Nos guides de bonnes pratiques

La prévention des cyber-risques

CNPP
Prévention et maîtrise des risques

AVEC

AITF
ASSOCIATION DES INGÉNIEUR.E.S ET INGÉNIEUR.E.S EN CHEF TERRITORIAUX DE FRANCE

AVEC

SMACL ASSURANCES

Sommaire

Préambule

Dématérialisation des documents, démarches en ligne, télétravail : si la transformation numérique permet d'améliorer l'organisation des collectivités, elle les expose, parallèlement, à de réelles vulnérabilités. Elle engendre aussi de nouvelles obligations en matière de sécurisation des systèmes d'information.

Avec la crise sanitaire, la menace cyber s'est encore amplifiée. Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), les attaques par rançongiciel sont en hausse constante.

Ces attaques peuvent avoir un lourd impact sur les services publics dont l'activité peut être, au moins temporairement, interrompue. L'impact peut également être critique sur les données détenues : l'état civil des habitants, les données bancaires des usagers, les données de santé des agents.

Si la plupart des collectivités ont aujourd'hui pris conscience du risque numérique, il reste un problème de taille : la complexité d'évaluer précisément ce risque, de prioriser les actions à mettre en œuvre et de mobiliser les ressources adéquates, en matière d'expertise et de budget, pour y faire face.

Grâce à ce guide, SMACL Assurances et ses partenaires, le Centre national de prévention et de protection (CNPP) et l'Association des ingénieurs territoriaux de France (AITF), vous aident à mieux comprendre la réalité de la menace cyber afin de prendre les mesures nécessaires pour vous en protéger efficacement, en s'appuyant sur des retours d'expérience et des témoignages de collectivités ayant subi des attaques, et en proposant des conseils concrets et simples à mettre en place.

LES GUIDES DE BONNES PRATIQUES DE SMACL ASSURANCES
Directeur de la publication : Patrick Blanchard • Directrice de la rédaction : Cécile Mexandeau • Rédactrice en chef : Anne-Sophie Tauran • Ont collaboré à ce numéro : Julie Boilley, Cécile Charrier, Stéphane Neuilly, Carole Rouger, Alexandre Freland et Pierre Bridon (SMACL Assurances), Jean-Marc Jouvenaux et Guillaume Vitse (CNPP) • Rédaction : Agence 4août • Mise en page : Émilie Fleuriault • Relecture : CorrectOgraphe • Crédits photos : Antoine Repessé, Getty Images • ISBN : 978-2-493076-01-4

1

Les collectivités confrontées à une menace bien réelle

1.1 Qu'est-ce qu'une cyberattaque ?

· En quelques mots

Une cyberattaque est une action volontaire malveillante menée par une personne seule ou un groupe et contrevenant aux traités internationaux ou aux lois nationales, en utilisant les réseaux ou les systèmes d'information. Il existe quatre types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises : la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage.

Les cyberattaques sont facilitées par des failles de sécurité dans les systèmes d'information.

En chiffres

La transformation numérique, première menace pour les collectivités en 2020.[1]

94%

des cybermenaces commencent par un e-mail.[2]

En 2020, **un tiers** des villes et régions ont déclaré avoir été touchées par un ransomware ou rançongiciel.[3]

Sources : [1] www.cybermalveillance.gouv.fr
[2] Darktrace. « *Rapport sur les menaces de ramsomware pour 2021* »
[3] CLUSIF. Étude « *Menaces Informatiques et Pratiques de Sécurité (MIPS)* ». juin 2020

1.2 Les grandes tendances

• La menace cyber : une réalité

En 2020, les attaques informatiques ont été multipliées par 4. Les rançongiciels génèrent les atteintes les plus fréquentes.

> Cybersécurité : un budget à augmenter

En moyenne, les collectivités investissent entre **2 et 7 % de leur budget informatique** dans la cybersécurité, malgré les recommandations des experts qui suggèrent d'investir un minimum de **10 % de ce budget chaque année**.

> Prise en compte des cyber-risques : peut mieux faire !

Selon notre étude, près d'un tiers des collectivités interrogées avoue n'avoir prévu aucune action pour se protéger d'une cyberattaque, pourtant la menace est considérée comme prioritaire pour la moitié des répondants.

Découvrez notre étude réalisée avec Courrier des Maires : « Les collectivités et les élu·e·s face aux risques »

> La prévention, nouvelle solution

Entre 2016 et 2020, les dépenses en lien avec l'audit des systèmes d'information ont augmenté de **14 %**. Selon le rapport du CLUSIF*, cette augmentation traduit **un changement de perception des enjeux en matière de cybersécurité**. Cependant, très peu de collectivités ont mis en place une nouvelle organisation.

Source : *CLUSIF (Club de la sécurité de l'information français). Étude « *Menaces Informatiques et Pratiques de Sécurité (MIPS)* ». juin 2020

3 mots-clés

• Dépendance

Avec le développement des outils digitaux et des services publics dématérialisés, de plus en plus de collectivités deviennent dépendantes de leur système informatique. Une réalité qui a pour conséquence d'impacter plus fortement leurs activités si le système d'information est hors service.

• Gouvernance

Peu de collectivités ont mis en place une organisation transversale pour piloter la sécurité de leur système informatique. Cette coordination est pourtant fortement conseillée pour anticiper et prévenir les risques.

• Sous-traitance

Les communautés de communes sont nombreuses à s'appuyer sur un consultant externe, contrairement aux communes. C'est pourtant une aide utile pour sensibiliser les équipes ou corriger les failles. Attention : la sous-traitance vous expose également du fait de la vulnérabilité potentielle de certains prestataires qui deviennent des cibles faciles pour atteindre vos propres systèmes.

Vos témoignages

Comment sensibiliser les élus en matière de cyberattaque ?

Quand on quitte son domicile, on ferme ses portes et fenêtres. Agissons de même avec nos systèmes informatiques.

Il faut accrocher les élus avec des choses simples comme les risques sur leur image ou les risques juridiques. Lorsque je sensibilise, j'utilise une astuce qui marche à chaque fois : je demande en début de réunion aux participants de noter sur un post-it leur mot de passe en leur disant que c'est pour vérifier s'il est suffisamment solide. Immanquablement, tous les participants s'exécutent. Ce n'est que lorsque je leur demande ensuite de noter aussi le code de leur carte bancaire qu'ils comprennent qu'ils viennent de se faire piéger.

Philippe Loudenot,
Délégué cybersécurité, administrateur du CESIN (Club des experts de la sécurité de l'information et du numérique) · 20e colloque de l'Observatoire SMACL « *Les collectivités face aux cyberattaques* », 21/10/2021

1.3 Quels risques ? Quels impacts ?

D'après l'Agence nationale de la sécurité des systèmes d'information (ANSSI), « aucun secteur d'activité ni zone géographique n'est épargné par le risque cyber. Chaque institution ayant un accès à Internet peut être infectée par un rançongiciel si elle n'a pas mis en œuvre des mesures de sécurité informatique ».

L'ANSSI note que « les collectivités territoriales et le secteur de la santé sont majoritairement concernés par ce risque (...). Cela peut montrer l'intérêt des attaquants pour des entités réputées faiblement dotées en sécurité informatique ou dont la rupture d'activité aurait un impact social important ».

• Les différents types de risques

Le rançongiciel (ou ransomware)

› Qu'est-ce que c'est ?

C'est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant. Les auteurs de l'attaque réclament une rançon pour en permettre de nouveau l'accès. L'ordinateur peut être infecté après l'ouverture d'une pièce jointe, après un clic sur un lien dans un courriel, après navigation sur des sites compromis, ou encore suite à une intrusion dans le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités dans les logiciels qui n'ont pas été correctement mis à jour.

Source : www.cybermalveillance.gouv.fr

En 2020, les signalements d'attaques par rançongiciel ont été multipliés par 3,5 par rapport à 2019. Toutes les collectivités sont concernées, quelle que soit leur taille.

Source : ANSSI

Cyberattaque : quel coût ?

Une collectivité française a subi une attaque par ransomware en janvier 2021. Selon elle, **le coût de l'attaque s'élève à 1 000 € par agent**, ils sont au nombre de 600 !

Au-delà des aspects financiers, il ne faut pas perdre de vue l'impact psychologique sur les agents qui se sont retrouvés sans outil de travail et ont dû adapter leur activité pendant des semaines.

Défiguration de site

› **C'est l'altération par un pirate de l'apparence d'un site internet :** la page d'accueil peut devenir noire ou blanche ou comporter des messages, des images, des logos ou des vidéos déplacés et/ou sans rapport avec l'objet initial du site. C'est le signe visible que l'attaquant a obtenu les droits lui permettant de modifier le contenu du site.

Durant l'attaque, le site n'est souvent plus utilisable. En étant visible publiquement, la défiguration démontre que l'attaquant a pu prendre le contrôle du serveur, ce qui porte atteinte à l'image de la collectivité.

Le contenu du site peut être modifié ou supprimé. Des revendications illégales peuvent y être formulées au nom de la collectivité.

Le phishing

› **Le phishing (ou hameçonnage) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles** (comptes d'accès, mots de passe, identifiants bancaires…) en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administration.

Le piratage de compte

› **C'est la prise de contrôle, par un individu malveillant, de comptes, d'applications de messagerie, d'un réseau social, de sites administratifs, ou de plateformes de commerce en ligne.**

Les attaquants ont eu accès à ces comptes de plusieurs manières : soit le mot de passe était trop simple, soit la collectivité a précédemment été victime d'hameçonnage (phishing).

L'usurpation d'identité

› **C'est un délit qui désigne l'utilisation d'informations personnelles permettant d'identifier une personne sans son accord pour commettre un acte frauduleux.**

Ces informations peuvent être obtenues par les cybercriminels suite à la perte ou au vol de documents d'identité, par le biais d'un message d'hameçonnage, par le piratage d'un compte en ligne, par le piratage d'un site internet, ou encore en étant récupérées de la corbeille de l'ordinateur piraté.

Source : www.cybermalveillance.gouv.fr

Impacts les plus fréquents

- Des informations personnelles ou professionnelles (comptes, mots de passe, données bancaires) peuvent être dérobées pour un usage frauduleux (revente des données, usurpation d'identité, transactions illégales, spam).
- En fonction des informations recueillies, lors d'une usurpation d'identité, les escrocs peuvent commettre diverses infractions au nom de la victime : ouverture de ligne téléphonique ou de compte bancaire, création de comptes sur les réseaux sociaux, souscription d'un crédit, location de voiture, escroquerie des proches, fausses petites annonces, diffamation, cyber-harcèlement, chantage ou extorsion. Au-delà du préjudice moral, l'usurpation d'identité peut avoir des conséquences importantes : les victimes pourraient se voir poursuivies pour des infractions dont elles devraient prouver qu'elles n'en seraient pas les auteurs.

Source : www.cybermalveillance.gouv.fr

1.4 À chaque service public son cyber-risque

	Risque associé
Transports publics avec numérisation des tickets et des abonnements ou géolocalisation de la flotte de transports en commun	**Risque financier lié au détournement du service : falsification, usage de faux**
Prestations sociales (de type chèque-livre ou pass culture) nécessitant l'inscription et la gestion dématérialisée	**Risque financier : contournement, indisponibilité du service**
Systèmes de vidéosurveillance mis en œuvre de façon locale ou centralisée	**Mise en échec des systèmes de sécurisation augmentant la vulnérabilité des lieux protégés**
Inscription d'enfants aux activités périscolaires avec facturation associée	**Récupération des données de facturation**
Système de gestion des places de stationnement et des contraventions associées	**Exploitation d'une vulnérabilité bloquant le système de paiement**
Services internes à la collectivité : comptabilité, ressources humaines...	**Attaques de type phishing et accès aux données de la collectivité**
Fichiers d'état civil	**Outil de gestion inaccessible pour la collectivité et/ou vol et revente des données personnelles des administrés**

Quand un sous-traitant est attaqué ?

Les collectivités peuvent aussi engager leur responsabilité pénale en qualité de personne morale s'agissant des activités déléguées ou sous-traitées, lorsque l'attaque est subie dans le cadre d'une délégation de service public (par un fournisseur d'eau par exemple) ou par un sous-traitant (opérateur de télécommunication ou de signalisation).
Cependant, pour prouver la faute, il faudrait qu'un lien de causalité soit établi entre la négligence imputée à la collectivité et le dommage résultant de l'attaque informatique.

Source : Observatoire SMACL. Rapport annuel *« Le risque pénal des élus locaux et des fonctionnaires territoriaux »*. Janvier 2022

Conséquence indirecte d'une cyberattaque : et les citoyens dans tout ça ?

Après une cyberattaque, la confiance des citoyens à l'égard de leurs élus peut être altérée et la réputation de la collectivité ternie, à plus ou moins long terme.

> Chiffres repères

Vous avez subi une cyberattaque au cours de ces douze derniers mois, quels ont été les principaux impacts sur votre organisation ?

Les collectivités répondent :

- Arrêt de l'exploitation

- Atteinte à l'image de la collectivité

- Perte de données

Source : Fédération nationale des collectivités concédantes et régies (FNCCR). « *Étude sur la cybersécurité des villes et territoires intelligents* ». Juillet 2021


“Cette période de six jours nous a permis de réaliser à quel point nous sommes dépendants de nos systèmes d’information.”

Vos témoignages

Le 9 décembre 2020, je suis dans mon bureau. Comme tous les matins, je râle parce que le système de messagerie semble ramer davantage que d'habitude et un certain nombre de logiciels métiers ne fonctionnent pas bien. La direction des systèmes d'information reçoit des tickets en tel nombre qu'elle s'en inquiète. Nous sentons que la situation est anormale, même si je doute qu'au moment même, nous ayons eu conscience de la menace.

Dans un premier temps, nous avons construit une parade d'urgence face à l'instabilité chronique de nos systèmes d'information. Nous constatons, d'une part, que deux adresses au moins nous paraissent usurpées (comportements anormaux en termes d'heure de connexion) et, d'autre part, que l'Active Directory, qui contient l'ensemble des mots de passe, est ciblé.

Nous convenons rapidement avec le directeur des systèmes d'information de couper les flux numériques et de débrancher tous les postes informatiques de la collectivité.

Cela nous prive d'outils de travail. Nous dégradons le service rendu, nous ne sommes plus joignables par les administrés et nous avons du mal à communiquer entre nous. Cette période de six jours nous a permis de réaliser à quel point nous sommes dépendants de nos systèmes d'information.

Jean-Louis Héno,
Directeur général des services, ville de Pantin
• 20e colloque de l'Observatoire SMACL
« *Les collectivités face aux cyberattaques* », 21/10/2021

2

Comment se protéger ?

Vous nous avez dit...

Le 21 octobre 2021 a eu lieu à Paris la 20e édition du colloque de l'Observatoire SMACL. L'occasion de partager des retours d'expérience d'experts et d'acteurs de terrain sur les enjeux de la cybersécurité au sein des collectivités.

« Les agents doivent être sensibilisés à l'anonymisation des données : le premier problème de la cybersécurité est interne. »

Virginie Bensoussan-Brulé,
Avocate, directrice du pôle Contentieux numérique,
Lexing Alain Bensoussan Avocats

« Déposer plainte après une attaque est capital. Cela permet notamment aux services d'enquête d'opérer des recoupements sur les modes opératoires des cyberattaques. »

Myriam Quéméner,
Avocat général à la cour d'appel de Paris, docteur en droit

« Les données de santé sont parmi les plus concernées par les attaques. »

Mathieu Ginestet,
Juriste, service des délégués à la protection des données de la CNIL (Commission nationale de l'informatique et des libertés)

Retrouvez l'intégralité des échanges dans les Actes du 20e colloque de l'Observatoire SMACL disponibles sur : www.smacl.fr/actes-obssmacl

2.1 Une bonne prévention : mode d'emploi

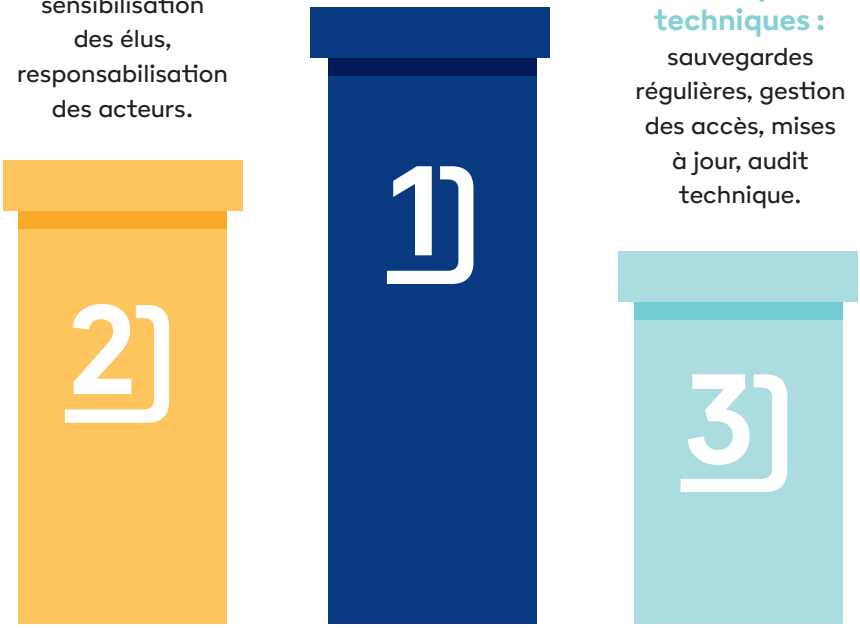
· Construire un plan de prévention efficace

Un dispositif de prévention des cyber-risques peut s'organiser autour de trois piliers :

L'organisation : cartographie des risques, gestion des prestataires, audit organisationnel.

Les moyens humains : formation du personnel, sensibilisation des élus, responsabilisation des acteurs.

Les moyens techniques : sauvegardes régulières, gestion des accès, mises à jour, audit technique.



· Première étape : l'organisation

> Mettre en place une gouvernance adaptée

La première étape de la prévention consiste à définir un programme adapté de gouvernance de la sécurité. Il répond à un besoin simple : comment mettre en place les mesures de sécurité suffisantes et nécessaires pour protéger les données et l'activité ?

Cette gouvernance « par les risques » permet notamment de prioriser les actifs les plus sensibles pour leur appliquer des mesures pertinentes.

Un exemple : l'ordinateur portable. Actif essentiel, il permet aux agents de travailler à l'extérieur et de stocker une quantité importante d'informations, parfois confidentielles.

Une gouvernance par les risques consiste à identifier les vulnérabilités de l'ordinateur et à préconiser des mesures pour les corriger.

> **“ Le rôle de l'élu est d'impulser une dynamique. ”**

« Une démarche de prévention ne peut être efficace que si on maîtrise les notions fondamentales de la sécurité de l'information et les enjeux. Bien que les élus soient de plus en plus sensibilisés au risque cyber, il est encore trop largement considéré que la sécurité de l'information se résume à l'informatique et aux mesures techniques mises en œuvre.
En questionnant le maire d'une petite commune sur la maîtrise du risque cyber, ce dernier m'a répondu "Oui, oui, c'est géré, notre prestataire nous a installé de nouveaux antivirus". L'antivirus est ici l'arbre qui cache la forêt des nombreuses solutions techniques et organisationnelles qui contribuent à la maîtrise du risque cyber. »

Guillaume Vitse,
Directeur du développement et de la relation client Groupe CNPP
· 20e colloque de l'Observatoire SMACL
« *Les collectivités face aux cyberattaques* »,
21/10/2021

Le service commun : une solution pour mutualiser la cybersécurité

La prévention peut être gérée de manière mutualisée entre plusieurs communes. L'intercommunalité peut alors tenir un rôle pivot d'organisateur.

Régi par la loi (article L.5211-4-2 du Code général des collectivités territoriales), le service commun peut faciliter les économies d'échelle et le développement de nouvelles expertises. Pour les petites communes et intercommunalités, il peut se concrétiser par le recrutement d'une personne ressource en matière de cybersécurité.

> Définir les responsabilités de chacun

Segmenter les tâches et les rôles-clés de l'organisation permet de protéger de façon optimale la structure et les données qu'elle détient.

Pour cela, le délégué à la protection des données (DPD) et le responsable de la sécurité des systèmes d'information (RSSI) doivent bénéficier d'un rattachement hiérarchique et d'une indépendance fonctionnelle, afin de remonter à la direction générale des services des alertes ou des manquements pouvant impacter l'organisation.

> Bien choisir les fournisseurs et les prestataires

Le recours à des fournisseurs ou prestataires dans la gestion d'un système d'information est aujourd'hui devenu la norme. Une pratique qui permet d'optimiser les coûts, mais qui n'est pas sans risque. La signature d'un accord de confidentialité avec le prestataire, un management par les risques de sécurité de l'information, l'obtention d'une certification ISO/CEI 27001 ainsi que la présence d'un responsable de la sécurité des systèmes d'information (RSSI) et d'un délégué à la protection des données (DPD) sont des éléments que le prestataire doit être en capacité de présenter.

Attention

Une certification ISO/CEI 27001 n'est pas synonyme d'absence de risque. Il est nécessaire de confronter le fournisseur sur les mesures en place et d'analyser le périmètre de la certification.

> Planifier la continuité de son activité

La crise sanitaire, en particulier lors du confinement du printemps 2020, a mis en lumière l'importance d'un plan de continuité d'activité. Pour prioriser les actions de reprise, il est essentiel :

- d'identifier les activités-clés et leurs délais de reprise acceptables ;
- de déterminer les ressources nécessaires pour assurer ces activités : nombre d'agents, matériel, infrastructures ;
- de mettre en œuvre des mesures pour assurer ces activités : fournir des ordinateurs portables, disposer de sites de reprise, identifier des canaux de communication via des applications spécifiques ;
- de tester ces mesures dans le cadre d'exercices en situation réelle.

La continuité d'activité a aussi sa norme !

ISO/CEI 22301 : c'est la norme qui précise les exigences d'un système de management afin de protéger la collectivité des incidents perturbateurs, de réduire leur probabilité et de garantir la récupération des données. Elle est la référence en la matière pour concevoir et piloter un plan de continuité d'activité.

Source : www.iso.org/fr/standard/50038.html

· Deuxième étape : les mesures techniques

> Choisir des solutions robustes

Intégrer un composant au sein de son système d'information ne se fait pas sans réflexion. La question doit se poser, en amont, du bien-fondé de cette brique informatique. Pour accompagner les collectivités dans cette démarche, l'ANSSI propose des certifications de produits : Critères communs (CC) et Certificat de sécurité de premier niveau (CSPN).

“ Limiter les risques ”

« En matière d'attaque informatique, l'analogie avec la pêche est pertinente : la commune la moins préparée va mordre à l'hameçon. Personne n'est visé en particulier. Notre rôle est de rendre votre système informatique moins intéressant que celui du voisin.
Il est important de mesurer la pénétration du système d'information. Il convient en permanence de s'interroger sur la manière de limiter les risques, en esquissant des scénarios catastrophiques. Ces tests sont régulièrement réalisés par des sociétés spécialisées. Dans 100 % des cas, elles parviennent à pénétrer dans le système de données. Ce n'est qu'une question de temps. Il convient donc de ralentir ces attaques pour devenir une cible moins prioritaire. »

Thomas Hébert,
DSI Délégué Assistance à maîtrise d'ouvrage Société Dimoxilo
· 20e colloque de l'Observatoire SMACL « *Les collectivités face aux cyberattaques* », 21/10/2021

> Mettre en place un système d'archivage sécurisé

L'archivage électronique stocke sur le long terme les informations nécessitant une attention particulière. Des solutions robustes d'archivage électronique sont synonymes de conservation pérenne. L'utilisation d'une clause de séquestre permettra, en cas de litige ou de faillite du partenaire, la récupération du code source afin de pouvoir assurer une continuité dans la réalisation du service.

> Mettre en œuvre un système d'authentification numérique

Le RGS et l'eIDAS (cf. page 32), dispositifs de signature électronique réglementés, établissent un lien de confiance dans l'usage de documents partagés entre tiers. La signature électronique atteste à un instant T qu'une personne, ou un organisme, a bien été à l'origine d'un message.

> Faire auditer son système d'information

Auditer son système d'information de manière régulière assure un niveau continu de sécurité. Il est recommandé de mettre en œuvre un programme d'audit pour définir, sur une période donnée, l'ensemble des tests devant être effectués, en fonction de la sensibilité des briques du système d'exploitation.

• Troisième étape : les moyens humains

> Sensibiliser son personnel aux risques cyber

La sensibilisation et la formation du personnel des collectivités sont au cœur de toute stratégie de sécurité de l'information. Il est notamment nécessaire de former les agents au respect des réglementations auxquelles la collectivité est soumise, par exemple celles relatives aux données personnelles.

La mise en place d'une gouvernance par les risques (voir la partie ci-dessus : **Première étape : l'organisation**) permet de prioriser en interne les actifs les plus sensibles afin de leur appliquer des mesures de sécurité pertinentes en fonction des menaces. À titre de comparaison, ce sont les mêmes questions que dans la construction d'un programme de prévention des risques routiers ou d'un document unique de prévention des risques professionnels : toute source de vulnérabilité doit faire l'objet d'une étude des risques et des dommages associés.

Par ailleurs, pour se préparer au mieux, il est recommandé d'énoncer plusieurs scénarios plausibles afin de mettre en lumière des dépendances vis-à-vis de bâtiments, de personnels, de technologies ou de prestataires, et d'identifier ainsi des actions de reprise d'activité en fonction des différents cas. En testant de manière régulière et sur des situations différentes son institution, le personnel sera sensibilisé et les réflexes seront acquis.

> Sensibiliser les usagers

Adapter sa communication externe et effectuer des campagnes de rappel sur les bonnes pratiques de sécurité de l'information font partie des règles de base pour se prémunir contre les cyber-risques. Un accompagnement pédagogique régulier des usagers complète les mesures techniques et organisationnelles prises en interne.

Virginie Bensoussan-Brulé, Avocate, directrice du pôle Contentieux numérique chez Lexing Alain Bensoussan Avocats · 20e colloque de l'Observatoire SMACL « *Les collectivités face aux cyberattaques* », 21/10/2021

« Les droits d'accès d'un agent RSSI s'apprêtant à quitter une collectivité avaient été suspendus au moment de son départ. Or, bien que, conformément à nos recommandations, la collectivité lui ait fait signer une déclaration sur l'honneur selon laquelle il reconnaissait ne détenir aucun élément de nature privée dans ses fichiers et messageries professionnels, cet agent va parvenir à se faire rétablir temporairement son droit d'accès en prétextant la nécessité de récupérer des dossiers personnels oubliés. Ceci en violation des procédures de sécurité, ce qui va lui permettre d'exfiltrer un certain nombre de données et de les partager sous couvert d'anonymat sur un réseau social en invoquant une fuite de données. Cet exemple illustre la nécessité de sensibiliser le personnel jusqu'au plus bas de l'échelle hiérarchique, notamment lorsqu'il est en contact avec les usagers. »

2.2 Une bonne protection : boîte à outils

Les 10 mesures essentielles

1. Protéger les accès avec des mots de passe solides
2. Sauvegarder les données régulièrement
3. Faire les mises à jour dès qu'elles sont proposées
4. Utiliser un antivirus
5. Télécharger les applications uniquement sur les sites officiels
6. Se méfier des messages (e-mails, sms) inattendus
7. Vérifier la fiabilité des sites d'achat en ligne utilisés
8. Ne pas ouvrir de pièces jointes provenant de sources inconnues
9. Séparer les usages personnel et professionnel
10. Éviter les réseaux wifi publics ou inconnus

Nos conseils

Éviter de brancher une clé USB ou un disque dur externe personnel ou inconnu sur son poste de travail. Ce sont des vecteurs de virus.

Ne pas ouvrir de pièces jointes provenant de sources inconnues, que ce soit par mail ou support tiers.

Ne pas cliquer sur des liens hypertextes quand l'expéditeur d'un e-mail est inconnu ou peu sûr.

> Lorsqu'on externalise...

L'externalisation doit assurer la bonne gestion de la sécurité informatique, et non créer de nouveaux risques, au moyen de mesures spécifiques :

- évaluer la durée de rétention des informations sauvegardées ;
- déterminer la durée d'interruption d'activité maximale : pendant combien de temps le service peut-il être inaccessible ?
- s'assurer que toute information sensible soit correctement protégée ;
- s'assurer également des compétences mises à disposition par le partenaire ;
- définir une gestion des incidents liés à la sécurité de l'information et la remontée d'informations vers la collectivité.

Les réponses apportées doivent être évaluées pour orienter la prise de décision dans la sélection d'un prestataire.

Source : www.cybermalveillance.gouv.fr

Les 5 règles d'or d'un mot de passe sûr

1. Utiliser un mot de passe différent pour chaque service
2. Définir un mot de passe suffisamment complexe et long
3. Créer un mot de passe impossible à deviner
4. Se servir d'un gestionnaire de mot de passe
5. Changer de mot de passe régulièrement

Chacun sa méthode pour créer un mot de passe solide !

- La méthode des premières lettres
  « Un tiens vaut mieux que deux tu l'auras »
  1 tiens vaut mieux Que 2eux tu l'Auras
  > 1tvmQ2tl'A
- La méthode phonétique
  « J'ai acheté huit CD pour cent euros cet après-midi »
  g ht 8 CD % E 7 am
  > ght8CD%E7am

Inventez une méthode connue de vous seul !

Source : www.cybermalveillance.gouv.fr

2.3 Que faire en tant que décideur ?

• Mise en situation

Durant le week-end, vos administrés vous informent que le site Internet de votre commune affiche des messages insultants.

> Que feriez-vous en tant qu'élu ?

Réponse :

Un dépôt de plainte est essentiel.

La priorité est de supprimer l'accès au site. Pour faire appel à des prestataires externes expérimentés, contactez votre assurance où rapprochez-vous de l'ANSSI qui propose une liste de structures habilitées.

Nous vous recommandons également de prévoir une communication à destination de vos usagers pour les rassurer.

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

Une fois l'incident terminé, prenez des précautions en entamant une démarche de sécurisation de vos systèmes informatiques.

Source : Fédération nationale des collectivités concédantes et régies (FNCCR). « *Étude sur la cybersécurité des villes et territoires intelligents* ». Juillet 2021

2.4 Se protéger : les textes réglementaires

Pour répondre au défi de la sécurité numérique, la France s'est dotée d'un cadre réglementaire mis en œuvre par son droit national et par les directives prises au niveau de l'Union européenne. En tant qu'autorités administratives, les collectivités ont l'obligation de les respecter.

• Le RGS

> Encadrer les échanges entre administrations et usagers

Le référentiel général de sécurité (RGS) est l'outil réglementaire permettant de fiabiliser les échanges entre les autorités administratives et leurs usagers. Il définit les exigences de sécurité pour les téléservices : inscription des enfants à l'école ou à la cantine par Internet, déclaration d'imposition, règlement d'une contravention, demande de prestation sociale, plateforme de dématérialisation des marchés publics...

Pour l'appliquer, il est possible d'avoir recours à des prestataires de services dits « qualifiés » : les prestataires de services de certification électronique (PSCE), les prestataires de services d'horodatage électronique (PSHE), les prestataires d'audit de la sécurité des systèmes d'information (PASSI).

• Le règlement eIDAS

> Sécuriser les signatures électroniques

Ce règlement européen établit un socle commun pour rendre plus sûres les interactions électroniques entre les citoyens, les entreprises et les autorités publiques au sein de l'Union européenne.

Les collectivités territoriales mettant en œuvre une identification, une signature ou un cachet électronique dans le cadre de leurs services en ligne sont directement concernées par ce règlement.

Le RGPD

> Protéger les données personnelles

Le règlement général sur la protection des données (RGPD) est un texte réglementaire européen qui encadre, depuis le 25 mai 2018, le traitement des données à caractère personnel.

Il a pour objectif de renforcer les droits des personnes, de responsabiliser les acteurs traitant des données et de consolider la régulation grâce à une coopération entre les autorités.

Il s'applique aux collectivités territoriales car ces dernières sont responsables du traitement de données à caractère personnel. Dans le cadre du RGPD, la CNIL est la seule autorité nationale compétente en matière d'accompagnement, d'établissement des référentiels et de contrôle.

Qu'est-ce qu'une donnée à caractère personnel ?

Selon l'article 4 du RGPD, une donnée à caractère personnel est « **toute information se rapportant à une personne physique identifiée ou identifiable, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale** ».

La HDS

Être autorisé à héberger des données de santé

Les données de santé à caractère personnel sont des données sensibles. Le Code de la santé publique prévoit que les personnes hébergeant des données de santé à caractère personnel pour le compte de tiers doivent être titulaires d'un certificat de conformité délivré par un organisme accrédité. Le coût et les délais d'obtention de la certification HDS (Hébergement de données de santé) peuvent amener les collectivités territoriales à contractualiser avec un hébergeur disposant déjà de l'agrément.

Sécurité des acteurs critiques : les autres règlements en vigueur

La loi de programmation militaire (LPM) s'adresse aux opérateurs d'importance vitale.

Ce sont les cyberattaques subies par les organisations qui, pourraient porter atteinte au potentiel de guerre ou économique, à la sécurité ou à la capacité de survie de la nation, ou mettre en cause la santé ou la vie de la population.

La directive européenne Network and Information Systems (NIS) s'adresse aux collectivités territoriales désignées comme Opérateur de services essentiels (OSE).

Ces opérateurs supportent des services dits essentiels au fonctionnement de la société ou de l'économie (alimentation, sanitaire) et dont la continuité pourrait être affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture de ces services.

Sources : ANSSI. Guide *« Sécurité numérique des collectivités locales, l'essentiel de la réglementation »*
www.economie.gouv.fr (ministère de l'Économie)

“Un pilote expert, indispensable pour une cybersécurité efficace.”

« Petite ou grande collectivité, il faut un pilote qui, par son expertise, sera capable de cartographier l'ensemble des données gérées par la collectivité et de dérouler une analyse de risques, c'est-à-dire évaluer les menaces potentielles qui pèsent sur chaque ensemble de données, la vraisemblance qu'une attaque se produise et avec quels impacts pour la collectivité. Ce pilote ne peut être qu'un responsable de la sécurité des systèmes d'information (RSSI). Si les plus grandes municipalités et communautés de communes se sont déjà dotées d'un RSSI, les plus petites ont tout intérêt, soit à se regrouper pour mutualiser cette ressource, soit à faire appel à un spécialiste comme CNPP. Malheureusement, aujourd'hui, à peine une collectivité sur deux inscrit cette démarche dans ses projets prioritaires. »

Romain Rousseau,
Manager Conseil et Formation Cybersécurité
Groupe CNPP

> Chiffres repères

136 M€

Dans le cadre du plan France Relance, l'ANSSI bénéficie d'une enveloppe de **136 millions d'euros** pour **renforcer la cybersécurité** de l'État et des territoires sur la période 2021-2022. L'objectif est d'élever durablement le niveau de cybersécurité de l'État, des collectivités, des établissements de santé et des **organisations au service des citoyens,** tout en développant le tissu industriel français de cybersécurité.

60 M€

C'est le montant prévu dans le cadre de France Relance pour renforcer la cybersécurité des collectivités territoriales : parcours de cybersécurité, cofinancement de projets et soutien à la création des CSIRT régionaux (Computer Security Incident Response Team). Les CSIRT sont des centres de réponse aux incidents cyber, ils traitent notamment les demandes d'assistance de collectivités.
Source : ANSSI


“
Il ne faut
pas hésiter à investir
dans l’infrastructure
informatique,
qui ne fait pas toujours
partie des priorités.
”

Vos témoignages

30 janvier 2021 à Houilles : nous devons marquer cette date d'une pierre noire puisque dans la nuit à 3h30, nous avons été victimes d'une cyberattaque et d'un ransomware, par le biais d'une faille de sécurité. Rapidement, nous avons débranché l'ensemble des connexions réseau pour éviter la propagation du virus. Nous sommes parvenus à isoler les parties RH et finances, avant de nous interroger sur la manière dont nous allions pouvoir rétablir les différents services de la commune, en les priorisant.

Cela nous a conduits à élaborer et à mettre en œuvre un plan d'action. Nous avons dû travailler manuellement pendant des semaines. Nous avons également été confrontés à une demande de rançon, à laquelle nous n'avons pas donné suite, conformément aux recommandations de l'ANSSI, et nous avons déposé plainte.

Nous en sommes sortis au prix d'un important effort financier et humain au bout d'un mois et demi. Il convient de prendre conscience des risques et des conséquences d'une cyberattaque sur la vie démocratique de la commune. Il ne faut pas hésiter à investir dans l'infrastructure informatique, qui ne fait pas toujours partie des priorités.

Sébastien Simonin,
Conseiller municipal délégué au numérique,
aux entreprises et à la prospective économique,
ville de Houilles • 20e colloque de l'Observatoire SMACL
« *Les collectivités face aux cyberattaques* », 21/10/2021

2.5 Regards croisés d'experts

Vincent Bimbard,
Président de l'AITF
(Association des ingénieurs
territoriaux de France)

Patrice Daverat,
Responsable du pôle
Prévention des risques
de SMACL Assurances

La culture du risque cyber au sein des collectivités est-elle une question d'expérience vécue ?

V.B. Oui, et de plus en plus de collectivités protègent leurs données et leurs systèmes numériques des risques d'intrusion et d'attaques tant intérieurs qu'extérieurs, tant volontaires que parfois involontaires.

Le développement d'Internet et la généralisation du numérique ont particulièrement augmenté les risques générés par l'usage exponentiel des technologies de l'information et de la communication.

Et ce, d'autant plus que les niveaux d'échanges et d'interconnexion se sont considérablement démultipliés depuis la crise sanitaire liée à la pandémie Covid-19.

P.D. Le retour d'expérience joue un rôle important dans l'argumentaire d'une politique prévention sur le risque cyber. C'est un tremplin pour démultiplier des actions d'information, de formation et d'organisation afin de créer les conditions d'adaptation et de méthodologie pour limiter les conséquences. C'est aussi une prise de conscience globale : la question n'est pas de savoir si le piratage peut arriver, mais quand !

Quels défis attendent les élus et décideurs dans le domaine de la cybersécurité ?

P.D. Transition numérique des territoires, dématérialisation accélérée de la gestion des services publics, responsabilités plus grandes des décideurs locaux : cet arrière-plan laisse imaginer l'importance des défis à relever, non seulement sur les actes de gestion au quotidien - l'évolution des

compétences territoriales touchant des activités sensibles et vitales – mais aussi la capacité de pilotage des plans de continuité d'activité comme de gestion de crise.

V.B. Plus que les élus, ce sont les cadres dirigeants des collectivités territoriales qui se sont saisis de ces sujets afin de protéger les personnes, les outils numériques, les données et échanges numériques immatériels.

La sécurisation des connexions et des réseaux est indispensable à la gestion administrative, financière, technique et économique des collectivités dans leur pratique professionnelle quotidienne comme, par exemple, dans le cadre de passation et de d'exécution de marchés publics.

Quels sont les deux mots-clés à retenir pour agir efficacement contre ce risque ?

V.B. Anticipation et protection !

P.D. Acculturation au risque avec pour principaux objectifs de limiter les impacts et garantir une continuité des services publics. Responsabilisation : compte tenu de l'importance des données sensibles, c'est une véritable stratégie à mettre en place à l'échelle décisionnelle.

Une suggestion ou un conseil ?

P.D. Il faut dépasser l'idée que le numérique est une affaire de spécialistes ! La prévention du risque cyber passe par une logique organisationnelle impliquant l'ensemble des acteurs avec un rattachement direct aux décisionnaires.

V.B. Les collectivités territoriales ont nécessité à en faire un des fondements de leur action, car la sécurisation des outils informatiques et données numériques est au cœur des interactions et de l'exécution de l'ensemble des missions de service public.

Comment SMACL Assurances aide-t-elle les collectivités à prévenir les cyber-risques ?

La cybermalveillance appelle une vigilance à tous les niveaux

Accompagner les territoires nécessite une parfaite connaissance de leur réalité institutionnelle, économique et sociale. Chez SMACL Assurances, c'est notre cœur de métier, nous proposons aux collectivités un plan de prévention personnalisé adapté à leurs systèmes d'information.

Grâce à ce guide, nous vous proposons de vous éclairer sur la menace cyber, de vous assister dans votre compréhension des enjeux et de répondre à vos différentes interrogations sur le sujet.

Les enjeux de la prévention des risques

Les 4 étapes d'une démarche de prévention

Nous vous proposons un plan de prévention adapté à votre système d'information, votre flotte automobile, votre patrimoine immobilier ou à la santé et la sécurité de vos agents et salariés.

Nos préventeurs vous accompagnent dans toutes les étapes de la procédure : de l'analyse de votre situation à la mise en œuvre et au suivi des actions.

Identifier et évaluer les risques

Identification des vulnérabilités par la réalisation d'un diagnostic (incendie, risques naturels, sûreté, malveillance, territoire et bâtiments, cybersécurité)

Élaborer un plan de prévention

Définition d'actions personnalisées à destination de la personne morale (services assurance, prévention, patrimoine...)

Mesurer l'efficacité et ajuster

Suivi du plan de prévention et de l'évolution de la sinistralité

Déployer des actions

Accompagnement au déploiement du plan de prévention (conseil, sensibilisation, formation, ateliers, groupes de travail...)

Votre plan de prévention des cyber-risques

Nouveaux dangers qui impactent autant les acteurs publics que les acteurs privés, les cyber-risques ne peuvent plus être considérés comme une menace potentielle. Ils sont bien réels et exigent un accompagnement professionnel. Pour répondre à vos sollicitations et vous assister dans votre compréhension des enjeux, nous nous sommes rapprochés de CNPP.

Nous sommes à votre écoute :

prevention@smacl.fr — **05 49 33 83 10**

Le mot de la fin

Jean-Luc de Boissieu,
Président de SMACL Assurances SA

Si un élu ou décideur local sur deux estime être insuffisamment formé et informé, et donc peu préparé pour gérer les cyber-risques de sa collectivité, notre responsabilité en tant qu'assureur est de lui apporter les éléments de connaissance et de maîtrise dont il a impérativement besoin.

Certes, c'est aux collectivités de se prémunir contre ces risques, car l'assureur n'a pas réponse à toutes les sources et à toutes les formes de dysfonctionnements qui peuvent toucher les systèmes d'information. Il ne suffit pas que la collectivité ait souscrit un contrat d'assurance pour sécuriser ses systèmes d'information : la sécurité est un tout global qui impose de bien connaître les processus et les failles mais également de mettre en place des politiques de prévention.

> **« L'élu doit être moteur de l'objectif de cybersécurité afin d'embarquer toute la collectivité. »**

L'élu doit être moteur pour que cet objectif embarque toute la collectivité. C'est à cette condition que SMACL Assurances pourra être un véritable appui et un partenaire des territoires.

Face aux cyberattaques, votre collectivité mérite une meilleure solution !

Les collectivités sont de plus en plus touchées par les cyberattaques. Pour vous aider à protéger vos données, à préserver vos agents et vos administrés, nous vous proposons une offre complète avec :

> une solution **PRÉVENTION** qui réduit les impacts et les conséquences des attaques ;

> une **ASSURANCE*** qui prend en charge la gestion de crise et son coût.

Pour plus d'informations, contactez-nous par e-mail vosservices@smacl.fr

L'ASSURANCE DES TERRITOIRES

smacl.fr | **05 49 32 56 56** (prix d'un appel local)

***Offre réservée aux villes de plus de 5 000 habitants et aux intercommunalités de plus de 20 000 habitants.**

Distribué par SMACL ASSURANCES SA – Société anonyme au capital de 260 071 379,48 € – entreprise régie par le Code des assurances – RCS Niort n° 833 817 224. 141, avenue Salvador-Allende – 79000 NIORT. La solution prévention est en partenariat avec **CNPP** – Société à responsabilité limitée au capital de 8 500 000 €. Route de La Chapelle Réanville – CS 22265 – 27950 SAINT-MARCEL – Tél. 02 32 53 64 00. La solution assurance est assurée par **HISCOX SA France** – Capital social : 59 730 000 € – RCS Paris n° 833 546 989 – TVA Intracommunautaire n° FR88833546989. 38, avenue de l'Opéra – 75002 PARIS – hiscox.info@hiscox.fr – Tél. 01 53 21 82 82.

03/2023 – Conception : Direction de la marque et de la communication SMACL Assurances. Crédit photo : Gettyimages.

SMACL ASSURANCES

La prévention des cyber-risques

Si la plupart des collectivités ont aujourd'hui pris conscience des risques liés à la cybermalveillance, il reste un problème de taille : la complexité d'évaluer précisément ses impacts, de prioriser les actions à mettre en œuvre et de mobiliser les ressources adéquates.

Ce guide réalisé par SMACL Assurances, en partenariat avec le Centre national de prévention et de protection et l'Association des ingénieurs territoriaux de France, propose d'éclairer les décideurs des collectivités sur la menace cyber et de les assister dans leur compréhension des enjeux afin qu'ils puissent prendre les mesures nécessaires pour s'en protéger efficacement.

Nous sommes à votre écoute :

05 49 33 83 10
du lundi au jeudi de 8 h 30 à 18 h
et le vendredi de 8 h 30 à 17 h

prevention@smacl.fr

141, avenue Salvador-Allende
CS 20000 - 79031 NIORT CEDEX 9

Espace assuré
smacl.fr

CNPP AVEC AITF AVEC SMACL ASSURANCES

smacl.fr

Ne pas jeter sur la voie publique

SMACL ASSURANCES SA – Société anonyme au capital de 138 801 048 euros, entreprise régie par le Code des assurances – RCS Niort n° 833 817 224 – Siège social : 141, avenue Salvador-Allende – CS 20000 – 79031 NIORT CEDEX 9.
SMACL ASSURANCES – Société d'assurance mutuelle à cotisations fixes régie par le Code des assurances – RCS Niort n° 301 309 605.
Siège social : 141, avenue Salvador-Allende – CS 20000 – 79031 NIORT CEDEX 9

L'ASSURANCE DES TERRITOIRES

Octobre 2022 — Conception : Direction développement et communication SMACL Assurances, Agence 4août.