GUIDE

CYBERSÉCURITÉ : TOUTES LES COMMUNES ET INTERCOMMUNALITÉS SONT CONCERNÉES

Novembre 2020

AMF
ASSOCIATION DES MAIRES DE FRANCE
ET DES PRÉSIDENTS D'INTERCOMMUNALITÉ

Éditorial

Guillaume POUPARD
Directeur général de l'ANSSI

Le risque numérique est une réalité prise de plus en plus au sérieux. Mais une fois réalisée la prise de conscience de l'importance du sujet, il est complexe d'évaluer précisément les risques, de prioriser les mesures à mettre en œuvre, d'identifier et de mobiliser les ressources adéquates (expertises, budget, etc.)... Pour vous accompagner dans ce délicat processus, nous avons joint notre expertise à celle de l'AMF, que je remercie chaleureusement pour la qualité de notre collaboration, afin de vous proposer un guide pratique porteur d'un message fort : vous n'êtes pas seuls !

Pour les communes et les intercommunalités, la transformation numérique est une source d'opportunités formidables dont vous mesurez chaque jour davantage l'intérêt : amélioration de la qualité des services en faveur des administrés, mutualisation et réduction associées des coûts, gain en notoriété et meilleure visibilité de l'action municipale et, plus largement, de l'action publique.

Cette transformation est aussi source de risques : défiguration de sites Internet, prise de contrôle de comptes de messagerie et de réseaux sociaux, vol de données sensibles, notamment celles à caractère personnel, ou encore rançongiciels pour ne citer que les plus visibles d'entre eux. Lorsque survient une attaque informatique, outre l'impact sur l'image de la commune et l'atteinte à la confiance de ses administrés, c'est la responsabilité même de l'élu qui peut être engagée. S'il est de plus en plus difficile de dire « Je ne savais pas » et qu'être victime d'attaque informatique ne doit pas être « honteux », il est en revanche de votre responsabilité de prendre en compte ces enjeux au juste niveau et de décider la mise en œuvre des mesures de sécurité numérique nécessaires.

Le dispositif cybermalveillance.gouv.fr, l'ANSSI à travers ses délégués régionaux et de plus en plus d'acteurs de proximité sont là pour vous accompagner. Plus proche encore de vous, votre responsable numérique saura établir un diagnostic de vos systèmes d'information s'il est bien formé et doté des ressources et moyens nécessaires à sa mission. Quant au présent guide, il a pour ambition de vous accompagner dans la prise en compte des questions de cybersécurité qui ne doivent plus être simplement perçues comme une épée de Damoclès mais bien comme une démarche collective nécessaire, ambitieuse et maîtrisée.

Bonne lecture et bon courage !

Éditorial

François BAROIN
Président de l'AMF

Les communes et les intercommunalités sont engagées, comme le reste de la société, dans une profonde transformation numérique. En particulier, leurs échanges dématérialisés avec les citoyens, les acteurs économiques et les administrations publiques se sont multipliés. Dans le même temps, elles sont aussi devenues, ces derniers mois, des cibles d'attaques informatiques de plus en plus nombreuses.

Pour cette raison, je me félicite du travail réalisé en commun avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui, s'appuyant sur une initiative conjointe de cette agence et de collectivités locales bretonnes, est destiné à sensibiliser les élus communaux et intercommunaux et leurs services aux enjeux de la cybersécurité.

Cette prise de conscience est plus que jamais nécessaire. Elle conduit tout à la fois à s'interroger sur les menaces qui pèsent sur la collectivité, sur les mesures à mettre en œuvre pour s'en protéger, mais aussi sur les actions à entreprendre pour répondre avec le plus d'efficacité aux attaques auxquelles elle pourrait, malgré tout, être confrontée.

Les vulnérabilités sont en effet nombreuses, car les intrusions peuvent venir tout autant d'un téléphone mobile que de la messagerie d'un poste de travail. Rappelons d'ailleurs que l'ANSSI, ses délégués régionaux et la plateforme cybermalveillance.gouv.fr sont à leur disposition, particulièrement en cas d'attaque numérique.

Ce document a donc pour vocation de susciter chez les élus cette prise de conscience. Il doit également leur permettre de vérifier l'état de préparation de leur commune ou de leur intercommunalité face à ces risques numériques et à leurs conséquences. En ce sens, il apporte des conseils pratiques et met en évidence les chantiers prioritaires à engager.

Il appartient donc à chaque commune et intercommunalité, selon ses moyens, de bâtir un environnement numérique de confiance. Ce guide est destiné à les y aider et j'en remercie l'ANSSI.

Sommaire

Introduction

Si ce guide propose une trentaine de recommandations et de bonnes pratiques en matière de sécurité numérique, sa finalité première est avant tout de susciter un questionnement pour les élus. La réflexion ainsi ouverte doit permettre de répondre à cette simple question : ma commune ou mon intercommunalité est-elle bien préparée face aux risques numériques ?

Quelle que soit la réponse, ce guide a vocation à apporter des conseils pratiques et à proposer les axes prioritaires à renforcer, sinon à développer. S'il n'est pas technique, ce guide propose cependant les briques nécessaires à l'élaboration d'une gouvernance qui devient dès lors garante de l'établissement d'un cadre de confiance numérique.

La vocation de ce guide est bien de renforcer la prise de conscience de chacun, élus, mais aussi cadres et agents territoriaux. Elle est aussi de mettre l'accent sur des points d'action très concrets puis d'inviter à partager et construire tous ensemble la sécurité numérique collective que chaque citoyen attend de son territoire.

Pourquoi les élus communaux et intercommunaux doivent se mobiliser ?

La dématérialisation engagée par l'ensemble des acteurs, qu'ils soient économiques ou au service des citoyens, participe au mouvement puissant et irréversible de transformation numérique de la société.

Facteur d'échanges et de réponse aux multiples besoins, cette transformation ne sera bénéfique pour tous qu'à la seule condition qu'elle s'opère dans un environnement de confiance. S'il n'y a pas de confiance, il n'y aura pas d'usages.

« Pas de territoire intelligent sans sécurité. Quand on construit une maison, on met des portes et des serrures. »
Valéria Faure-Muntian, députée de la Loire – colloque « La gestion du risque numérique dans les collectivités territoriales » - 25 février 2020.

Les communes et les intercommunalités, quelle que soit leur taille, ne sont pas à l'abri d'une cyberattaque

Alors que les menaces sont multiples, permanentes et de plus en plus agressives, le risque numérique s'accroît à mesure que prolifèrent les attaques non-ciblées, massives et diffuses telles que les rançongiciels. L'objectif de ces opérations est de toucher le maximum de victimes, privées comme publiques, grandes comme petites, de manière opportuniste.

Pour les communes et les intercommunalités, ces situations de crise peuvent avoir un impact important, d'une part, sur leurs activités, ce qui peut notam-

ment les conduire à ne plus pouvoir assurer leurs missions, et d'autre part, sur les données qu'elles détiennent telles que les données d'état civil des habitants, les données bancaires des usagers, les données de santé des agents...

Les sites Internet ne doivent pas être l'unique point d'attention. L'origine des attaques informatiques est multiple, elles peuvent être d'origine externe (site Internet, téléphone mobile, cybercriminels...) ou interne (élus, agents, prestataires, clés USB, mots de passe faibles...). Dans tous les cas, elles utilisent des vulnérabilités techniques, juridiques, organisationnelles ou humaines.

Les communes et les intercommunalités doivent s'organiser pour répondre à ces nouveaux enjeux

Devant les risques d'attaques accrus et les usages numériques qui se développent, notamment le télétravail, on ne peut que recommander aux communes et aux intercommunalités d'investir pour développer la protection de leur système d'information* et se prémunir contre un « sinistre numérique ».

Il convient en premier lieu de se doter d'une gouvernance renforcée pour mobiliser efficacement les services et impliquer les élus qui doivent opérer des choix stratégiques et budgétaires. Il convient bien entendu de l'adapter à la taille de la commune, pour les plus petites, un adjoint pourra être en charge de ces sujets, pour les plus grandes, un comité de pilotage réunissant élus et techniciens pourra se mettre en place. La gestion de ce dossier pourra également se faire de manière mutualisée entre plusieurs communes ou via des structures de mutualisation telles que les opérateurs publics des services numériques, par exemple.

QUATRE CHANTIERS DOIVENT ÊTRE LANCÉS PRIORITAIREMENT :

- **la conduite du changement et la sensibilisation des agents**
  Le comportement humain étant un facteur multipliant ou réduisant les risques, cet aspect devient prioritaire pour mener une vraie politique de sécurité numérique et de protection des données.
- **la vision claire des systèmes d'information employés et leur pertinence en terme d'activités et de services rendus**
  Pour y parvenir, il faut établir un inventaire patrimonial des systèmes d'information, des installations matérielles, et des applications, sous la forme d'une cartographie, s'interroger sur le risque numérique généré par chacun d'entre eux et enfin élaborer un plan d'action de réduction des risques.
- **l'analyse des clauses contractuelles des marchés de prestations informatiques intégrant ou pas le risque numérique**
- **l'élaboration d'un plan de crise**
  Les victimes de cyberattaques sont souvent confrontées à la fois à la gestion d'impacts immédiats et à la mise en place de réponses pérennes. L'existence de plans ou de procédures de continuité et de reprise d'activité est cruciale dans le cas d'une crise d'origine numérique.

Les élus communaux et intercommunaux ne sont pas seuls face aux risques

En dépit des efforts pour réduire les risques numériques, un incident de sécurité numérique peut se produire. Différents organismes publics et dispositifs de réponse ou d'aide sont à la disposition des communes et des intercommunalités pour faire face à la situation rencontrée.

Elles peuvent à la fois s'informer auprès de l'ANSSI et de la plateforme cybermalveillance.gouv.fr pour se prémunir d'une attaque et les saisir lorsque le risque est devenu réalité.

Enfin, la commune ou l'intercommunalité devra se mobiliser pour accompagner ses agents et prendre en charge les risques psychologiques que pourra provoquer une attaque numérique.

La synthèse des recommandations

Les différentes recommandations recensées dans ce document sont reprises en synthèse ci-dessous et réparties en quatre grands thèmes : gouvernance, moyens, résilience et relations avec des tiers.

GOUVERNANCE

Recommandations	
1	Prévoir un dispositif financier d'accompagnement pour une gouvernance partagée entre les communes et les intercommunalités.
2	Promouvoir la mutualisation, afin que les plus petites communes puissent s'appuyer sur l'expertise et les moyens financiers des structures plus importantes. Des économies substantielles pourront être réalisées grâce à l'émergence de groupements d'achats.
6	Inciter les communes et les intercommunalités à entreprendre une réflexion sur le développement et le renforcement de la sécurité numérique.
7	Mutualiser les services de sécurité numérique à travers le mécanisme de « service commun » entre les intercommunalités et leurs communes membres ou le recours à un syndicat mixte « numérique » déjà existant entre plusieurs collectivités.
8	Motiver les décideurs à prendre les mesures de gouvernance.
9	Transmettre la prise de conscience du risque numérique et porter cette responsabilité au plus haut niveau de l'organisation.
10	Organiser une gouvernance adaptée au contexte local, par exemple un comité simple composé d'élus et de techniciens, voire des formes d'organisation plus élaborées (comité technique, commission, élu référent).
11	Porter la démarche au plus haut niveau de la commune ou de l'intercommunalité et en assurer le pilotage sur le long terme.

MOYENS

Recommandations	
3	À l'inverse des pratiques majoritaires actuelles, il serait préférable d'évaluer d'abord les exigences en matière de sécurité numérique pour pouvoir ensuite dimensionner le budget à allouer.
4	Opérer les choix stratégiques et budgétaires issus des réflexions associant les élus et les techniciens.
5	Insister auprès du préfet pour obtenir des financements dédiés.
12	Miser sur l'humain et accompagner les communes et les intercommunalités à sensibiliser leurs agents aux bonnes pratiques.
13	Prioriser un accompagnement des agents qui produisent, traitent et exploitent des données sensibles. Un bon moyen d'acculturer les personnels peut être de s'appuyer sur le règlement général de la protection des données (RGPD) et les nouvelles pratiques induites.
14	S'appuyer sur le guide « Maîtrise du risque numérique – L'atout confiance » sur le site de l'ANSSI afin d'évaluer, organiser, bâtir et piloter un socle complet de sécurité.
19	Un travail préalable de cartographie des données et des flux, de classification des données et d'analyse des risques devra avoir été réalisé en amont de la souscription d'une offre d'informatique en nuage (cloud).
20	Ne souscrire, si possible, qu'à des offres d'informatique en nuage auprès de prestataires de confiance et notamment ceux disposant d'un Visa de sécurité de l'ANSSI . Dans le cadre de cette démarche, l'ANSSI a élaboré le référentiel SecNumCloud en vue de permettre la qualification de prestataires de services d'informatique en nuage. Sont concernés les prestataires d'informatique en nuage offrant des services de type SaaS (Software as a service), PaaS (Platform as a service) et IaaS (Infrastructure as a service).

RÉSILIENCE

Recommandations	
21	Rédiger le volet numérique du plan de crise de la commune ou de l'intercommunalité en s'appuyant sur les dispositifs existants (exemple : plan communal de sauvegarde (PCS)). L'intégrer au plan communal de sauvegarde de la commune et/ou à un Centre de ressources numériques territorial (CRNT).
22	Élaborer des éléments de langage liés à des scénarios de cyberattaque avant que la crise ne survienne. Intégrer ces éléments de langage au plan de communication de crise.
23	Faire un exercice de gestion de crise avec un scénario de cyberattaque.
24	Développer un scénario de cyberattaque dans le plan de continuité d'activité (PCA)/ plan de reprise d'activité (PRA) de la collectivité (privilégier le scénario d'attaque par rançongiciel *).
25	Maintenir le PCA/PRA à un niveau opérationnel via l'organisation régulière d'exercices.
26	Mettre en place, former et animer un réseau de référents locaux en matière de sécurité numérique.
27	Fournir son plan de crise à ses fournisseurs afin qu'ils l'appliquent (chaîne de réponse).
28	Désigner un responsable qui sera chargé de diffuser les informations tant en interne qu'à l'extérieur de la collectivité.
29	Tenir « une main courante » durant la crise afin de faciliter la formalisation du retour d'expérience.
30	Accompagner les agents en cas de cyberattaque pour améliorer la résilience collective.

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.

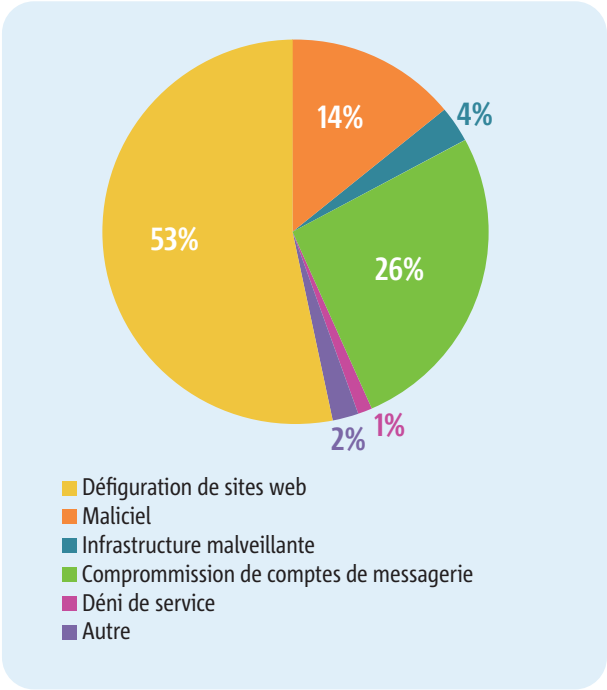
Le périmètre retenu pour cette étude comprend tous les incidents de sécurité d'origine cyber affectant les communes, les communautés de communes, d'agglomération, urbaines ainsi que les métropoles françaises traités par l'ANSSI tout au long de l'année 2019.

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.

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).

- 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

2. Comment s'organiser pour prévenir le risque ?

1. Le coût de l'insécurité

Pour la commune ou l'intercommunalité, sécuriser son système d'information se construit grâce à un investissement en moyens humains, financiers et techniques. Au même titre qu'une assurance, ceux-ci sont nécessaires pour se prémunir contre un «sinistre numérique».

Devant les risques d'attaques accrus et les usages numériques qui se développent, les collectivités investissent pour développer la protection de leur système d'information.

L'investissement se fait suivant trois axes :

• la dotation de compétences au sein des collectivités

On observe que les plus importantes directions informatiques, en termes d'effectif, s'organisent afin de dédier une ressource ou même une équipe à la sécurité des systèmes d'information. L'objectif est de garantir un pilotage tant sur le plan technique qu'organisationnel de la protection, impliquant son intégration dans le cycle de vie de tout projet numérique, de la conception à l'évolution jusqu'au retrait du système.

Plusieurs profils et organisations se développent comme la création de postes, externalisés et/ou partagés, de responsable de la sécurité des systèmes d'information (RSSI) et, via la mise en œuvre du RGPD au sein des collectivités, de délégués à la protection des données (DPD/DPO). Certaines communes ou intercommunalités proposent également des séances de sensibilisation à la sécurité numérique pour l'ensemble de leurs agents. Il est indéniable que la taille des collectivités influence la dotation en régie de ressources dédiées : les plus importantes consacrent au sein de leurs DSI des moyens humains, tandis que les plus petites font davantage le choix de l'externalisation auprès notamment de partenaires privés ou de structures de mutualisation.

• la mise en place d'outils dédiés

En parallèle, les communes et les intercommunalités doivent renforcer techniquement la sécurité de leurs réseaux et de leurs équipements via la mise en place d'outils dédiés. Aujourd'hui, elles se dotent de moyens hétérogènes en matière de protection des matériels et des logiciels pour leurs réseaux, serveurs et postes informatiques, y compris nomades : firewall, antivirus, gestion des accès et des identités, sécurisation des points d'accès Wifi et des terminaux mobiles (téléphone et tablettes), etc.

S'ajoute à ces moyens techniques le maintien en condition de sécurité (MCS) des infrastructures de protection et de tout élément numérique constituant leur système d'information. Maintenir en condition de sécurité un système consiste à s'assurer que tout au long de son cycle de vie ses besoins de sécurité sont maintenus en tenant compte de l'évolution du contexte de menaces et des risques associés. Il implique notamment l'actualisation régulière des analyses de risque, la définition et le suivi des habilitations d'accès autant que l'application des mises à jour du système.

• la mobilisation de moyens financiers

Le corollaire de l'ensemble de ces mesures sera le niveau d'investissement alloué par la commune ou l'intercommunalité à la mise en place de la cybersécurité.

Proportionnellement, quelle que soit la taille des collectivités, sur un échantillon de collectivités sollicitées restreint, on peut observer que celles-ci investissent de manière similaire entre 4 et 7% du budget d'investissement informatique[1], avec d'importantes variations annuelles pour les les communes et les intercommunalités de moins de 10 000 habitants.

(1) La recommandation de l'ANSSI se situe, elle, dans une fourchette comprise entre 5 et 10%

Ce constat[2] confirme une prise de conscience uniforme des enjeux de la sécurité numérique mais cache une disparité importante entre les moyens mis en œuvre dans les collectivités, compte tenu de leur taille, pour y faire face. La typologie de la collectivité n'influe pas sur les moyens développés. Les départements, intercommunalités ou communes investissent de manière équivalente. Cependant, force est de constater que plus la taille d'une entité est importante, meilleure est la structuration des équipes, les moyens techniques mis en œuvre et les moyens financiers dédiés.

Les pratiques en termes de développement de la protection doivent évoluer. Il est souhaitable que le niveau de disponibilité attendu du système d'information, impactant les besoins en termes de protection, vienne conditionner les moyens à mettre en œuvre et non l'inverse.

Recommandations	
1	Prévoir un dispositif financier d'accompagnement pour une gouvernance partagée entre les collectivités et les intercommunalités.
2	Promouvoir la mutualisation, afin que les plus petites communes et intercommunalités puissent s'appuyer sur l'expertise et les moyens financiers des collectivités plus importantes. Des économies substantielles pourront être réalisées grâce à l'émergence de groupements d'achat.
3	À l'inverse des pratiques majoritaires actuelles, il serait préférable d'évaluer d'abord les exigences en matière de sécurité numérique pour pouvoir ensuite dimensionner le budget à allouer.
4	Opérer les choix stratégiques et budgétaires issus des réflexions associant les élus et les techniciens.
5	Insister auprès du préfet pour obtenir des financements dédiés.

2. Favoriser une prise de conscience en interne

La prévention passe également par une prise de conscience interne des risques auxquels sont exposées les communes et les intercommunalités. Cette prise de conscience peut être favorisée par différents leviers.

En premier lieu, la sensibilisation des acteurs aux enjeux et aux risques de sécurité apparaît comme un levier essentiel. Dans le même esprit, relayer l'actualité au moyen d'une veille active est une piste intéressante.

L'audit de sécurité informatique est également un levier extrêmement puissant en ce sens qu'il permet à tous les acteurs d'avoir une vision objective des vulnérabilités et du niveau d'exposition aux risques du système d'information tout en proposant de partager une vision commune de ce que pourraient être les axes d'amélioration. Les acteurs sont, de fait, associés à la conduite du changement et deviennent dès lors pro-actifs dans la conduite du plan d'amélioration à mettre en place.

FOCUS

Résistance au changement

En matière de politique de cybersécurité, la résistance au changement des entreprises est forte, y compris après une attaque informatique. C'est le principal enseignement d'un rapport de l'éditeur de logiciels CyberArk sur les menaces avancées.
Ce rapport[3] (Global Advanced Threat Landscape Report 2018) est basé sur une enquête internationale menée par le cabinet Vanson Bourne. 1300 responsables de la sécurité informatique, décideurs métiers et développeurs, ont été interrogés. Globalement, 46 % des organisations concernées modifient rarement leur stratégie de sécurité de manière significative, même après avoir été la cible d'une cyberattaque. En France, ce taux est bien plus élevé : 61 %.

(2) Basé sur un échantillonnage réalisé auprès de communes et intercommunalités représentatives et de tailles différentes
(3) Référence : https://www.silicon.fr/cybersecurite-resistance-changement-france-201805.html

3. Une gouvernance renforcée

La mise en œuvre d'une politique de sécurisation des outils et données numériques nécessite bien évidemment une organisation portée par une gouvernance renforcée pour mobiliser efficacement les services et impliquer les élus qui doivent opérer des choix stratégiques et budgétaires. En outre, ce dossier peut être géré de manière mutualisée entre plusieurs communes et l'intercommunalité d'appartenance peut tenir un rôle pivot d'organisateur et de facilitateur. Une gouvernance à l'échelle intercommunale, impliquant étroitement les communes, doit être pensée en conséquence.

FOCUS

La mutualisation via le service commun

La loi a prévu un dispositif spécifique pour permettre aux EPCI à fiscalité propre et à leurs communes membres de coopérer et gérer de manière mutualisée des fonctions support (ressources humaines, commande publique, informatique…). Ces services communs sont en principe gérés par l'EPCI à fiscalité propre mais peuvent, si le conseil communautaire en délibère ainsi, être confiés à une commune membre (ville centre par exemple). Ils ont vocation à exercer des missions fonctionnelles ou opérationnelles pour l'intercommunalité, les communes membres et leurs établissements publics rattachés (CCAS ou CIAS par exemple).

Régi par la loi (article L 5211-4-2 du Code général des collectivités territoriales - CGCT), le service commun est potentiellement source d'économies. Il peut faciliter les économies d'échelle et/ou le développement de nouvelles expertises : tel peut être le cas notamment pour les acquisitions de licences et pour le matériel informatique (un groupement d'achats peut s'avérer nécessaire). Les gains en termes de sécurité juridique et technique sont également importants pour les petites communes et intercommunalités, car elles bénéficient d'une expertise qu'elles ne peuvent acquérir seules. Ce peut être la mise à disposition aux communes membres d'une personne ressource en matière d'aide et de conseil en cybersécurité.

La mise en place d'un service commun fait l'objet d'un encadrement juridique spécifique précisé à l'article L 5211-4-2 du CGCT. Il suppose en particulier la signature d'une convention entre les parties qui détermine le nombre de fonctionnaires et d'agents non titulaires transférés, la consultation préalable des comités techniques compétents, la mise en commun des moyens et des ressources.

En outre, il convient de signaler que la loi du 20 juin 2018 relative à la protection des données personnelles et son article 31 incitent les collectivités locales et les intercommunalités à établir des partenariats pour gérer en commun les charges et obligations liées au traitement de données à caractère personnel.

Des formules simples et déjà éprouvées existent. Il convient de les adapter selon la configuration de la commune (dimension de la commune, association de plusieurs communes au sein d'une intercommunalité par exemple).

Le plus fréquemment, un comité de pilotage, réunissant élus et techniciens, peut être constitué. Il est présidé par un élu référent.

Dans les plus petites communes, un adjoint au maire pourra être en charge de ce sujet.

Enfin, pour des organisations plus complexes, rassemblant un plus grand nombre de communes ou une intercommunalité par exemple, pourront être retenus :

- un comité technique composé des agents et/ou salariés pour apporter des préconisations techniques et des éclairages budgétaires ;

- **une commission composée d'élus** (associant notamment les élus des communes membres d'une intercommunalité) chargée de proposer les choix et les arbitrages aux instances décisionnelles (assemblées délibérantes). Elle peut se faire accompagner par des représentants du comité technique ;

- **un élu référent** au sein de la commission. Pour une plus grande efficience, il est préconisé que l'élu référent siège aussi dans les instances décisionnelles afin d'apporter si nécessaire les informations utiles à la prise de décision.

Bien évidemment chaque mode de gouvernance comporte son lot d'avantages et d'inconvénients qu'il convient de soupeser avant d'engager la démarche. Il est tout à fait envisageable, par exemple, de rattacher le suivi de ce dossier à une commission déjà existante.

Recommandations

6	Inciter les communes et les intercommunalités à entreprendre une réflexion sur le développement et le renforcement de la sécurité numérique.
7	Mutualiser les services de sécurité numérique à travers le mécanisme de « service commun » entre les intercommunalités et leurs communes membres ou le recours à un syndicat mixte déjà existant entre plusieurs collectivités.
8	Motiver les décideurs à prendre les mesures de gouvernance.
9	Transmettre la prise de conscience du risque numérique et porter cette responsabilité au plus haut niveau de l'organisation.
10	Organiser une gouvernance adaptée au contexte local, par exemple un comité simple composé d'élus et de techniciens, voire des formes d'organisation plus élaborées (comité technique, commission, élu référent).
11	Porter la démarche au plus haut niveau de la commune ou de l'intercommunalité et en assurer le pilotage sur le long terme.

4. La conduite du changement

Il est indispensable d'intégrer fortement l'accompagnement à la conduite du changement auprès des agents. Les agents sont principalement ceux qui produisent de la donnée, qu'elle soit à caractère personnel ou non, et leur adhésion est indispensable.

La conduite du changement comprend l'ensemble des actions à mettre en œuvre afin d'accompagner le déploiement d'une solution ou d'une nouvelle organisation dans le but que celles-ci aboutissent conformément aux objectifs recherchés.

Elle doit permettre à tous les acteurs du projet (de l'exécutif à l'utilisateur final, en passant par le chef de projet) de comprendre les enjeux du projet, de se les approprier et enfin d'être associés aux changements qui vont l'accompagner.

Cette conduite du changement est d'autant plus nécessaire que la sécurité numérique est un sujet transverse au sein de la collectivité et que sa gouvernance influera donc sur tous les niveaux de l'organisation.

Le facteur humain représentant l'essentiel des facteurs de risques, cet aspect devient prioritaire pour mener une vraie politique de sécurité numérique et de protection des données dans les structures.

• Dans un premier temps, il est recommandé de proposer une structure identifiée – quel que soit le niveau[4] choisi - pour les accompagner dans ces changements de pratiques. L'avantage sera d'avoir un interlocuteur identifié qui sera un point d'entrée « ressources » avec des guides de bonnes pratiques, des modes d'emploi, des liens vers des référents locaux, etc.

• Dans un second temps, dépendant de la structure précédente ou non, la conduite du changement sera plus efficace si des actions d'accompagnement et de formation sont possibles dans la commune ou l'intercommunalité. Il s'agit d'accompagner la mise en œuvre mais également d'expliquer les enjeux et les nécessités (le rôle pédagogique est essentiel dans la réussite des transformations internes).

• Structure par structure, des sessions de sensibilisation, telles qu'elles ont pu être menées, par exemple par la ville de Vannes dès 2017 avec 1 200 agents formés en demi-journée au RGPD et aux bonnes pratiques de la sécurité numérique, sont particulièrement recommandées.

• Les nouveaux outils numériques permettent également d'organiser des sessions vidéo ou des « quizz » qui rendront les formations/sensibilisations plus aisées et plus ludiques pour les agents.

Cette politique d'accompagnement pourrait être déclinée à plusieurs niveaux en s'appuyant sur le leitmotiv suivant : une meilleure efficacité grâce à une organisation resserrée, plus de réactivité grâce à l'agilité, un renforcement des compétences grâce à des organisations accompagnatrices légitimes.

FOCUS

Formation

Sur le fond, les formations utiles aux agents territoriaux pour les sensibiliser à la sécurité numérique reposent essentiellement sur le fait que les données qu'ils collectent sont propriété du citoyen ou de la collectivité et que la totale responsabilité incombe au collecteur ainsi qu'aux dirigeants de leurs collectivités, à savoir les maires ou les présidents d'intercommunalité. La connaissance parfaite du RGPD et le travail de sensibilisation du délégué à la protection des données (DPO) sont de solides bases pour mettre en œuvre les bonnes pratiques de la sécurité numérique.

Les communes et les intercommunalités peuvent être accompagnées pour appréhender les enjeux de la sécurité numérique par : leur DPO (interne ou externe), un syndicat mixte spécialisé dans le numérique, le centre de gestion du département éventuellement, les cabinets de consultants spécialisés... L'ANSSI propose des conseils et des référentiels de formation sur son site internet (https://www.ssi.gouv.fr/administration/formations/). L'AMF a sensibilisé le CNFPT à l'intérêt de formations spécifiques pour tous les agents territoriaux. La communication interne peut également jouer un rôle de mobilisation collective via un site extranet dédié aux agents ou encore via une lettre interne spécifique aux agents. La sécurité numérique doit devenir un sujet abordé en continu auprès des salariés (bonne pratiques, extraits d'articles illustrant des attaques, etc.). Il est important de transmettre les informations de manière ludique, courte mais percutante pour marquer les esprits.

Recommandations

12	Miser sur l'humain et accompagner les communes et les intercommunalités pour sensibiliser leurs agents aux bonnes pratiques.
13	Prioriser un accompagnement des agents qui produisent, traitent et exploitent des données sensibles. Un bon moyen d'acculturer les personnels peut être de s'appuyer sur le règlement général de la protection des données (RGPD) et les nouvelles pratiques induites.

(4) Une fédération nationale, une association régionale ou départementale, etc.

5. Bâtir son socle de sécurité numérique

Les communes et les intercommunalités doivent tout d'abord avoir une vision claire des systèmes d'information employés et de leur pertinence en termes d'activités et de services rendus. Pour y parvenir, il faut établir un inventaire patrimonial des systèmes d'information, des installations matérielles, et des applications, sous la forme d'une cartographie[5]. Cette vision permettra de définir les objectifs de sécurité attendus des différents systèmes, mais aussi d'évaluer leurs degré d'importance (criticité).

La cartographie peut être plus ou moins détaillée et inclure, par exemple, les biens matériels, les logiciels, les réseaux de connexion, mais aussi les informations, activités et processus qui reposent sur ces biens. Pour être complète, la cartographie doit également identifier les acteurs de l'écosystème en lien direct ou indirect avec la commune ou l'intercommunalité : personnels, administrés, partenaires, cotraitants, prestataires, sous-traitants ou fournisseurs, etc.

Une fois cet environnement défini, il faut s'interroger sur le risque numérique généré par chacun et la menace potentielle représentée par chaque partie prenante sur les systèmes d'information cartographiés. Par exemple, une partie prenante peut être considérée comme « critique » dès lors qu'elle est susceptible de constituer un vecteur d'attaque pertinent, du fait de son accès numérique privilégié aux systèmes étudiés, de sa vulnérabilité ou de son exposition. À contrario, un système d'information peut être également considéré comme « critique » de par le service qu'il rend et les impacts engendrés, en cas d'un arrêt non programmé ou l'exfiltration de données personnelles.

Ensuite, les risques numériques pesant sur l'environnement et les systèmes d'information critiques doivent être évalués sur la base de leurs gravités et de leurs vraisemblances, puis formalisés au travers de scénarios[6] de risque. Ces scénarios devront également estimer les impacts et le coût de chacun d'eux sur la collectivité et les services rendus.

Enfin, sur la base des scénarios de risque précédemment identifiés, il conviendra de travailler sur les moyens de réduire les risques en se basant sur des mesures techniques, organisationnelles ou humaines. Ces mesures doivent être formulées par un plan d'action de réduction des risques et l'investissement financier associé doit être validé en accord avec les choix stratégiques et budgétaires des élus.

Les étapes décrites précédemment participent à la démarche d'homologation[7] de sécurité dont l'objectif est de faire connaître et comprendre, aux responsables comme aux maîtres d'ouvrage, les enjeux, le cadre légal et réglementaire et les risques de sécurité numériques qui pèsent sur ses systèmes d'information.
Ce processus doit aboutir à un acte formel, celui de la décision, prise par le responsable de l'organisation quant aux ressources allouées pour les réduire.

Recommandation

14 S'appuyer sur le guide « Maîtrise du risque numérique – L'atout confiance » sur le site de l' ANSSI[8] afin d'évaluer, organiser, bâtir et piloter un socle complet de sécurité.

L'ANSSI a publié, en janvier 2020, un guide rappelant l'essentiel de la réglementation concernant la sécurité numérique des collectivités territoriales [référentiel général de sécurité (RGS), règlement général sur la protection des données (RGPD)...].

https://www.ssi.gouv.fr/guide/securite-numerique-des-collectivites-territoriales-lessentiel-de-la-reglementation/

(5) Pour plus d'informations, voir le guide de l'ANSSI "Cartographie du système d'information, Guide d'élaboration en 5 étapes" publié en octobre 2018
(6) Pour en savoir plus sur la formalisation des scénarios de risque, se reporter à la méthode EBIOS Risk Manager, publié par l'ANSSI en 2018, https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/
(7) Voir le guide de l'ANSSI «L'homologation de sécurité en neuf étapes simples» publié en 2017, www.ssi.gouv.fr/guide-homologation-securite/
(8) Voir le guide de l'ANSSI, https://www.ssi.gouv.fr/guide/maitrise-du-risque-numerique-latout-confiance/

6. Les clauses contractuelles

L'analyse des clauses contractuelles des marchés en cours et à venir est une priorité. En effet, il est impératif d'identifier dans les contrats de prestation ou de sous-traitance quels pourraient être les manques ou les faiblesses en matière de sécurité numérique. Il n'est pas rare de constater que les clauses contractuelles vont à l'encontre des objectifs de sécurité de la collectivité ou que tout simplement aucune clause ne permet de garantir une bonne sécurité (délai de retour à la normale, sauvegarde/restauration, réversibilité...).

Une fois ce travail d'inventaire réalisé, il est nécessaire de définir des modèles de clauses contractuelles à inclure dans les futurs contrats. Ces clauses se nourrissent des conclusions de la cartographie des risques et des politiques de sécurité. Leur rédaction suppose de s'entourer de compétences particulières (juridique et technique).

Dans le cas d'une gestion déléguée (délégation de service public par exemple), la commune ou l'intercommunalité choisit de faire gérer un ou plusieurs de ses services par un ou plusieurs délégataire(s). Elle définit alors dans le cahier des charges de la convention établie avec le délégataire les conditions de gestion du système d'information en général et des données personnelles en particulier. Il convient de noter que la délégation de gestion d'une compétence n'implique pas de transfert de responsabilité. Le délégant et le délégataire sont conjointement responsables de la sécurité en général.

Il est alors fortement conseillé de préciser dans la convention les clauses explicites et expresses rappelant la répartition des responsabilités et obligations entre les deux partenaires.

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 le guide « Maîtriser les risques de l'infogérance » de l'ANSSI sur son site Internet.
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, les clauses explicites et express précisant la répartition des responsabilités et 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.
19	Un travail préalable de cartographie des données et des flux, de classification des données et d'analyse des risques devra avoir été réalisé en amont de la souscription d'une offre d'informatique en nuage.
20	Ne souscrire, si possible, qu'à des offres d'informatique en nuage (cloud) auprès de prestataires de confiance et notamment ceux disposant d'un Visa de sécurité de l'ANSSI . Dans le cadre de cette démarche, l'ANSSI a élaboré le référentiel SecNumCloud en vue de permettre la qualification de prestataires de services d'informatique en nuage. Sont concernés les prestataires d'informatique en nuage offrant des services de type SaaS (Software as a service), PaaS (Platform as a service) et IaaS (Infrastructure as a service).

FOCUS

Informatique en nuage

L'informatique en nuage (en anglais *cloud computing*) est définie par le Journal Officiel du 6 juin 2010 comme « un mode de traitement des données d'un client, dont l'exploitation s'effectue par l'Internet, sous la forme de services fournis par un prestataire ».
Ce traitement de données se fait par la mutualisation de ressources informatiques du prestataire, puissance de calcul et stockage, selon les besoins de ses différents clients.

Aussi nous retrouvons dans la mise en œuvre de ce type de solution les risques inhérents à l'infogérance dite « classique » auxquels s'ajoutent les risques liés à :

- **la protection des données à caractère personnel :** le règlement européen (RGPD) encadre notamment les transferts internationaux de données ;
- **la perte de gouvernance,** le client de prestations d'informatique en nuage concède un contrôle total à son prestataire, y compris dans la gestion des incidents de sécurité ;
- **la dépendance technologique,** il n'est pas toujours compris dans les offres de l'informatique en nuage une transférabilité ;
- **la réversibilité du service :** il convient de prévoir au moment de la contractualisation initiale les termes et les modalités selon lesquels la collectivité se verra remettre l'ensemble des données nécessaires au changement éventuel de prestataires ;
- **l'isolation défaillante,** le principe de mutualisation des ressources présente un risque pouvant porter préjudice à l'intégrité ou la confidentialité des données hébergées ;
- **l'effacement incomplet ou non sécurisé,** il n'y a pas ou peu de garantie qu'une donnée soit réellement effacée ou qu'il n'existe pas de copie stockée dans le nuage.

Il est difficile de se prémunir de ces risques car le client souscrit à une offre par validation d'un contrat type qu'il est bien souvent impossible de modifier ou de personnaliser notamment par l'ajout de clauses particulières en matière de sécurité.
Au vu de ces risques, il est nécessaire de bien maîtriser les ressources qui seront éligibles à ce mode d'hébergement. Il convient de réaliser une cartographie de son système d'information (données, flux réseaux…), d'engager un processus de classification des données par sensibilité et criticité d'exposition et réaliser une analyse de risque adaptée aux enjeux de la collectivité.
Une fois cette qualification des ressources éligibles, le choix d'une offre d'informatique en nuage sécurisée est essentiel. Dans la mesure du possible, les offres certifiées par l'ANSSI sont à privilégier, en particulier si les données exploitées sont considérées comme sensibles (https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf).

Trois documents de référence apportent un nombre considérable de recommandations tant techniques que juridiques :

- Les « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing » de la CNIL : https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf
- « Maîtriser les risques de l'infogérance » de l'ANSSI : https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf
- Les prestataires de service d'informatique en nuage : https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/

7. Le plan de crise

A - Qu'est-ce qu'une crise de sécurité numérique dans le contexte d'une collectivité ?

Face à la transformation numérique et aux risques qui s'y rapportent, les communes et les intercommunalités doivent se préparer à devoir gérer une crise de sécurité du numérique. Même s'il n'y a pas à proprement parler de crise de sécurité du numérique mais des crises ayant pour fait générateur une ou des atteintes à la sécurité du numérique. Les situations de crise sont en effet définies par les conséquences, c'est-à-dire les impacts sur les activités des collectivités. Ces impacts sont générés par l'indisponibilité, la perturbation ou le sabotage des systèmes d'informations qui soutiennent ces activités. Ces crises, d'ampleur différente, pourraient avoir les effets (non exhaustifs) suivants :

- incapacité à réaliser la mission de service public suite à l'indisponibilité ou le sabotage complet du système d'information de la collectivité ;
- divulgation massive de données d'état civil, d'identité ou de données d'identification contenues dans les systèmes d'information de la collectivité ;
- non-respect des obligations légales engageant la responsabilité juridique des élus ;
- atteinte à l'image de la commune, de l'intercommunalité ou des élus dans les médias ;
- pertes financières importantes.

B - Quelles sont les spécificités des crises dont le fait générateur est une atteinte à la sécurité numérique ?

Du fait de la nature technologique de ces crises et de la complexité des systèmes d'information, les acteurs au cœur de la gestion de crise sont les experts techniques.

De plus, la résolution d'une crise de sécurité du numérique n'est pas immédiate. En effet, l'investigation numérique et la remédiation des systèmes infectés nécessitent un temps long. Les victimes de cyberattaques sont ainsi confrontées à la fois à la gestion d'impacts immédiats pouvant être étendus et à la mise en place d'une réponse viable sur le long terme. L'existence de plans ou de procédures de continuité d'activité est ainsi cruciale dans le cas d'une crise de sécurité du numérique.

Enfin, la révélation d'une situation de crise d'origine informatique dans l'espace public peut soulever des interrogations sur la protection des données personnelles et plus généralement sur le niveau de sécurité informatique de la collectivité.

C - Les fondamentaux de la gestion de crise numérique

Principes généraux

Compte-tenu des spécificités rappelées, les trois piliers de la gestion d'une crise numérique sont :

- **la résolution technique,** à savoir l'investigation numérique et la remédiation des systèmes infectés. Ces actions peuvent s'étaler sur plusieurs semaines ;
- **la continuité d'activité** pour assurer les services essentiels de la collectivité dans la perspective d'une situation dégradée qui peut durer dans le temps ;
- **la mise en place d'une communication** appropriée pour accompagner les parties prenantes sur le suivi de la crise. Cela inclut la communication interne vers les agents de la collectivité et la communication externe vers les usagers du service public local et les médias.

Ces spécificités sont à prendre en compte, cependant il est primordial de retenir que la gestion d'une crise liée à la sécurité du numérique et notamment la gestion de la continuité d'activité ou la communication de crise ne diffèrent pas fondamentalement d'une crise avec une autre origine (intempéries, accident majeur, etc.). En termes d'organisation (acteurs, cellule de crise, formation, exercice) et/ou d'outillage (plans, main courante), les fondamentaux de la gestion de crise s'appliquent.

L'intégration d'un volet numérique dans les plans de crise des collectivités territoriales

Les plans de crise des communes et des intercommunalités doivent être complétés par un volet numérique. Lors de la cartographie des acteurs principaux de la gestion de crise, au premier rang desquels se situent les élus – le maire ou ses adjoints pour une

commune, le président ou ses vice-présidents pour une intercommunalité, l'enjeu sera d'associer les experts techniques identifiés préalablement et de faire en sorte qu'ils se comprennent et travaillent ensemble. En cas de compromission de données à caractère personnel, la CNIL devra être notifiée.

Pour assurer une résolution technique efficace, il est nécessaire de s'assurer que la direction des systèmes d'information est préparée à répondre à un incident de grande ampleur en identifiant par exemple en amont les prestataires extérieurs susceptibles d'intervenir en cas d'incident. Le dispositif national d'assistance aux victimes de cybermalveillance[9] (www.cybermalveillance.gouv.fr) recense ces prestataires.

Pour les collectivités désignées opérateurs d'importance vitale et/ou opérateur de service essentiel, une assistance peut être demandée à l'ANSSI en cas d'incident. Dans ce cas, il est recommandé de prendre attache auprès du CERT-FR de l'ANSSI (lien : https://www.cert.ssi.gouv.fr/contact/).

La planification de continuité d'activité

Les communes et les intercommunalités, tout comme les administrations publiques et les entreprises, doivent se préparer à affronter des évènements soudains, susceptibles d'altérer sérieusement leur fonctionnement (incendies, intempéries, crises sanitaires, menaces terroristes, etc.). Parmi ces risques, la menace de cyberattaque doit être prise en compte. Il s'agit d'identifier les scénarios liés à des cyberattaques à intégrer dans le plan de continuité des activités (PCA), par exemple, le scénario d'attaque par rançongiciel. Pour ce scénario, il convient de mettre en place une solution de sauvegarde hors ligne des données essentielles de la collectivité. Des tests de restauration des données sauvegardées doivent être menés régulièrement afin de s'assurer de la capacité à récupérer les données en cas d'incident.

Des méthodologies existent pour élaborer ces plans, en particulier celui qui a été rédigé par le Secrétariat général de la défense et de la sécurité nationale : www.sgdsn.gouv.fr (guide édité en 2013 dont les principes restent d'actualité : ce guide décrit les principales étapes et comprend de nombreuses fiches pratiques).

Enfin, le plan VIGIPIRATE, dispositif permanent de vigilance, de prévention et de protection, associant tous les acteurs du pays et notamment les collectivités territoriales contient un volet sur la sécurité du numérique. Les communes et les intercommunalités sont invitées à appliquer les mesures de vigilance relatives à ce volet mentionnées dans les notes de posture qu'elles reçoivent deux fois par an pour se prémunir d'attaques ou être mieux préparées en cas de survenance d'une attaque.

La communication

La communication intervient à plusieurs étapes de la gestion de crise :

En amont :

- **communiquer en interne** sur l'existence d'un plan de gestion de crise, sa mise à jour, la tenue de formations et/ou d'exercices sur la thématique pour sensibiliser les agents ;
- **préparer des éléments de langage** adaptés aux différents scénarios craints ; pendant et après la crise cf. le chapitre 3-2 (page 26).

D - Les activités complémentaires qui permettent d'assurer une bonne préparation à la gestion de crise numérique

La formation et l'entraînement

Les plans de gestion de crise doivent être connus par les personnes susceptibles d'être mobilisées. La formation est un levier indispensable pour diffuser le plan, le faire connaître et professionnaliser un vivier d'agents pouvant armer le dispositif de crise. Les exercices de gestion de crise doivent permettre d'entrainer collectivement la commune ou l'intercommunalité et de tester les procédures mises en place dans le plan. Ces exercices doivent être suivis d'un RETetour d'EXpérience (RETEX) permettant de revenir sur les faits marquants, ce qui a bien fonc-

(9) La plateforme Cybermalveillance s'adresse aux collectivités territoriales (hors OIV) avec pour objectif la mise en relation de victimes de cyberattaque avec des prestataires de proximité susceptibles de les assister techniquement via une plate-forme numérique.

tionné et ce qui doit être amélioré. Le retour d'expérience participe également grandement à la sensibilisation des personnels. Le guide pour réaliser un plan de continuité d'activité (PCA) édité par le SGDSN comprend une fiche modèle de retour d'expérience qui retrace les points d'analyse aux principales étapes de la crise pour mener à bien cette opération : caractéristique de l'évènement, alertes, gestion de crise, planification, mise en œuvre des actions, implication des parties prenantes, respect des obligations, communication, circulation de l'information.

Il est conseillé de réaliser un exercice qui a pour scénario une cyberattaque si la collectivité n'en a jamais réalisé.

La sensibilisation

Face à une menace sourde, il convient de développer une culture globale pour accroître la vigilance, notamment celle des agents territoriaux dans leurs usages numériques. Cette fonction peut être confiée au responsable des systèmes de sécurité d'information dans les structures qui en sont dotées ou à une personne ressource. Il existe de nombreux guides pédagogiques visant à diffuser de bonnes pratiques (cf Focus « Les bonnes pratiques pour prévenir les risques de malveillance numérique » page 24).

FOCUS

Les bonnes pratiques pour prévenir les risques de malveillance numérique

Prévenir le risque de malveillance numérique nécessite l'acquisition de nouveaux réflexes qui concernent autant les élus que les agents des collectivités.

Que ce soit la mise en place de mots de passe robustes, la sécurité des téléphones mobiles, la sensibilisation aux usages « pro-perso » ou aux risques d'hameçonnage, le kit du dispositif national cybermalveillance.gouv.fr propose des fiches pratiques de sensibilisation accessibles à tous les utilisateurs.
https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/

Le site internet de l'ANSSI propose quant à lui un ensemble complet de guides et de notes techniques.

Recommandations

21	Rédiger le volet numérique du plan de crise de la commune ou de l'intercommunalité en s'appuyant sur les dispositifs existants. L'intégrer au plan communal de sauvegarde (PCS) de la commune et/ou à un Centre de ressources numériques territorial (CRNT).
22	Élaborer des éléments de langage liés à des scénarios de cyberattaque avant que la crise ne survienne. Intégrer ces éléments de langage au plan de communication de crise.
23	Réaliser un exercice de gestion de crise avec un scénario de cyberattaque.
24	Développer un scénario de cyberattaque dans le plan de continuité d'activité (PCA)/plan de reprise d'activité (PRA) de la collectivité (privilégier le scénario d'attaque par rançongiciel).
25	Maintenir le PCA/PRA à un niveau opérationnel via l'organisation régulière d'exercices.
26	Mettre en place, former et animer un réseau de référents locaux en matière de sécurité numérique.
27	Fournir son plan de crise à ses fournisseurs afin qu'ils l'appliquent (chaîne de réponse).

8. La mise en place de structures supra communales

Au-delà de l'échelle intercommunale, l'agrégation des ressources autour d'un centre territorial (région, département, métropole, agglomération, centre de gestion, syndicat mixte numérique, technopole, etc.) qui disposerait d'une maturité reconnue en matière de sécurité numérique est à encourager.

L'appréciation de l'échelle de ce territoire sera fonction des intérêts, des motivations et des effets de mutualisation qui auront été envisagés au travers d'une étude d'opportunité. Autour de ce centre de ressources, le regroupement de fonctions métier existantes (notamment les Directions des systèmes d'information (DSI) et des Technologies de l'information et de la communication (TIC)) et un renforcement des métiers de la cybersécurité devront être encouragés au travers de mécanismes financiers (mutualisation des budgets et si la possibilité existe d'un abondement de ceux-ci par un mécanisme régional / national / européen).
L'évolution de structures déjà existantes ou la création de celles-ci en Centre de ressources numériques territorial (CRNT) correspondraient à ce principe de mutualisation recherché.

Ces CRNT pourraient :
- entretenir une liste de produits, de services et de prestataires de confiance (Visas de sécurité de l'ANSSI, autres labels, etc.) à destination des collectivités,
- faire de la réponse « de proximité » aux incidents de cybersécurité ;
- assurer ou relayer une veille des menaces cyber ciblant plus particulièrement les collectivités (notion de CERT Collectivités Territoriales) ;
- renforcer la formation et le recrutement de RSSI mutualisés au profit des communes et intercommunalités ;
- mettre à disposition un ou plusieurs RSSI et Délégués à la protection des données (DPO, Data Protection Officer) partagés entre les différentes parties prenantes ;
- renforcer la sensibilisation des agents par la mise en place d'une formation équivalente à celle des référents cyber sécurité TPE/PME, en liaison avec le CNFPT .

3. Que faire lorsque le risque devient réalité ?

1. Saisir un dispositif d'aide et de réponse (ANSSI, Cybermalveillance, CNIL, gendarmerie, police)

En dépit des efforts pour réduire les risques numériques, un incident de sécurité numérique peut se produire. Différents organismes publics et dispositifs de réponse ou d'aide sont à la disposition des communes et des intercommunalités pour faire face à la situation rencontrée.

Il est recommandé de consulter le site Internet de l'ANSSI qui précise les démarches qu'il convient d'engager en cas d'incident (plainte auprès des services de police ou de gendarmerie, saisine de la plateforme d'assistance aux victimes de cybermalveillance, notification auprès de la CNIL...).

Sans attendre un incident, n'hésitez-pas à contacter, lorsqu'elle existe, une structure de mutualisation numérique de proximité (liste structures adhérentes au réseau Déclic : https://www.asso-declic.fr/

notre-reseau/#cartographie) ainsi que le délégué régional de l'ANSSI (https://www.ssi.gouv.fr/agence/cybersecurite/action-territoriale/).

FOCUS

Violation des données personnelles

En application du règlement général sur la protection des données (RGPD), lorsque des données à caractère personnel ont fait l'objet d'une violation, il convient de la notifier à la CNIL dans un délai de 72 heures.
https://www.cnil.fr/fr/les-violations-de-donnees-personnelles

2. Préparer et mettre en place un plan de communication

Pendant la crise :

- désigner un responsable pour diffuser les informations. Le responsable doit être connu des interlocuteurs potentiels de l'organisation. Son autorité doit être assez élevée au sein de la hiérarchie pour que ses discours soient crédibles et ne pâtissent pas des délais inhérents au processus de validation hiérarchique car si l'organisation ne s'exprime pas, les autres le feront à sa place ;

Après la crise :

- rédiger un RETour d'EXpérience (RETEX) et afficher en interne et en externe les réussites de la gestion de crise (cf. 3-3 « Tracer les actions réalisées »). Le plan de communication de crise doit intégrer des éléments de langage liés à un scénario de cyberattaque, un rançongiciel par exemple. Dans ce cas, l'attention des médias serait portée sur la question du paiement de la rançon par la collectivité pour recouvrer ses données.

Recommandation

28 Désigner un responsable qui sera chargé de diffuser les informations tant en interne qu'à l'extérieur de la collectivité.

3. Tracer les actions réalisées

Lorsque le risque se réalise, il est essentiel de tenir une main courante de l'ensemble des évènements survenus afin de la documenter (constats, décisions, actions, etc.). Cette traçabilité permet, une fois la crise terminée, d'analyser son déroulement et sa résolution par la cellule de crise.

Mené « à froid », ce retour d'expérience a pour objectif d'identifier les points forts et les points faibles de la conduite de résolution de crise afin de prendre les mesures correctives adéquates en cas de réitération.

L'ensemble de ces mesures permet de s'inscrire dans une démarche d'adaptation et d'amélioration continue face au risque.

Recommandation

29 Tenir « une main courante » durant la crise afin de faciliter la formalisation du retour d'expérience.

4. Se préparer à prendre en charge les risques psychologiques

Plusieurs témoignages convergents de victimes travaillant dans des organisations de nature (entreprises, collectivités) et de taille différentes ont attiré l'attention des rédacteurs de ce guide. Ces victimes, témoins voire complices bien involontaires de forfaits et de délits avec parfois un préjudice financier important (plusieurs centaines de milliers d'euros), ont souvent fait part d'un traumatisme psychologique d'intensité variable où, parfois, la détresse peut se révéler profonde et réelle.

Une cyberattaque peut provoquer un véritable choc sur les agents. Ils peuvent être traversés par plusieurs sentiments : l'humiliation, la remise en cause de leurs compétences et de leur sens des responsabilités, la peur et enfin la culpabilité.

Au-delà de la culpabilité qui conduit, dans la majeure partie des cas, vers une forme de résilience c'est à dire l'acceptation d'avoir été manipulé puis abusé, un niveau d'émotion extrême a aussi donné lieu à des arrêts de travail prolongés (de plusieurs jours à plusieurs mois).

En l'état, s'il est difficile de conduire une réflexion plus poussée, nous avons souhaité attirer l'attention du lecteur et, particulièrement, des décideurs des conséquences potentiellement préjudiciables des attaques numériques en matière de santé publique et d'ordre social. À terme, la question d'une prise en charge spécifique des victimes, adossée à des études scientifiques, se posera avec de plus en plus d'acuité.

Recommandation

30	Accompagner les agents en cas de cyberattaque pour améliorer la résilience collective.

FOCUS

Illustration des effets d'une cyberattaque dans une petite commune

Suite à cette cyberattaque, le maire et la directrice générale des services (DGS) ont noté spontanément un changement radical des pratiques au sein de la mairie, mais aussi des comportements des agents. Cette aventure collective subie a eu pour effet de souder les agents dans leur responsabilité commune de protéger l'un des biens les plus précieux : les données des habitants. Ils communiquent davantage et dans le doute face à un mail « anormal », ils consultent un collègue et échangent sur la conduite à tenir et les bonnes pratiques à observer.

Glossaire

Compromission : en langage informatique, une compromission est une exposition à une menace ou à un danger suite à une action réalisée sur un ordinateur (clic de souris, mise à jour, etc). De par le risque qu'elle engendre, cette action peut alors être considérée comme une faille informatique.

Cryptomineur : un cryptomineur est un logiciel malveillant qui permet d'allouer une partie de la puissance de calcul de l'ordinateur à des opérations de minage (vérification de transactions) dédiées à la gestion des cryptomonnaies. Dans le cas précis du Bitcoin, les ressources des machines infectées par les cryptomineurs sont utilisées pour résoudre des problèmes mathématiques complexes générant la création de nouvelles unités de monnaie.

Défiguration de site Internet : la défiguration d'un site Internet est la modification du contenu de ce dernier résultant de l'intrusion d'un attaquant sur la plateforme d'administration du site. Par cette technique, l'attaquant prouve qu'il peut prendre le contrôle du site pour se faire connaître, en bloquer l'activité ou encore diffuser des messages préjudiciables à l'organisation cible.

Déni de service : une attaque par déni de service est une attaque envers un service en ligne (site Internet, téléservice, etc.) qui consiste en sa saturation par d'innombrables requêtes simultanées. Ne pouvant répondre à l'ensemble des requêtes reçues, le service attaqué devient inopérant et indisponible pour les usagers.

Hameçonnage (phishing / spearphising) : l'hameçonnage est une technique visant à dérober les données personnelles d'un individu (numéro de carte de crédit, mots de passe, etc.) via la copie d'un site officiel de confiance (banque, démarches administratives, sites gouvernementaux, etc.) dans le but d'usurper l'identité de ce dernier. Les données ainsi collectées peuvent servir à détourner de l'argent ou encore être revendues au marché noir.

Maliciel : logiciel malveillant.

Portail captif : le portail captif est une technique consistant à forcer les clients HTTP d'un réseau de consultation à afficher une page web spéciale (le plus souvent dans un but d'authentification) avant d'accéder à Internet normalement (source : Wikipedia).

Rançongiciels (*ransomware* en anglais) : un rançongiciel est un logiciel malveillant venant d'une source extérieure qui s'installe au sein d'un système d'information afin d'en bloquer tout ou partie l'accès ou de prendre en otage les données de ses utilisateurs. La résolution du problème rencontré est alors proposée en échange d'une rançon. Ces logiciels ciblent le plus souvent des données stratégiques et/ou personnelles et s'installent à la faveur d'une faille dans le système d'information pouvant avoir diverses origines : matérielle, logicielle ou humaine (défaut de mises à jour, ouverture de mails frauduleux, insertion de clé USB infectées, etc.).

Il existe deux principaux types de rançongiciels : avec ou sans chiffrement des données.

- Un rançongiciel est un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Pour y parvenir, le rançongiciel va empêcher l'utilisateur d'accéder à ses données, par exemple en les chiffrant, puis lui indiquer les instructions utiles au paiement de la rançon en échange de la restitution de ses données ;
- Les rançongiciels avec chiffrement sont également appelés cryptovirus. Les informations ciblées par ce type de logiciel sont alors rendues illisibles par le système d'information par cryptage des données ou modification des extensions de fichiers. Une rançon est alors exigée en échange de la clé de déchiffrement des données. Exemples de cryptovirus les plus connus : Petya (2016), WannaCry (2017), NotPetya (2017).

Pour aller plus loin : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf

Système d'information : un système d'information est un ensemble organisé de ressources matérielles, logicielles et humaines permettant de collecter, de traiter et de diffuser l'information d'une organisation. Sa finalité est de permettre aux différents acteurs de l'organisation d'exploiter les informations à des fins de gestion, de contrôle et/ou de prise de décision.

Concepts clés

Contexte national

• **ANSSI : Agence nationale de la sécurité des systèmes d'information**
Service du Premier ministre rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN), l'ANSSI assure la sécurité et la défense des systèmes d'information de l'État et des entreprises critiques en créant les conditions d'un environnement de confiance. Promotrice de solutions et de savoir-faire, elle participe à la protection et à la défense du potentiel économique de la nation et assure un service de veille, de détection, d'alerte et de réaction aux attaques Informatiques.
Plus d'infos : https://www.ssi.gouv.fr/

• **Cybermalveillance.gouv.fr**
Cybermalveillance.gouv.fr a pour missions d'aider les entreprises, les particuliers et les collectivités victimes de cybermalveillance, de les informer sur les menaces numériques et de leur donner les moyens de se défendre.

• **CNFPT : Centre national de la fonction publique territoriale**
Le Centre national de la fonction publique territoriale est un établissement public paritaire déconcentré dont les missions de formation et d'emploi concourent à l'accompagnement des collectivités et de leurs agents dans leur mission de service public.
Plus d'infos : www.cnfpt.fr

• **RGS : Référentiel général de sécurité**
Le Référentiel général de sécurité est le cadre règlementaire dans lequel doivent s'inscrire les échanges informatiques au sein de l'administration française et avec les citoyens (téléservices notamment). Entré en application dans sa version actuelle (2.0) depuis le 1er juillet 2014, la mise en œuvre du RGS permet d'établir des échanges sécurisés de confiance entre les administrations et avec les citoyens. Si le RGS s'impose de fait aux administrations, il constitue également une référence pratique pour les autres organismes et évolue régulièrement au gré des technologies et du contexte règlementaire (national, européen et international).

Lien vers l'arrêté du Premier ministre du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques : www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029122964&dateTexte=&categorieLien=id

• **RSSI : Responsable de la sécurité des systèmes d'information**
Au sein d'une organisation, le responsable de la sécurité des systèmes d'information est garant de la sécurisation des moyens informatiques. La désignation d'un RSSI dans une organisation (privée ou publique) ne revêt pas de caractère obligatoire mais est fortement recommandée, notamment afin de prévenir et de se prémunir des conséquences d'une interruption des services informatisés.

• **PCA : Plan de continuité d'activité**
Un plan de continuité d'activité est une procédure établie au sein d'une organisation dans le but de garantir la continuité de productivité face à l'indisponibilité des moyens informatiques possiblement survenus pour diverses raisons (défaillance des matériels, cyberattaque, etc.). L'élaboration d'un PCA relève généralement des missions du RSSI.

• **PRA : Plan de reprise d'activité**
Le plan de reprise d'activité (PRA) d'une organisation constitue l'ensemble des « procédures documentées lui permettant de rétablir et de reprendre ses activités en s'appuyant sur des mesures temporaires adoptées pour répondre aux exigences métier habituelles après un incident » (Norme ISO 22301, Sécurité sociétale —Systèmes de management de la continuité d'activité, article 8.4.5 Reprise).

• **Structures de mutualisation**
Dans la présente publication, on entend par « structure de mutualisation » une organisation publique regroupant des collectivités membres œuvrant pour ces dernières dans le champ du développement des usages numériques via la mise à disposition de services mutualisés. En France, ces structures de mutualisation prennent généralement la forme d'un syndi-

cat mixte ou d'un GIP créé à l'échelle départementale ou régionale (exemples : Mégalis en Bretagne, Manche numérique, Soluris en Charente-Maritime, Territoires Numériques en Bourgogne-Franche-Comté…).
La recommandation de regrouper plusieurs structures communales et/ou départementales à l'échelle d'un centre unique de ressources intitulé « Centre de ressources numériques territorial (CRNT) » participe concrètement à offrir une performance de services renforcée tout en optimisant les moyens financiers disponibles.

Contexte européen

- **Règlement européen eIDAS : Electronic IDentification Authentication and trust Services**

Le règlement européen « eIDAS » (Electronic IDentification Authentication and trust Services) n°910/2014 du 23 juillet 2014 a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur. Il établit un ensemble de normes régissant les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques au sein de l'Union européenne (source : Site Internet de l'ANSSI, https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/).

- **RGPD : Règlement général de protection des données personnelles**

Le Règlement général de protection des données personnelles est un règlement européen entré en vigueur le 25 mai 2018 visant à renforcer la protection des données personnelles permettant d'identifier une personne directement (identité) ou indirectement (numéro de téléphone, immatriculation d'un véhicule, etc.). Le RGPD responsabilise juridiquement les organisations opérant des traitements sur ces données (privées et publiques) et oblige, notamment, les structures publiques à désigner un Délégué à la protection des données (DPP ou DPO en anglais).
Lien vers le règlement européen en version française : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

- **DPD (ou DPO) : Délégué à la protection des données (ou Data protection officer en anglais)**

Le Délégué à la protection des données est missionné par le responsable de traitement d'une organisation afin d'assurer le respect de la mise en œuvre du RGPD. Il est le garant de la protection des données personnelles au sein de son organisme. Ses missions sont les suivantes :

1. informer et conseiller le responsable de traitement sur les risques relatifs à chaque traitement mis en place au sein de l'organisme, tant du point de vue de la protection des personnes que de l'image de l'organisme ;
2. tenir le registre exhaustif des traitements opérés et gérer la documentation associée (identification des risques, mode de collecte des données, moyens de protection mis en œuvre, etc.) ;
3. contrôler que les moyens mis en œuvre pour assurer la sécurité et la protection des données sont en adéquation avec les risques encourus ;
4. diffuser une culture Informatique et Liberté au sein de la collectivité ;
5. assurer le rôle d'interlocuteur privilégié en interne mais également vis à vis de l'extérieur pour toutes les demandes liées aux traitements des données (demandes des personnes concernées – droit d'accès, de rectification, d'opposition - ou des autorités compétentes).

Contexte international

- **CLOUD Act : Clarifying lawful overseas use of data Act [États-Unis]**

Le Clarifying lawful overseas use of data Act est une loi fédérale des États-Unis de 2018 contraignant les fournisseurs de services numériques américains [et notamment les GAFA (Google, Apple, Facebook, Amazon)] à fournir aux services de surveillance américains les données stockées sur leurs serveurs, qu'ils soient situés sur le territoire américain ou à l'étranger.
Lien vers le texte de loi du CLOUD Act (en anglais) : https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

Remerciements

Un groupe de travail, animé par le délégué à la sécurité numérique de l'ANSSI pour la région Bretagne, a été créé en octobre 2017 avec pour objectifs de proposer un état des lieux le plus exhaustif possible, de lister les freins et les leviers et de proposer 30 recommandations pouvant être adaptées à chaque collectivité territoriale, quelle que soit sa taille et son budget.

Ce document et les recommandations qui en découlent n'auraient jamais pu voir le jour sans l'engagement des membres de ce groupe de travail :

Anne LE HENANFF,
Adjointe au maire de Vannes chargée de la communication, des systèmes d'information et du développement numérique,

Gaëlle CHRISMENT,
Directrice des systèmes d'information, Redon agglomération,

Estelle LE PRIOL,
Responsable du service numérique et SI, Montfort Communauté,

Eric QUILLIOU,
Chargé de mission territoire et intelligence économique, Préfecture des Côtes d'Armor,

Hervé TROALIC,
Directeur Antéo Trust and Security, groupe Sodifrance,

Eric HAZANE & Christian CEVAËR,
Délégués successifs de l'ANSSI à la sécurité numérique pour la région Bretagne.

Nos remerciements vont également à
Benoît LIENARD,
Directeur général de Soluris (Syndicat mixte de Charente-Maritime), membre de la Commission Numérique de l'AMF,
pour sa collaboration à ce document

Avec la participation et le soutien de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Dépôt légal : novembre 2020

Éditeur : Association des maires de France et des présidents d'intercommunalité - Mise en page : Cassiopée Graphisme, Paris
Crédits photos : Photo de la couverture AobeStock ©momius - Photo en page 3 ©Arnaud Février pour l'AMF

41, quai d'Orsay 75343 Paris cedex 07
Tél : 01 44 18 14 14
amf@amf.asso.fr
www.amf.asso.fr
@l_amf