départementaux et château de Blandy

Les musées départementaux sont ouverts au public, excepté le musée-jardin Bourdelle actuellement fermé au public. Les sites internet des musées départementaux et du château de Blandy sont opérationnels.

Pour tout renseignement, les usagers peuvent contacter les musées et château aux numéros habituels, les lignes téléphoniques étant rétablies :

- Musée-Jardin Bourdelle : 06.07.32.93.33
- Musée de Préhistoire d'Île-de-France : 01.64.78.54.80
- Musée de la Seine-et-Marne : 01.60.24.46.00
- Musée des peintres de Barbizon : 01.60.66.22.27
- Musée Stéphane Mallarmé : 01.64.23.73.27
- Château de Blandy : 01.60.59.17.80

Pour information, Les musées départementaux sont ouverts au public gratuitement jusqu'à nouvel ordre.

Archives départementales

La consultation des archives numérisées en salle et la réservation des cotes à distance sont temporairement indisponibles. La consultation des documents papier reste cependant possible en salle de lecture à l'adresse : 248, avenue Charles Prieur 77190 Dammarie-les-Lys.

Pour tout renseignement, les usagers peuvent joindre le 01.64.87.37.17. Plus d'informations sur le site des Archives départementales de Seine-et-Marne.

Médiathèque départementale

En cas d'urgence, les usagers peuvent joindre le 06.33.16.02.55. Plus d'informations sur le site de la Médiathèque départementale.

Direction des transports

En cas d’urgence, la Direction des Transports est joignable au 06.72.98.80.03.

Direction des routes

La Direction des Routes est joignable aux numéros suivants :

- Direction : 06.37.02.05.65
- ARD de Coulommiers : 06.76.54.42.95
- ARD de Meaux : 06.76.54.35.20
- ARD de Melun : 06.76.99.64.43
- ARD de Moret : 06.84.80.58.82
- ARD de Provins : 06.84.80.30.20

Direction de l’eau, de l’environnement et de l’agriculture

La Direction, les responsables des services et les chargés de mission restent joignables sur leur téléphone portable. Les activités du laboratoire restent normales. Toutes les activités extérieures des autres services (réunions, prélèvements) sont assurées normalement.
En cas d’urgence, la Direction de l’Eau, de l’Environnement et de l’Agriculture est joignable au 06.76.09.50.41.

Direction des sports

En cas d’urgence, la Direction des Sports est joignable au 01.64.14.55.34.

La Direction de l'architecture, des bâtiments et des collèges

En cas d'urgence, la Direction de l'architecture, des bâtiments et des collèges est joignable au 06.08.63.24.26

La Direction de l'Aménagement et du développement des territoires

L'accompagnement des communes et des intercommunalités dans leurs projets d'investissements est maintenu et le suivi des grands dossiers d'aménagement continue. Vous pouvez joindre la direction au 06.74.01.72.98

Direction des Affaires culturelles

La campagne de subventions 2023 se déroule normalement. Les services accuseront réception des dossiers reçus exclusivement par voie postale.

DOCUMENT 8

Cyberattaques dans les hôpitaux : « Le paiement de rançon n'est pas une solution, sinon, ça devient le Far West »

Julien Lemaignen et Manon Romain - *leMonde.fr* - décembre 2022.

Comment les hôpitaux doivent-ils faire face aux cyberattaques ? Pour Vincent Trely, spécialiste de la sécurité des systèmes de santé, l'investissement doit s'accompagner du recrutement d'experts.

Les urgences sont réduites à la moitié de leur activité habituelle, la maternité, au tiers, mais *« la sécurité des soins est assurée ».* Tel était le bilan, lundi 5 décembre au soir, de la cyberattaque qui a visé le centre hospitalier de Versailles (Yvelines) deux jours plus tôt, selon Richard Delepierre, le coprésident du conseil de surveillance de l'établissement. Celui-ci a fait savoir que les pirates avaient demandé le paiement d'une rançon, au montant non divulgué, pour rétablir le système informatique.

Le 22 août, le Centre hospitalier Sud-Francilien de Corbeil-Essonnes (en Ile-de-France également) avait vu son fonctionnement perturbé pendant plusieurs semaines par une attaque comparable. En 2021, *« on a constaté près d'une attaque par semaine sur nos établissements de santé »*, avait expliqué Jean-Noël Barrot, le ministre délégué à la transition numérique, lors d'une visite sur place, précisant qu'en 2022 *« ce chiffre a baissé au premier semestre de 50 % ».*

Dans un entretien au *Monde*, le consultant Vincent Trely, fondateur et président de l'Association pour la sécurité des systèmes d'information de santé, détaille les protocoles de sécurité mis en place pour anticiper et répondre à ces menaces. Un défi majeur, car, selon lui, il n'y a *« aucune raison »* pour que les établissements de soins cessent d'être la cible des hackeurs.

Quelles sont les conséquences d'une cyberattaque pour le fonctionnement des établissements ?

Vincent Trely : Toutes les attaques n'ont pas la même gravité. Des hôpitaux peuvent s'en remettre en trois ou quatre jours, parce que l'attaque a été prise au bon moment, ou n'a pas exploité tout ce qu'elle pouvait faire. Dans le cas extrême, tout est chiffré par les pirates, jusqu'à la sauvegarde du système, comme dans le cas de Dax, dans les Landes, en 2021, où l'hôpital a perdu dix ans de données.

Quel protocole les hôpitaux suivent-ils en cas de cyberattaque ?

La première étape est la détection : le directeur de garde est alerté d'une manière ou d'une autre qu'il y a un problème. Il appelle le responsable de la sécurité informatique ; ils vont mettre une heure et demie ou deux heures à qualifier le problème en cyberattaque. On procède alors au cloisonnement : on débranche, en partant du principe que l'infection ne s'est peut-être pas propagée partout.

Puis est constituée une cellule de crise, avec notamment la direction générale et le président de la commission médicale d'établissement. Elle va orchestrer la réponse. Elle recense tous les problèmes liés aux patients. L'hôpital passe en mode « plan blanc », qui couvre la sécurité sanitaire. Les transferts de patients critiques, préalablement établis entre l'hôpital et des établissements partenaires, sont exécutés.

Au bout de six à dix heures, la cellule a une cartographie des dégâts. Si l'établissement est un « opérateur de services essentiels », l'Agence nationale de la sécurité des systèmes d'information (Anssi) va envoyer des experts. A-t-on toujours la sauvegarde ? Où se trouve le virus ? Il n'est pas question de redémarrer les machines si on n'a pas la certitude de l'avoir éliminé partout. Il faut douze à quinze heures pour comprendre ce qu'il s'est passé et évaluer l'étendue du sinistre.

Ensuite, il va probablement y avoir une phase de négociation avec le pirate qui demande une rançon. Elle ne se passera pas bien, car les hackeurs croient que les hôpitaux, qui disposent de budgets importants, pourront payer des sommes importantes comme une grosse entreprise. Mais l'hôpital ne paiera pas, et le pirate diffusera des données. L'établissement entre dans une phase de crise juridique, car il n'est plus en conformité avec le règlement général sur la protection des données (RGPD). Le pirate vend alors à d'autres pirates des morceaux de sa base de données : copies de passeports, de cartes Vitale, adresses e-mails, numéros de téléphone…

Du côté informatique, on reconstruit et on sécurise. Si on disposait de bonnes sauvegardes et d'un système à peu près solide, au bout de dix à douze jours on peut rétablir l'activité à 80 %. On va mettre plusieurs semaines ou plusieurs mois à travailler sur les 20 % pour lesquels ça ne s'est pas bien passé.

Des hôpitaux ont-ils déjà payé une rançon ?

A ma connaissance, non, ni dans le public ni dans le privé. Les directives sont très claires. On n'a jamais considéré le paiement de rançon comme une solution, comme pour les prises d'otages. Sinon, ça devient le Far West. Il y a d'ailleurs eu un peu d'émoi lorsque Bercy a autorisé les assureurs à proposer le paiement de rançon dans leurs garanties. Cela envoie un très mauvais signal, en contradiction avec l'Anssi qui est rattachée au premier ministre.

S'ils ne payent pas de rançon, pourquoi les hôpitaux sont-ils pris pour cibles ?

Un hôpital contient des millions de documents avec des données de santé à caractère personnel. On peut les voler pour les vendre, ou les rendre indisponibles pour faire du chantage.

La quatrième révolution numérique, c'est l'intelligence artificielle (IA) ; or, pour faire apprendre quelque chose à une IA, il faut de la data. Aujourd'hui, on a le moteur et le carburant : le moteur, c'est la puissance de calcul ; le carburant, ce sont les données. Pour le premier qui détectera automatiquement le cancer du sein cinq ans avant les radiologues, ce sont des dizaines de milliards de dollars à long terme.

On est au début de l'histoire. Aux Etats-Unis, entre 2000 et 2007, à la grande époque de la numérisation des hôpitaux, 170 millions de dossiers ont été volés, quasiment 100 %. Il n'y a aucune raison pour que les pirates nord-coréens ou russes arrêtent, et aucune raison pour que les narcotrafiquants ne commencent pas à s'y intéresser.

Les hôpitaux présentent-ils des failles de sécurité spécifiques ?

Beaucoup de systèmes sont connectés, comme les couveuses en néonatalité pour gérer les températures, ou les pousse-seringues en réa. Or, le matériel biomédical est parfois supporté par une informatique obsolète : beaucoup d'appareils tournent sous Windows XP *[lancé en 2001, et dont Windows a arrêté le support en 2014]* et certains systèmes datent même de 1998 ou 2000.

On travaille aussi sur les comportements : pour les personnels hospitaliers, dans un monde idéal, tous les ordinateurs sont allumés en permanence. Acheter 10 millions d'euros de produits de sécurité et recruter cinq personnes à temps plein sur le sujet, ça va avoir un impact, mais c'est ne traiter qu'une partie du problème : si les gens cliquent sur un faux e-mail qui clignote en promettant de gagner 10 000 euros, vos outils feront long feu.

Les établissements de santé sont-ils assez bien préparés ?

Les hôpitaux sont numérisés depuis vingt ans, et toute une génération n'a connu que le plan de soins informatisé. Depuis 2019, un certain nombre de sites ont pris le temps de simuler le travail sans informatique. Le risque numérique est de plus en plus pris en compte dans le plan blanc de chaque hôpital. En général, les hôpitaux ont une expérience de crise, du fait notamment du Covid-19. Entre public et privé, la situation est à peu près similaire.

Les responsables de la sécurité sont bien plus écoutés qu'il y a quelques années, mais on a 1 300 systèmes informatiques dans le public, 3 000 en comptant le privé, qui sont très hétérogènes. Les incidents récents ont, entre guillemets, « fait du bien ». En février 2021, les 135 principaux hôpitaux ont été nommés « opérateurs de services essentiels », et ont l'obligation d'appliquer 23 règles de sécurité spécifiques décidées au niveau européen. Et le président de la République a annoncé un plan d'investissement de 350 millions d'euros, dans le Ségur de la santé, ciblés sur le cyber.

La difficulté majeure, c'est que l'argent ne suffit pas, il faut aussi des bras. Or tout le monde cherche des techniciens cyber : le CAC 40, les collectivités, les start-up, les entreprises de services du numérique… Par conséquent, il peut être intéressant de partager les compétences entre plusieurs hôpitaux, car il ne sert à rien qu'un petit hôpital de campagne ait son propre responsable sécurité et cyberexpert payé 120 000 euros par an.

DOCUMENT 9

Pour sécuriser les petites communes, faut-il mutualiser les RSSI ?

Louis Adam - *zdnet.fr* - juin 2021.

Sécurité : Les attaques visant les collectivités territoriales se sont multipliées au cours de l'année passée.
L'Anssi a été chargée, au travers du fonds du plan de relance, de soutenir l'effort de sécurisation de ces organisations, mais la sécurisation des petites communes reste un chantier complexe.

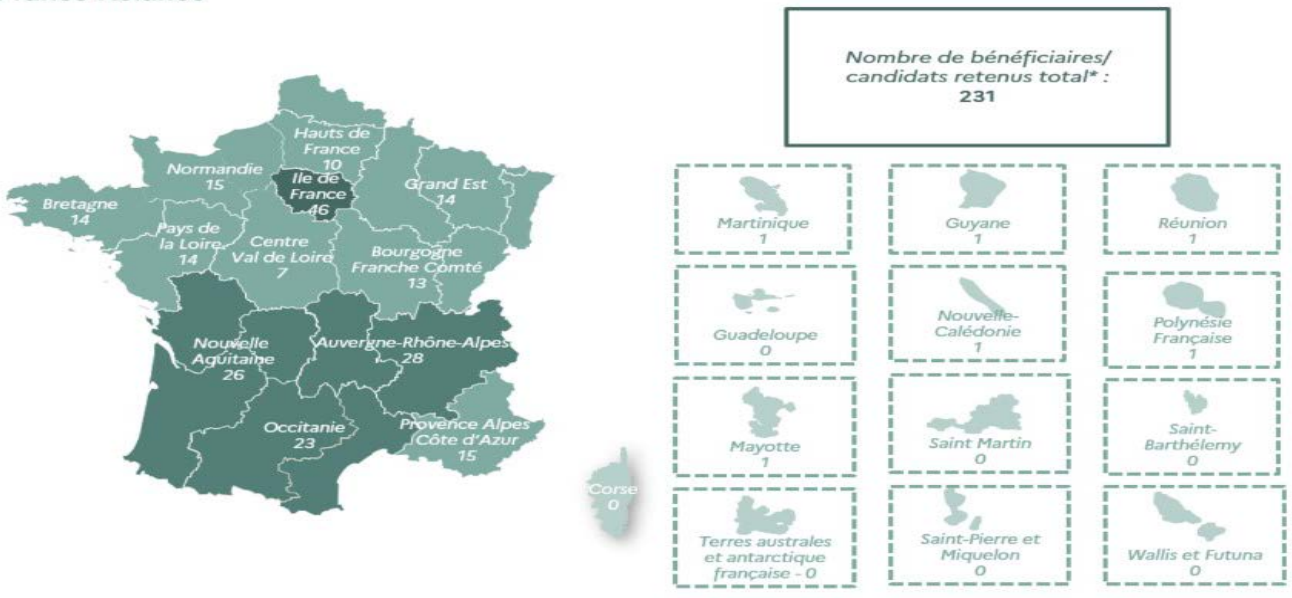
Les attaques au ransomware ont mis en lumière la vulnérabilité des communes françaises face aux attaques informatiques au cours de l'année passée. Si les attaques ayant visé les grandes métropoles comme Marseille ont fait beaucoup parler d'elles, les communes de taille plus modeste n'ont pas échappé aux ransomwares : Mitry-Mory, Antony, Morière-lès-Avignon, la liste des victimes est longue et loin d'être exhaustive.

L'initiative de l'Anssi

La situation n'a pas échappé à l'Anssi et au gouvernement, qui ont commencé en début d'année à s'appuyer sur les fonds alloués à l'agence dans le cadre du plan de relance pour financer un soutien à la sécurisation des collectivités territoriales et des établissements de santé, deux secteurs particulièrement touchés par les attaques au ransomware. « Nous avons mis en place différentes mesures », expliquait Gwenaëlle Martinet, chef du projet France Relance à l'Anssi, lors de la conférence de presse consacrée au rapport d'activité 2020 de l'agence.

« Tout d'abord, la mise en place de "parcours sécurité" » visant à comprendre le niveau de maturité des bénéficiaires, voire à mettre en place des actions de premier niveau pour les acteurs les plus avancés. » Des audits de sécurité financés par l'Anssi, et confiés à des acteurs privés, afin de mieux comprendre l'état de sécurité des collectivités territoriales intéressées. « Nous avons actuellement 230 bénéficiaires qui profitent d'un de ces parcours, qui travaillent avec un prestataire », précise Gwenaëlle Martinet.

Répartition en métropole et dans les DOM-TOM des bénéficiaires du volet cybersécurité de France Relance



Source / données de référence : bénéficiaires de l'expérimentation + bénéficiaires candidats retenus et sur liste d'attente de la phase de généralisation

Le second volet du plan s'adresse quant à lui à des collectivités territoriales plus matures en termes de sécurité et qui souhaitent bénéficier des aides de l'Anssi pour cofinancer un projet de sécurisation, prenant la forme d'achat de matériel ou de logiciel par la collectivité. Les grandes lignes de ce plan avaient déjà été présentées au travers d'une lettre transmise aux collectivités territoriales en début d'année.

Viser le bon niveau

Restait une question en suspens : celle des plus petites collectivités territoriales, les nombreuses petites communes qui n'ont pas toujours les moyens de s'offrir des équipements ou des outils dédiés à la sécurité, mais qui restent néanmoins ciblées par ces attaques. Et l'Anssi n'a pas les moyens de financer des audits de sécurité pour l'ensemble des communes de France, même avec les moyens alloués dans le cadre du plan de relance.

Interrogée à ce sujet, Gwenaëlle Martinet explique la logique de l'agence en la matière : « il n'y a pas à proprement parler de seuil de population pour accéder à ces parcours de cybersécurité, mais il y a un critère de maturité technique. Il faut que la commune ait un service informatique ou un RSSI, qui pourra être notre interlocuteur dans le cadre de ce parcours.

C'est celui qui sera en mesure de comprendre ce que l'on fait et de le faire perdurer dans le temps une fois le parcours achevé ». Mais, avec 36 000 communes dans le pays, on imagine mal les mairies de 3 000 habitants se doter d'un RSSI quand certaines ont déjà bien du mal à assurer leur fonctionnement au quotidien. La chef de projet de l'Anssi évoque une piste : celle de la mutualisation des RSSI pour les plus petites communes.

La mutualisation des ressources informatiques n'est pas une idée complètement nouvelle. C'est notamment l'objet des différentes associations et structures fédérées au sein du réseau Declic, avec lequel l'Anssi avait passé un partenariat en 2020. Si l'approche existe déjà pour de nombreuses fonctions liées à l'informatique, décliner celle-ci pour le domaine de la sécurité est une chose assez nouvelle, comme nous l'explique Emmanuel Vivé, président du réseau Déclic et DG de l'Adico : « on commence depuis quelque temps à proposer des services de RSSI mutualisé au sein de nos structures, en s'inspirant du modèle des DPO mutualisés qui se sont créés avec l'entrée en vigueur du RGPD.

On décline la logique et on essaie de convaincre les autres organisations du réseau Declic de faire de même ». Pour l'instant, une poignée de structures ont mis en place ce type de prestations, entièrement financées par les communes adhérentes. « Il s'agit toujours de trouver le bon équilibre financier pour proposer ce type de prestation, et surtout de convaincre les communes qu'elles ont un intérêt à les financer » explique-t-il.

« On tombe sur des serveurs vieux de 12 ans »

L'idée est nouvelle, mais elle fait son chemin, et les premiers RSSI mutualisés travaillent déjà avec des communes. La tâche se concentre principalement sur la mise en place d'audits RGS auprès des communes intéressées. « Il faut bien comprendre qu'on part de loin avec ces organisations. On tombe des fois sur des serveurs qui sont là depuis 12 ans, sans mise à jour. La sécurité informatique n'est pas une priorité pour les maires des petites communes, donc le travail c'est avant tout de les sensibiliser et de revoir les bases en la matière.

Le référentiel RGS est bien fait pour ces cas de figure, il n'est pas trop technique et permet d'aborder le sujet de façon concrète », explique le dirigeant du réseau Declic. Les actions d'un RSSI de ce genre se concentrent principalement sur la sensibilisation et sur l'audit des communes. Ce qui ne l'empêche pas d'aller intervenir directement lorsqu'une situation de crise se présente, mais cela reste une exception.

Reste que si l'idée commence à prendre forme, elle reste délicate à mettre en œuvre. Il est par exemple difficile de recruter des profils expérimentés, surtout quand les moyens des communes et des structures de mutualisation sont bien en deçà des prix du marché. « Dans la plupart des cas, on préfère former des gens de chez nous », confie Emmanuel Vivé. Ce qui ne signifie pas non plus que la tâche sera simple : principe de libre administration des collectivités territoriales oblige, chaque système informatique est différent et présente ses spécificités propres, une complexité de plus pour un RSSI qui devra auditer et conseiller plusieurs dizaines de communes dans l'année. Et il faut enfin convaincre les élus de l'intérêt de la démarche, qui n'est pas toujours considérée comme une priorité.

DOCUMENT 10

Cybercriminalité : « Nous ne voulons plus qu'un élu nous dise qu'il ne savait pas »

Hélène Lerivrain - *lagazettedescommunes.com* - décembre 2021.

Quelles sont les missions du responsable de la sécurité des systèmes d'information ?

Philippe Steuer, RSSI de Bordeaux Métropole : Elles sont triples. Sur la partie amont, c'est lui qui met en place des règles de sécurité en lien avec une analyse du risque. Une évaluation est ainsi réalisée pour chaque nouvelle application ou nouveau service puis tout au long de leur vie sous la forme d'audit/contrôle.

En parallèle, le RSSI a une mission de sensibilisation des utilisateurs et des élus, l'objectif étant que ces derniers prennent conscience des enjeux de la cyber, qu'ils comprennent l'évolution de la menace et les risques que cela implique pour le fonctionnement des services. Comment fera-t-on demain quand nous n'aurons plus d'informatique dans le cadre d'une attaque ?

Le RSSI, dans sa fiche de poste, est souvent rattaché au directeur des systèmes d'information. C'est un sujet sur lequel vous échangez régulièrement au sein du club.
En quoi est-ce discutable ?

Le RSSI, qui doit protéger un système d'information est piloté par le DSI dont le métier consiste à faire fonctionner ce même système d'information. Selon ce schéma, la priorité est donnée à la mise en place de services et non systématiquement à la sécurité qui est souvent une variable d'ajustement.

Au niveau du club RSSI, nous faisons donc du lobbying auprès du CNFPT pour modifier la fiche de poste du RSSI voire créer un profil de directeur sécurité numérique. Ces profils pourraient, par exemple, être rattaché au directeur général des services qui fait le lien entre l'administration et le politique. Il est très important que le RSSI puisse aller voir directement et très en amont les élus qui prendront les décisions.

A quels types de risques doivent faire face les collectivités ?

Aujourd'hui, le risque numéro un est le rançongiciel qui bloque les missions de services publics et exige le paiement d'une rançon. La crainte porte également sur les systèmes industriels tels que la distribution de l'eau, l'assainissement ou encore le réseau de transport qui sont bien souvent des technologies anciennes qui n'ont pas embarqué nativement les aspects de cybersécurité et sont, par ailleurs, de plus en plus interconnectés.

Pour améliorer la cyberprotection, vous avez lancé, avec vos homologues de Toulouse et Grenoble, un club RSSI que vous officialiserez très prochainement à l'occasion de la création d'une association. Qu'apporte-t-il de nouveau ?

En premier lieu, ce club s'adresse aux collectivités et aborde donc des sujets qui leurs sont propres. Concrètement, nous menons des actions communes auprès des éditeurs pour répondre à nos exigences de sécurité. Nous avons également mis en place une plateforme d'échange technique d'indices de compromission, hébergée à l'Institut national pour la cybersécurité et la résilience des territoires (INCRT), pour signaler des adresses IP, des mails, des noms de domaines qui constituent des menaces. Nous partageons également les bonnes pratiques et proposons des retours d'expériences de collectivités. L'entraide est capitale, y compris avec des collectivités qui n'ont pas de RSSI.

L’une des limites du club étant justement de ne concerner que les RSSI et donc les grosses collectivités, quelles modifications ont été apportées ?

Nous intégrons, par exemple, des syndicats mixtes qui gèrent l’informatique et la sécurité des petites communes comme Gironde Numérique ou Soluris à La Rochelle, ce qui permet de diffuser l’information vers les plus petites collectivités. Quand il n’y a pas de RSSI, il est également possible de faire adhérer la personne qui occupe les missions d’un RSSI.

Nous demandons, dans ce cas, un courrier de son chef l’attestant. Et puis nous évoluons d’une « vision RSSI », jugée souvent et à tort technique, vers un périmètre plus global de la sécurité numérique ce qui pourrait nous amener à intégrer d’autres profils. D’où notre changement de nom, pour « club de la sécurité numérique des collectivités ».

Quelles sont vos ambitions pour 2022 ?

Nous ne pouvions pas nous développer sans structure, ce sera donc chose faite début 2022. Ensuite, alors que le club qui travaille avec l’Anssi compte aujourd’hui 150 RSSI, il s’agira d’accélérer le déploiement national, d’industrialiser nos actions.

Une attaque, c’est une perte financière, une perte d’image, des retards dans les dossiers de service public, la perte de données, la baisse de moral des agents et une baisse de confiance des usagers. Nous ripostons avec des valeurs fortes : l’échange, la cohésion, la confiance et le partage. Mais surtout, nous essayons de faire en sorte qu’un élu ne nous dise plus « je ne savais pas ».

DOCUMENT 11

Cyberattaques : la négligence des collectivités pourrait leur coûter cher

Lucas Boncourt - *banquedesterritoires.fr* - juillet 2022.

Les collectivités territoriales qui négligeraient la sécurité de leurs données et infrastructures numériques risquent gros. C'est ce qu'il ressort du guide sur les obligations cyber des collectivités que viennent de publier la Cnil et Cybermalveillance.

Résumer en 16 pages dans un langage accessible les obligations des collectivités locales en matière de (cyber) protection des données est le défi que s'est fixé le guide obligations et responsabilités en matière de cybersécurité des collectivités locales que viennent de publier la Cnil et le GIP Acyma (Cybermalveillance). Un guide qui complète les ressources existantes – mise en œuvre du RGPD, hygiène informatique, notification de cyberattaque… - tout en clarifiant le cadre juridique en vigueur.

Risques financiers

Une récente enquête d'Acyma (notre article du 18 mai 2022) avait en effet montré la faible conscience des petites collectivités sur le périmètre et la réalité des risques cyber qui les menacent. Le guide insiste ainsi sur les conséquences matérielles des cyberattaques affectant les collectivités avec de potentiels préjudices financiers directs (prestataire, réinstallation, reconfiguration…) mais aussi indirects (pertes de recettes de services comme la piscine ou le stationnement).

Des dommages qui s'ajoutent à la "perte du lien de confiance" qui relie la collectivité à ses administrés. Plus grave encore : la mise en danger de la vie d'autrui pouvant résulter de feux de circulation hors service ou d'un panneau de signalisation piraté. Autant d'incidents susceptibles d'engager la responsabilité administrative, civile ou pénale des collectivités, des élus et des agents.

Collectivités et élus responsables

En cas de fuite de données personnelles, les collectivités comme leurs satellites ou les sociétés d'économie mixte risquent tout d'abord les foudres de la Cnil. Au titre du RGPD, la commission peut prononcer des sanctions financières pouvant aller jusqu'à 20 millions d'euros si elle constate des "manquements graves aux mesures de sécurité nécessaires à la protection des données personnelles".

Les citoyens sont également susceptibles d'engager la responsabilité de la collectivité pour faute s'il était établi que le préjudice subi est lié à des manquements en matière de cybersécurité. Le guide mentionne l'exemple (plausible) d'un achat frauduleux réalisé à la suite d'une fuite de coordonnées bancaires stockées par la collectivité.

Le dysfonctionnement d'un équipement public pourrait également entrainer la responsabilité administrative de la commune "pour dommage de travaux publics". Les élus et agents risquent également leur mise en cause personnelle, au titre de leur responsabilité civile. Le guide cite l'exemple (fictif) d'un téléservice défaillant mis en place par un élu sans étude de sécurité préalable malgré les mises en garde d'un agent.

Enfin, en cas d'atteinte à l'intégrité physique d'une personne résultant des conséquences d'une cyberattaque les élus et agents pourraient être attaqués au pénal.

Clarification des lois applicables

Au-delà des règles usuelles sur la protection des données – qui sont en vigueur pour la plupart depuis 1978 – les juristes apportent ensuite des clarifications sur les lois applicables. Il s'avère ainsi que l'ensemble des téléservices des collectivités locales – demandes d'extraits d'état civil, inscription et paiement de la cantine, demande de logement social… - sont soumis au Référentiel Général de Sécurité, ou "RGS", qui les oblige, entre autres, à une analyse de risque et à protéger leur système d'information.

Les téléservices nécessitant une identification, une authentification ou une signature électronique doivent aussi respecter les spécifications techniques imposées par le règlement européen eIDAS (1) pour être interopérables avec ceux des autres pays européens. Il apparait enfin qu'au titre de leurs compétences sociales, les départements et communes sont assujettis à la législation sur l'hébergement des données de santé.

Autant d'obligations qui devraient inciter les petites collectivités à se doter de véritables compétences en matière d'informatique et de sécurité, quitte à les mutualiser au niveau d'un EPCI.

(1) La réglementation eIDAS pour Electronic IDentification And Trust Services est le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein des 28 Etats membres de la communauté européenne.