LA PRÉVENTION
DES CYBER-RISQUES

AITF
ASSOCIATION DES INGÉNIEURS TERRITORIAUX DE FRANCE

SMACL ASSURANCES
GROUPE VYV

AGIR ENSEMBLE POUR MAÎTRISER VOS RISQUES

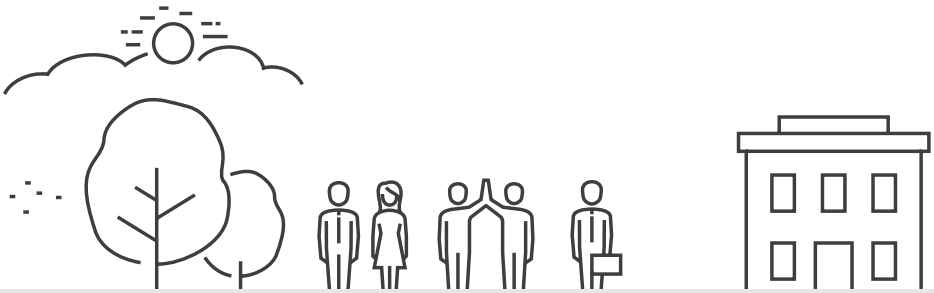
Parce qu'ils sont tous différents, accompagner les territoires est un défi quotidien qui appelle une expertise pointue et nécessite une parfaite connaissance de leur réalité institutionnelle, économique et sociale. En complément des garanties sur-mesure, SMACL Assurances accompagne ses sociétaires dans leur démarche de prévention des risques professionnels.

Les enjeux de la prévention des risques

ANTICIPER LES INCIDENTS

MAÎTRISER LES RISQUES

- Préserver la continuité de service
- Pérenniser votre plan d'assurance
- Protéger l'image de votre entité



Les 4 étapes d'une démarche de prévention

SMACL Assurances propose un plan de prévention personnalisé, adapté à votre système d'information, votre flotte automobile, votre patrimoine immobilier ou à la santé et la sécurité de vos agents et salariés.

Les 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.

Votre plan de prévention des cyber-risques

CNPP CYBERSECURITY Prévention et maîtrise des 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 aux sollicitations de ses sociétaires et les assister dans leur compréhension technique des enjeux, SMACL Assurances s'est rapprochée du CNPP Cybersecurity.

prevention@smacl.fr

05 49 33 83 10

LES GUIDES DE BONNES PRATIQUES SMACL

SMACL Assurances - 141 avenue Salvador Allende - 79000 Niort - Directeur de la publication : Jean-Luc de Boissieu, Président de SMACL Assurances - Directrice de la rédaction : Cécile Mexandeau - Rédactrice en chef : Valérie Cardon - Ont collaboré à ce numéro : Olivier Daroux, Anaïs Griman, Stéphane Neuilly (SMACL Assurances), Jean-Marc Jouvenaux, Guillaume Vitse (CNPP Cybersecurity) - Relecture : CorrectOgraphe - Crédits photos : Getty Images - ISBN : 978-2-9537147-3-9.

SOMMAIRE

INTRODUCTION

Les collectivités territoriales n'échappent plus à la cybermallveilance. Si elles n'en avaient pas pleinement conscience, elles ne peuvent plus nier ce risque désormais. Les nombreuses attaques récentes le démontrent : commune rurale, intercommunalité, métropole, région, centre hospitalier..., aucune structure n'est épargnée. Les conséquences d'un incident de cybersécurité ou d'une cyber-attaque peuvent être irrémédiables si elles conduisent à la destruction de fichiers ou à l'indisponibilité d'une ou plusieurs ressources névralgiques. La matière est abrupte : risque relativement récent, vocabulaire technique, fossé numérique entre les agents ou entre les élus..., la maîtrise n'est pas simple. Pour autant, la cybermalveillance appelle une cybervigilance à tous les niveaux de la collectivité !

Pour accompagner les décideurs dans la mise en œuvre de leur plan de prévention, SMACL Assurances et son partenaire CNPP Cybersecurity exposent les points de vigilance et présentent plusieurs bonnes pratiques à appliquer par les collectivités territoriales.

1 //

UN ENSEMBLE DE RISQUES AUX CONSÉQUENCES MULTIPLES

1. Un ensemble de risques aux conséquences multiples

La généralisation des échanges dématérialisés complexifie les architectures des systèmes d'information et les rend vulnérables aux attaques malveillantes. Les cyberattaques ont d'abord touché de grands groupes privés, puis des TPE et PME. Désormais, ce sont des acteurs publics, de toutes tailles, qui doivent affronter des ransomwares[1] ou autres menaces sur la sécurité de leurs données.

Dans ce contexte, comment protéger au mieux ses informations ?

LES CYBER-RISQUES AFFECTENT PARTICULIÈREMENT LES COLLECTIVITÉS

L'enjeu majeur de l'attractivité des territoires porte la transition numérique au cœur des collectivités. De nouveaux modes de gestion et services digitaux à destination des citoyens voient le jour. L'exposition au numérique est de plus en plus forte et engendre, de fait, de nouveaux risques.

Exemples d'expositions	Exemples d'atteintes et de menaces
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 (par exemple chèque livre ou chèque culture) nécessitant l'inscription et la gestion dématérialisées	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'enfant 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, etc.)	Attaques de type phishing[2] 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

[1]Un ransomware, ou rançongiciel, est un logiciel malveillant qui, lorsqu'il est activé, chiffre les données afin de les rendre inaccessibles sans une clef de chiffrement. Cette clef est supposée être délivrée à l'utilisateur par la personne malveillante en échange d'une somme d'argent.

[2]Une attaque par phishing, ou hameçonnage, désigne une technique utilisée par des personnes malveillantes dans le but de faire croire à l'attaqué qu'il s'adresse à un tiers de confiance (administration, collectivité, entreprise) afin de lui soutirer des informations ou de lui faire installer un logiciel malveillant sur son poste de travail.

Ces quelques exemples illustrent la nécessité de réaliser une analyse de risque pour à minima tout nouveau service mis en œuvre et en attendant de pouvoir l'appliquer à l'ensemble des services en production. Cette analyse porte sur quatre exigences de sécurité des systèmes d'information :

- la confidentialité ;
- l'intégrité ;
- la disponibilité ;
- la traçabilité.

> Risques liés à la confidentialité des informations collectées

La confidentialité est la propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou à des parties prenantes non autorisées. Cette notion est au cœur de toutes les préoccupations puisque les collectivités détiennent des fichiers de données personnelles et sensibles (données sociales ou fiscales notamment).

La fuite d'informations peut être découverte par un utilisateur des services (un administré découvre que ses données sont rendues publiques), ou par une alerte provenant d'un fournisseur ou d'un partenaire de la collectivité (services de l'État par exemple).

Cette anomalie peut provenir d'une configuration trop fragile de la solution ou du service proposé, l'utilisation de technologies obsolètes, ou encore un manque de restriction des droits d'accès.

Le risque sous-jacent est l'exploitation frauduleuse de ces données personnelles, particulièrement celles relatives à des informations de paiement.

> Risques liés à l'intégrité des flux traités

L'intégrité est la propriété selon laquelle l'information reste exacte et complète.

Cette notion prend notamment tout son sens dans le domaine sanitaire. Il serait inimaginable d'envisager l'opération d'un patient au sein d'un hôpital tout en sachant que son dossier médical n'est plus intègre. Le risque sous-jacent serait donc qu'une personne interne à cette structure ait modifié accidentellement, ou non, des données médicales : suppression des médicaments auxquels le patient est allergique, changement du groupe sanguin, etc. Les conséquences sur la vie sont réelles et graves.

Ce risque pourrait être rendu possible par une mauvaise conception de l'application utilisant ces données sensibles. C'est pourquoi l'erreur de manipulation est un élément à prendre en compte dès la conception d'un logiciel.

La fiabilité et l'intégrité des échanges de données bancaires entre une collectivité et un administré constituent un autre risque. Les attaques de type « man in the middle », de plus en plus courantes, consistent pour la personne malveillante à s'immiscer entre la collectivité et le citoyen afin de modifier le flux de la transaction.

> Risques liés à la disponibilité d'infrastructures mises à disposition

La disponibilité est la propriété selon laquelle l'information est accessible et utilisable à la demande par une entité autorisée.

Ces derniers mois, de nombreux services en ligne et ressources ont été rendus indisponibles par une attaque de type *ransomware*.

L'absence de maintenance appropriée d'un système d'information par des personnes qualifiées pourrait porter préjudice à la notion de disponibilité des infrastructures.

> Risques liés à la traçabilité des opérations

La traçabilité permet de surveiller tout accès ou modification d'une information et de relier ces derniers à une personne identifiée.

Plusieurs types d'événements nuisent à la traçabilité des opérations :

- Incendie, perte du stockage des journaux d'événements (logs)
- mauvaise implémentation d'une solution ne permettant pas de tracer les actions
- ransomware [1] sur les serveurs de journaux d'événements (logs).

La demande d'accès aux données personnelles est une autre source d'atteinte à la traçabilité. L'absence de vérification de l'identité du demandeur par le délégué à la protection des données (RGPD, voir page 13) entraîne une violation de la réglementation et des conséquences juridiques en matière de responsabilité.

[3]L'authentification forte désigne le fait de se connecter à un service en utilisant deux méthodes d'authentification sur trois possibles (ce que je sais (exemple : un mot de passe, un code pin) ; ce que je possède (exemple : un téléphone portable, une carte, une clef USB) ; ce que je suis (exemple : comportement, iris, digital).

> Quels impacts pour les collectivités ?

Un incident de cybersécurité engendré par une perte de confidentialité, d'intégrité, de disponibilité ou de traçabilité peut avoir de multiples impacts pour les collectivités. En voici quelques exemples :

- Impacts en termes financiers

- Pénalités financières pouvant aller jusqu'à 20 M€ pour une infraction au RGPD ;
- Frais liés à la remise en fonctionnement du système d'information après une attaque ou un incident (restauration des sauvegardes, recherche et éradication des logiciels malveillants ou correction des vulnérabilités informatiques).

- Impacts en termes d'image

- Publication des infractions à la demande de la CNIL ou dans la presse entamant la confiance des citoyens vis-à-vis de la collectivité.

- Impacts juridiques

- Poursuites d'administrés suite à la violation de leurs données personnelles.

- Impacts en termes d'activité

- Dégradation de l'offre de services aux administrés ;
- Blocage complet de l'activité.

LES ENJEUX DE SÉCURITÉ DANS LE CADRE DE L'EXTERNALISATION

Plusieurs parties de ce guide concernent l'externalisation de la gestion des systèmes d'information. En effet, il s'agit d'un point de vigilance essentiel dans la maîtrise de la cybercriminalité.

L'externalisation consiste à confier à un prestataire de services une partie ou l'ensemble de son système d'information. Cela peut être le cas, par exemple, d'une gestion de la paye externalisée pour laquelle un prestataire propose une solution logicielle incluant l'hébergement des données sur ses serveurs ainsi qu'un panel de services associés.

Ce type d'externalisation apporte des avantages certains, comme la gestion du maintien en condition opérationnelle et de la sécurité par un prestataire spécialisé.

Cependant, l'externalisation n'est pas sans risque et cela suscite les questions suivantes :

- Comment identifier et départager les responsabilités portées par les prestataires ?
- Comment s'assurer que les obligations et responsabilités des prestataires, notamment en matière de cybersécurité, sont bien appliquées ?
- Comment assurer une visibilité constante de l'ensemble de ses informations et de ses processus métiers, alors que ceux-ci sont de plus en plus répartis parmi différents systèmes d'information ?
- Comment réagir, continuer son activité et reconstruire quand le prestataire subit une attaque ?

L'externalisation de tout ou partie du système d'information est de plus en plus fréquente. Le mouvement des smart territoires (*smart city*[1] et smart villages) intensifie le recours à de multiples prestataires rendant ainsi les systèmes d'information de plus en plus complexes.

Attention !

Penser que l'externalisation est une simplification à l'extrême de la gestion d'une partie de son système d'information est une idée reçue. Bien que certaines tâches soient complètement déléguées au prestataire, les risques liés à cette externalisation sont partagés et non transférés. Les données et la responsabilité sont toujours portées par la collectivité, malgré cette externalisation.

[1]Smart city, ou ville intelligente, désigne une ville utilisant la donnée pour créer ou adapter ses services auprès du citoyen permettant la modulation des transports en commun en fonction de l'affluence, la gestion des réseaux énergétiques, la mise en place de capteurs pour surveiller les temps de stationnement ou l'utilisation des administrations en ligne, etc.

DES RÉGLEMENTATIONS ET DES RÉFÉRENTIELS SUR LESQUELS S'APPUYER

La protection des données fait l'objet d'un cadre juridique renforcé compte tenu des conséquences causées aux usagers et des obligations qui incombent aux responsables des traitements informatiques.

> Le Référentiel général de sécurité (RGS)

Le Référentiel général de sécurité (RGS), a pour objet le renforcement de la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives, notamment les collectivités territoriales.

Le Référentiel général de sécurité propose une méthodologie orientée autour de la responsabilisation des autorités ainsi qu'un ensemble de règles et bonnes pratiques que doivent mettre en œuvre les administrations lorsqu'elles recourent à des prestations spécifiques : certification et horodatage électroniques, audit de sécurité...

> Le Règlement général sur la protection des données (RGPD)

Les données personnelles des citoyens sont de plus en plus collectées, traitées et analysées pour pouvoir rendre des services à valeur ajoutée. À cela s'ajoute, comme indiqué précédemment, une complexification des systèmes d'information liée à des usages internes et externes.

Le Règlement général sur la protection des données (RGPD) est applicable à toute collectivité territoriale. Il a pour objectif d'encadrer le traitement des données personnelles sur le territoire de l'Union européenne.

Les questions suivantes peuvent se poser pour identifier les enjeux réglementaires :

- Quelles sont les informations traitées au sein du système d'information concerné ?
- Quels sont les partenaires impliqués dans ce système d'information ?
- Dans quel pays ces informations sont-elles physiquement traitées, stockées ou transmises ?

Il est à noter qu'une veille constante est nécessaire pour identifier les nouvelles lois, normes ou réglementations relatives à son activité. Ce travail peut être complexe mais des solutions existent pour agréger l'information applicable à son domaine d'activité.

Attention !

Le recours à un prestataire, bien qu'expert dans son domaine, pour la mise à disposition d'un service n'exonère pas la collectivité de la recherche de responsabilité. En effet, c'est bien la collectivité qui sera mise en demeure par la CNIL en cas de d'infraction dans ce domaine. Selon la CNIL, c'est l'entité en contact avec l'utilisateur final qui sera condamnée en cas d'infraction (les responsabilités peuvent toutefois être partagées avec les sous-traitants).

Avec le RGPD, les collectivités territoriales sont tenues de nommer un délégué à la protection des données.

Des centres de gestion départementaux proposent de mutualiser cette fonction et d'accompagner les collectivités adhérentes dans la mise en oeuvre de programmes de sensibilisation de leurs agents.

> Le règlement eIDAS

Le règlement eIDAS a pour but de cadrer l'utilisation de l'identification électronique et des services de confiance (signature électronique, horodatage électronique, recommandé électronique).

Le règlement prévoit un organe de contrôle qui prend notamment en charge la définition des modalités techniques permettant le respect des exigences du règlement ainsi que la qualification des prestataires de confiance établis sur le territoire français. En France, c'est l'ANSSI, autorité administrative placée sous l'autorité du Secrétariat général de la défense et de la sécurité nationale (SGDSN), qui assure ce rôle.

Découvrez le dossier spécial « collectivités territoriales » de la CNIL : https://www.cnil.fr/fr/collectivites-territoriales

et le guide dédié : https://www.cnil.fr/sites/default/files/atoms/files/cnil-guide-collectivite-territoriale.pdf

Les publications de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Guide d'hygiène informatique

https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

Cybersécurité, toutes les communes et les intercommunalités sont concernées, en partenariat avec l'Association des maires de France (AMF)

https://www.ssi.gouv.fr/

VOS QUESTIONS

Les activités sensibles font-elles l'objet d'une protection particulière ?

La Loi de Programmation Militaire (LPM) 2014-2019 renforce la sécurité des opérateurs d'importance vitale[6] (OIV) (opérateurs d'eau, activités judicicaires, activités d'approvisionnement en énergie, transports, etc.) et des opérateurs de services essentiels[7] (OSE) (opérateur tributaire des réseaux ou systèmes d'information) concernant leur système d'information.

Les OIV et OSE sont désignés par le gouvernement français en fonction de la criticité de l'activité de l'organisme. La liste des opérateurs est toutefois "confidentiel défense". Des collectivités territoriales peuvent être considérées comme OIV ou OSE en fonction de leur activité. Dans ce cas, il convient de s'assurer que les exigences légales qui leur incombent sont respectées et de contacter l'ANSSI le cas échéant.

Les collectivités territoriales déclarées comme OIV ou OSE doivent faire évaluer leurs systèmes d'information par des organismes de certification titulaires de qualifications adaptées (exemple : PASSI, pour Prestataire d'audit de la sécurité des systèmes d'information).

Quel programme d'assurance permet de couvrir ce risque ?

Votre contrat Dommages aux biens peut couvrir ce risque. Dans votre cahier des charges, prévoyez des clauses notifiant une couverture pour les incidents affectant le système d'information et résultant d'une fraude ou d'un virus informatique.
La fraude correspond dans cette situation aux pertes pécuniaires consécutives à une infraction pénalement qualifiée, à savoir :
- une escroquerie (article 313-1 du Code pénal) ;
- une extorsion (article 312-1 du Code pénal)
- un abus de confiance (article 314-1 du Code pénal) ;
- un faux ou usage de faux (article 441-1 et suivants du Code pénal).

Votre contrat Dommages aux biens prend en charge :
- les frais d'investigation,
- les frais de reconstitution des données,
- les frais de décontamination des systèmes d'information,
- les frais supplémentaires.

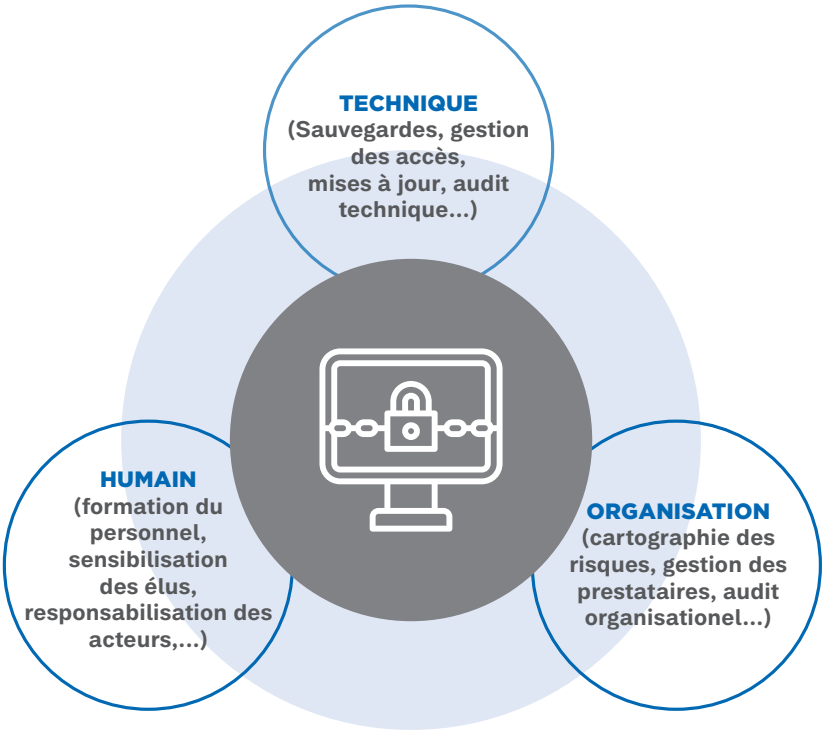
En complément, l'offre Solucrise de SMACL Assurances vous propose un panel de services vous accompagnant dans la gestion de crise, notamment en termes de communication.

[6]Un Opérateur d'importance vitale est un organisme, public ou privé, identifié par l'État comme ayant des activités indispensables à la survie de la nation.
[7]Un Opérateur de services essentiels est un organisme, public ou privé, identifié comme fournissant des services essentiels à la nation, étant tributaire d'un système d'information, et dont l'arrêt aurait un impact majeur sur le fonctionnement de la nation.

2 //

CONSTRUIRE UN PLAN DE PRÉVENTION EFFICACE

Ce guide des bonnes pratiques a pour but de donner les grandes orientations pour établir un dispositif de prévention des cyber-risques, lequel peut s'organiser autour de trois piliers majeurs :



Le dispositif mis en œuvre par la collectivité sera efficace s'il est accompagné d'un ensemble de procédures et de formations du personnel (la force d'une chaîne est fonction du maillon le plus faible).

Pour une sécurisation optimale, les moyens organisationnels, techniques et humains doivent être cohérents, fiables et suivis.

2.1 Mesures organisationnelles de prévention

DÉFINIR UN PROGRAMME ADAPTÉ DE GOUVERNANCE DE LA SÉCURITÉ

> Une gouvernance de risques « classique »

La gouvernance par les risques répond à un besoin simple : comment mettre en place les mesures de sécurité suffisantes et nécessaires pour protéger les données et l'activité ?

Ce sont les mêmes questions qui se posent pour construire un programme de prévention du risque routier, ou un document unique des risques professionnels, etc.

Ainsi, toute source de vulnérabilité doit faire l'objet d'une étude des risques et dommages associés en vue d'instaurer les mesures correctives.

L'avantage d'une gouvernance par les risques est également de pouvoir prioriser les actifs les plus sensibles afin de leur appliquer les mesures de sécurité pertinentes au vu des menaces pesant sur celle-ci.

Prenons l'exemple des outils nomades professionnels (tels que les ordinateurs portables, ou smartphones). L'ordinateur portable est un actif essentiel d'un système car il permet aux agents de travailler et de stocker une quantité importante d'informations dont certaines peuvent être considérées comme confidentielles.

Une gouvernance par les risques consisterait à identifier les vulnérabilités présentes sur l'ordinateur, apprécier la survenance d'un menace exploitant cette vulnérabilité et préconiser une ou plusieurs mesures de sécurité pour corriger cette vulnérabilité.

Dans le cas présent, l'ordinateur pourrait être considéré comme vulnérable en raison du risque d'attaque en l'absence de protection antivirus. L'impact de la réalisation du risque pourrait être estimé majeur au vu de la criticité des données présentes. L'installation d'un antivirus permettrait de réduire la survenance de ce risque. Sans oublier le risque de vol qui doit faire l'objet d'une sensibilisation particulière.

> Définition des responsabilités sur le maintien des différentes briques du système d'information

Chaque collectivité territoriale est unique par son histoire, son métier et les personnes qui la composent. Cependant, afin de protéger la structure et les données dont elle dépend contre un éventuel conflit d'intérêt pouvant mener une mauvaise prise de décision, Il convient d'appliquer et de segmenter les tâches de rôles clefs de l'organisation.

Ces acteurs sont considérés comme éléments essentiels de la sécurité de l'information :

- la direction générale des services : organe de décision qui, généralement, porte le plus souvent les risques pouvant peser sur l'organisation ;
- la direction des systèmes d'information (DSI) : organe chargé d'assurer l'exploitation du système d'information dans sa globalité (briques internes comme externes) ;
- le responsable de la sécurité des systèmes d'information (RSSI) : agent chargé d'assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité des actifs de l'organisation.
- le délégué à la protection des données (DPD) : veille au respect du RGPD (fonctions encadrées par l'article 39 du RGPD).

De par leurs missions de contrôle, le DPD et le RSSI doivent bénéficier d'un rattachement hiérarchique et d'une indépendance fonctionnelle leur permettant de remonter à la direction générale des services des alertes ou des manquements pouvant impacter l'organisation. Le contraire pourrait induire de mauvais choix dans les mesures de sécurité à appliquer.

Les agents des collectivités sont également des acteurs majeurs. Ils doivent suivre les formations / sensibilisations et alerter en cas d'éléments suspects. Les agents sont la première ligne de défense du système d'Information.

l'ANSSI, l'agence gouvernementale de la cybersécurité

Autorité nationale en matière de sécurité et de défense des systèmes d'information, l'ANSSI constitue un réservoir de compétences qui met son expertise et assiste les administrations et les opérateurs d'importance vitale.

Elle est chargée de la promotion des technologies, des systèmes et des savoir-faire nationaux. Elle contribue au développement de la confiance dans le numérique.

En savoir plus sur https://www.ssi.gouv.fr/

Des délégués régionaux sensibilisent les acteurs locaux du public et du privé aux bonnes pratiques informatiques.

https://www.ssi.gouv.fr/agence/cybersecurite/action-territoriale/

Le portail https://www.cybermalveillance.gouv.fr/ est une mine d'informations intéressantes pour les entreprises, les administrations et les particuliers sur les menaces numériques et les moyens de se défendre.

> Choix et gestion des fournisseurs en fonction des données traitées et hébergées

Le recours à des fournisseurs ou prestataires dans la gestion d'un système d'information est devenu la norme aujourd'hui. Cette pratique permet d'optimiser les coûts mais ne reste pas sans risque.

De multiples critères permettent de reconnaître l'expertise d'un fournisseur : « certification ISO/CEI 27701 » (données personnelles), « certification ISO/CEI 27001 », etc. Comment s'y retrouver parmi ces appellations et quels sont les moyens à mettre en œuvre pour permettre une bonne gestion des fournisseurs ?

Il convient tout d'abord de cartographier toute partie prenante externe apportant un service ou une solution (gestion externalisée de la paie, hébergement de l'infrastructure, infogérance, etc.).

Seront priorisés les fournisseurs qui auront un impact fort en termes de disponibilité, d'intégrité ou de confidentialité sur les données ou processus. Selon leurs incidences sur le système d'information, il sera nécessaire d'établir des exigences de sécurité afin de limiter les risques vis-à-vis de l'accès aux actifs de l'organisation.

La signature d'un accord de confidentialité avec le prestataire, d'un management par les risques de sécurité de l'information, l'obtention d'une certification ISO/CEI 27001 et/ou 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 !

L'obtention d'une certification ISO/CEI 27001, bien que gage d'investissement sur la sécurité de l'information de la part d'une organisation, n'est pas synonyme de perfection ou d'absence de risque. Il est nécessaire de confronter le fournisseur sur les mesures en place et d'analyser le périmètre de la certification.

> Continuité d'activité

La continuité d'activité est une composante essentielle au sein des organismes. Elle a notamment été testée par la force des choses durant la crise sanitaire au printemps 2020. Deux cas de figure se sont présentés : d'une part, les organismes préparés, et d'autre part, des organismes ayant dû s'adapter sur le moment.

Afin de se préparer au mieux, il est nécessaire d'énoncer plusieurs scénarios plausibles : une pandémie, telle que celle de la Covid-19, mais également un incendie, une panne électrique majeure ou encore la destruction d'un bâtiment.

Ces scénarios, différents, mettent en exergue les dépendances des collectivités envers des bâtiments, du personnel, des technologies, ou encore des prestataires. Afin de prioriser les actions de reprise, il est donc 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 permettant d'assurer ces activités lorsque celles-ci sont soumises aux scénarios de continuité d'activité (fournir des ordinateurs portables, disposer des sites de reprise, identifier des canaux de communication différents via des applications spécifiques, etc.)
- de tester ces mesures dans le cadre d'exercices en situation réelle.

C'est en testant de manière régulière, et sur des situations différentes, que le personnel sera sensibilisé, que les méthodes seront éprouvées et que les bons réflexes seront acquis.

ISO/CEI 22301 et management de la continuité d'activité

La norme ISO/CEI 22301 précise les exigences d'un système de management afin de protéger la collectivité des incidents perturbateurs, de réduire leur probabilité et garantir la récupération.

Elle est la référence en la matière pour concevoir et piloter un plan de continuité d'activité.

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

EXTERNALISER : LES BÉNÉFICES ET LES RISQUES

> Le choix du sous-traitant

L'externalisation d'une partie ou de la totalité de son système d'information impose de renforcer le contrôle de ses sous-traitants, d'une part quant à la gestion des données personnelles mais également de la gestion de la sécurité.

Il convient donc de s'interroger quant au choix d'un sous-traitant :

- Possède-t-il des certifications relatives à son activité, comme l'ISO/CEI 27001, ou est-il en voie de se faire certifier ?
- A-t-il nommé un responsable de la sécurité des systèmes d'information et un délégué à la protection des données ?
- Une stratégie de management par les risques a-t-elle été mise en œuvre par le prestataire, se matérialisant par un PAS (Plan assurance sécurité) ?
- Au regard de son activité, est-il en capacité d'apporter une assurance sur les contrôles spécifiques au service qu'il fournit ?

Ces questions, somme toute relativement simples, permettent cependant de mieux cerner son appétence à la sécurité : l'externalisation doit apporter une assurance sur la correcte gestion du service concerné, et non créer de nouveaux risques majeurs.

Des mesures de sécurité spécifiques devront notamment être étudiées avec précision :

- la gestion des sauvegardes et la durée de rétention des informations assurée ;
- la continuité d'activité, devant être cohérente avec sa propre stratégie (pendant combien de temps le service peut-il être inaccessible ?) ;
- la gestion du chiffrement et l'assurance que toute information sensible est correctement protégée ;
- la gestion de ses propres sous-traitants à qui le prestataire doit répliquer ses propres exigences ;
- la gestion des développements informatiques dans l'optique de créer des applications, respectant des standards connus comme l'OWASP* ;
- la sensibilisation des équipes et, plus globalement, les compétences mises à disposition par le partenaire ;
- la 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 de la sélection d'un prestataire.

*Open Web Application Security Project, fournit de nombreux travaux et recommandations pour sécuriser les applications web.

> Quelles mesures organisationnelles de prévention pour la gestion en interne du système d'information ?

La gestion en interne du système d'information permet, a contrario, de centraliser toutes les fonctions d'administration et d'exploitation des briques le composant. Même si cette tendance n'est pas d'actualité, certaines collectivités font le choix d'internaliser de nouveau certaines fonctions plutôt que de les déléguer à un tiers. Pour les petites collectivités, c'est la possibilité de concevoir une infrastructure simple et peu coûteuse.

Dans le cas d'une internalisation, les risques seront moins focalisés sur la gestion des partenaires, mais plutôt sur la délivrance et la pérennité du service. Il conviendra donc d'aborder les sujets sous un angle différent :

- La gestion des sauvegardes : la solution permet-il de récupérer l'information avec un niveau d'assurance suffisant, en cas de sinistre sur le site principal par exemple ? Le matériel est-il encore sous garantie ? Les sauvegardes ont-elles été testées ?
- La continuité d'activité : le système mise en œuvre permet-il de continuer à travailler en cas de panne d'électricité, de pandémie, d'inondation ?
- La gestion du chiffrement : les informations sensibles sont-elles protégées contre le vol et accessibles uniquement au personnel habilité ?
- La gestion des prestataires : les licences et les technologies utilisées sont-elles supportées sur une période pérenne ?
- Les procédures de développement et d'exploitation, couvrant notamment l'utilisation de données de test, la sécurité dans les communications, la journalisation sont-elles formalisées, connues des équipes et suffisantes ?
- La sensibilisation des équipes, basée sur leurs compétences, permet-elle de s'adapter à l'évolution des menaces ?
- La gestion des incidents est-elle définie et le circuit de traitement est-il identifié ?

Dans les deux cas, l'utilisation de référentiels reconnus, comme l'ISO/CEI 27001 et l'ISO/CEI 27002, permet d'assurer une couverture minimale des mesures à respecter. Des guides, réalisés et fournis par l'ANSSI, permettent également d'obtenir une liste de contrôles simples et pragmatiques.

“Interview”

Benoît liénard,
Directeur de Soluris

- **Quelles sont les missions, la vocation de Soluris ?**
  Soluris est le syndicat de mutualisation informatique des collectivités territoriales de Charente-Maritime, créé il y a une trentaine d'années pour mutualiser les coûts matériels. Nos missions autour des usages se sont développées avec l'arrivée d'Internet et de son impact dans l'organisation des collectivités, en interne mais aussi dans leurs relations avec l'État ou les administrés.

- **Quelles sont les mesures le plus couramment déployées pour prévenir les cyberattaques ?**
  Les mesures prioritaires sont des mesures organisationnelles et ne relèvent d'ailleurs pas toujours d'une solution informatique. Par exemple, on ne classe pas un document confidentiel dans un tiroir ouvert à tous, il est dans un coffre. Pour un fichier, c'est la même logique : un fichier sensible doit être conservé dans un endroit sécurisé, même si c'est plus simple au quotidien de pouvoir ouvrir ce fichier depuis son bureau. Les cyber-risques nous contraignent à raisonner par risque et non par habitude.

- **Comment êtes-vous organisés avec les structures homologues des autres départements ?**
  Nous sommes membres de l'association Déclic (www.asso-declic.fr) qui réunit des structures de mutualisation de toute la France (syndicats mixtes, GIP, associations, centres de gestion...). Le maillage des structures d'accompagnement permet quasiment à toute collectivité, quel que soit son département, d'accéder à une prestation telle que celle que nous proposons pour les communes de Charente-Maritime. Plusieurs réussites sont à saluer grâce à la force du groupe.

  D'abord, la collaboration avec l'ANSSI qui a conduit à la création d'un pôle collectivités. Avec l'ANSSI nous nous entendons sur un ensemble de bonnes pratiques et de recommandations à mettre en œuvre dans les collectivités. L'ANSSI propose aux membres de Declic des formations pour actualiser nos connaissances sur des évolutions techniques et réglementaires.

  Enfin, Soluris a conçu, pour les communes, un logiciel d'accompagnement à la mise en place du RGPD. Nous ne trouvions pas sur le marché ce qui répondait à nos besoins, nous l'avons donc fait développer sous le nom de MADIS et l'avons partagé aux membres de Declic qui souhaitaient le diffuser à leurs adhérents. MADIS est aujourd'hui le premier logiciel sur ce sujet, c'est la force du réseau qui a permis ce succès.

Vrai/ faux

Un prestataire certifié est un gage de confiance

Vrai mais encore faut-il qu'il puisse présenter les mesures pour assurer la sécurité des données hébergées, les délais d'intervention en cas d'incident de sécurité, les dispositifs de récupération de données, et tout élément qui lui a permis d'être certifié.

La sous-traitance des missions de sécurité à un prestataire permet à la collectivité d'éviter d'être mise en cause notamment devant la CNIL

Faux, les responsabilités sont partagées. Même en cas de sous-traitance, le responsable d'un traitement (base de données personnelles) est la collectivité territoriale qui aurait sous-estimé, par exemple, le risque de vol de données, même si ce vol a lieu chez le sous-traitant.

Le contrat avec le sous-traitant doit prévoir que celui-ci met en œuvre, par exemple, les moyens permettant de garantir la confidentialité et l'intégrité. Le sous-traitant est reconnu coresponsable en cas de mise en cause, que le contrat ait prévu les mesures ou non.

L'analyse des risques s'apparente à l'évaluation des risques professionnels nécessaire à la réalisation du document unique

Vrai, il s'agit d'un parallèle évocateur pour démontrer que la prévention des cyber-risques est à mener comme toute démarche de prévention des risques, quel que soit le domaine de ces derniers. Ainsi tout dispositif de prévention comprend ces quatre étapes :

- l'identification des risques ;
- la réalisation d'un plan d'action ;
- le déploiement de ce plan, notamment les actions de formation ;
- l'évaluation annuelle (au moins) des mesures et l'ajustement, si nécessaire, notamment au regard d'un nouveau risque ou d'un nouvel élément de prévention.

2.2 Mesures techniques de prévention

La partie technique donne un aperçu des informations qui peuvent être complétées par des ouvrages dédiés aux responsables des systèmes d'information.

CHOISIR DES SOLUTIONS RÉPUTÉES ROBUSTES

La sécurité des systèmes d'information ne repose pas uniquement sur la promesse des produits de sécurité, vantée par de nombreuses solutions proposées sur le marché. En effet, la configuration des outils, l'environnement, l'exposition, ainsi que la motivation des personnes malveillantes sont également à prendre en compte.

Pour illustrer ce propos, prenons l'exemple récent d'un des plus grands hébergeurs français victime d'une attaque par déni de service distribué[4]. Ce type d'attaque consiste à surcharger un service jusqu'à ce qu'il ne soit plus disponible. L'acte malveillant a impacté des milliers de caméras de surveillance, identifiées a posteriori comme vulnérables mais qui n'avaient pas fait l'objet de mesures correctives.

Intégrer un composant au sein de son système d'information ne se fait pas sans réflexion. La question doit se poser, en amont, de la nécessité et du bien-fondé de cette brique informatique. Pour cela, des initiatives ont été lancées. L'ANSSI propose des certifications de produits (Critères communs (CC) et Certificat de sécurité de premier niveau (CSPN) qui permettent de garantir un niveau de sécurité pour l'outil en question.

« FERMEZ LES PORTES D'ENTRÉE INDÉSIRABLES »

« Le niveau de sécurité d'un outil ne garantit pas une absence de risque. L'utilisation d'un composant passe par son intégration dans le système. Cette intégration doit faire l'objet d'une réflexion et d'un durcissement spécifique. Le durcissement, plus communément appelé « hardening », consiste à fortifier un équipement réseau, un serveur, un poste client ou plus généralement une brique d'un système d'information dans le but d'en augmenter son niveau de sécurité. Ports ouverts, comptes par défaut, protocoles obsolètes, fonctions non utilisées et donc vulnérables avec le temps : il existe de nombreuses « options » nécessitant d'être paramétrées pour supprimer d'éventuelles portes d'entrées indésirables.
Le site Shodan.io permet de constater l'ampleur de ces configurations un peu laxistes. Ce sont des centaines de milliers de serveurs, ordinateurs, caméras, objets connectés qui peuvent être accessibles depuis n'importe quel poste connecté à l'extérieur.
Plusieurs guides proposés par le STIG (Security Technical Implantation Guides), ou le CIS (Center for Internet Security) et bien sûr l'ANSSI peuvent être utilisés afin de parfaire la sécurité des actifs d'une organisation. »

Loick PELET
Directeur du Pôle Technique et Sécurité Opérationelle (TSO) CNPP Cybersecurity

[4] L'attaque par déni de service ou en déni de service distribué vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service. (Source : cybermalveillance.gouv.fr)

METTRE EN ŒUVRE DES SYSTÈMES D'ARCHIVAGE ÉLECTRONIQUE

L'archivage électronique est un principe de stockage, sur le long terme, des informations nécessitant une attention particulière en termes de durée de conservation mais également d'intégrité.

Les délais de conservation des informations sont réglementés en fonction du type d'information concerné, de l'usage de l'information, ainsi que de la finalité. L'utilisation de solutions robustes d'archivage électronique permet une conservation pérenne, tout en se basant sur des principes de non-répudiation comme l'usage de signatures électroniques.

Enfin, l'utilisation d'une clause de séquestre est nécessaire lors de la sélection de partenaires pour des développements spécifiques à son besoin. Cette clause permettra la récupération du code source développé lors de la prestation, en cas de litige ou de faillite du partenaire, afin de pouvoir assurer une continuité dans la réalisation du service (après migration).

METTRE EN ŒUVRE UN SYSTEME D'AUTHENTIFICATION NUMÉRIQUE

Le RGS et l'eIDAS traitent sensiblement des mêmes sujets, à savoir l'authentification, la signature électronique, l'horodatage et la confidentialité.

Ils définissent même la définition de trois niveaux de certificats, permettant un niveau d'assurance plus ou moins élevé quant à l'identification de l'auteur d'un message électronique :

- signature électronique simple : permet d'authentifier des documents présentant un risque relativement faible, comme un contrat d'assurance ;
- signature électronique avancée : permet d'authentifier des documents de risque moyen et de réduire substantiellement le risque d'usurpation ;
- signature électronique qualifiée : permet d'authentifier des documents considérés comme de risque élevé, à savoir des factures, des opérations bancaires ou des réponses à appels d'offres.

Ces dispositifs de signature électronique réglementés permettent d'établir la confiance dans l'usage de documents partagés entre tiers. En effet, la signature électronique permet d'attester à un *instant T* que telle personne, ou tel organisme, a bien été à l'origine du message.

FAIRE AUDITER SON SYSTÈME D'INFORMATION

Auditer son système d'information de manière régulière permet d'assurer un niveau continu de sécurité. En effet, les mesures mises en œuvre à un *instant T* ne sont peut-être plus suffisantes à T+1 et pour plusieurs raisons : nouveau prestataire en charge de la maintenance applicative, renouvellements du personnel induisant des rotations dans les comptes créés et à supprimer, technologies non actualisées ou supprimées, nouvelles vulnérabilités nécessitant des composants de sécurité complémentaires…

Il est donc très fortement recommandé de procéder à la mise en œuvre d'un programme d'audit, permettant de définir sur une période donnée l'ensemble des tests nécessitant d'être effectués, en fonction de la sensibilité des briques du système d'exploitation.

Il existe deux grandes familles d'audits :

- Les audits organisationnels permettent de vérifier le fonctionnement d'une application, de processus conformément à un référentiel (interne ou réglementé). La réalisation d'audits de partenaires est une pratique de plus en plus fréquente, permettant de s'assurer que le niveau d'engagement contractuel est à la hauteur de la prestation rendue, a minima sur les aspects de sécurisation du système. Les analyses de risque entrent également dans le cadre d'audits organisationnels.
- Les audits techniques permettent d'identifier des vulnérabilités présentes sur une application ou un système d'information. Différents types d'audits techniques peuvent être réalisés, en fonction de l'objectif visé :
  - Les tests d'intrusion (simulations d'attaques) sont les plus courants ;
  - L'identification des vulnérabilités à spectre plus large et complémentaires aux tests d'intrusion ;
  - Des audits de configuration, d'architecture ou encore de code source permettent d'analyser avec des visions différentes une brique ou un segment du système d'information.

La réalisation d'audits doit être une pratique normée ; une rigueur est indispensable dans la correction et le suivi des vulnérabilités détectées lors de ces audits.

VOS QUESTIONS

Que faire en cas de cyberattaque ?

Cybermalveillance.gouv.fr a pour mission 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.

En cas de cyberattaque :

1. Conservez ou faites conserver les preuves de l'attaque par un professionnel, notamment un exemple de message piégé, les fichiers de journalisation (logs) de votre pare-feu, des copies physiques des postes ou serveurs touchés (à défaut, conservez leurs disques durs)
2. Connectez-vous sur : *https://www.cybermalveillance.gouv.fr/*
3. Cliquez sur : Assistance
4. Choisissez « professionnel » puis « administration et collectivité » et suivez les indications !

Faut-il payer la rançon ?

De nombreuses collectivités territoriales ont été victimes de *ransomwares*, ces virus qui réclament une rançon en échange du déblocage de l'accès au système d'information. Il est communément recommandé de ne pas payer la rançon.

En effet, le paiement de celle-ci ne garantit pas un retour à la normale. Par ailleurs, cela pourrait alimenter un système mafieux qui se cache le plus souvent derrière ces attaques.

2.3. Les moyens humains

SENSIBILISER ET FORMER SON PERSONNEL AUX RISQUES ENCOURUS ET AUX RÉGLEMENTATIONS EN VIGUEUR

Les attaques envers des collectivités, des hôpitaux ou des entreprises n'ont jamais été aussi fréquentes. Il est vital de traiter toutes les thématiques de la sécurité de l'information dans la sensibilisation de tous les acteurs de la collectivité.

La sensibilisation et la formation du personnel des collectivités sont au cœur de toute stratégie de sécurité de l'information. Elle est la première ligne de défense contre les menaces externes et internes à une organisation.

Tout comme nous formons le personnel au massage cardiaque ou à l'évacuation des locaux en cas d'incendie, il est primordial de former les collaborateurs à la détection d'anomalies (comportement anormal de son ordinateur, appels à but malveillant[9]...).

La sensibilisation du personnel est l'une des plus grandes priorités en termes de sécurité de l'information.

Au-delà des aspects de prévention technique, il est nécessaire de former les agents au respect des réglementations auxquelles la collectivité est soumise, par exemple celles relatives aux données personnelles. Correctement formés, les agents sont en capacité d'alerter le délégué à la protection des données sur un processus non conforme au RGPD.

5 CRITÈRES POUR UN MOT DE PASSE PROFESSIONNEL SÉCURISÉ

Il est recommandé de **modifier régulièrement le mot de passe** d'ouverture de session.

[9]L'ingénierie sociale, ou social engineering, désigne une tentative de la part d'une personne malveillante de récupérer des informations confidentielles en utilisant son charisme ou la crédulité de son interlocuteur mais également toute forme de tromperie (en se faisant passer pour une personne légitime grâce à des informations collectées sur internet - et disponibles publiquement - par exemple).

SENSIBILISER LES USAGERS

Les usagers des services des collectivités sont également soumis à des menaces grandissantes. Les tentatives de *phishing* se faisant passer pour une administration (impôt, mairie, assurance maladie, etc.) sont croissantes. Prendre en compte ce risque en adaptant sa communication (ne pas mettre de lien dans les mails par exemple) et ses méthodes d'authentification (via une authentification forte) permet de réduire les répercussions au niveau des administrés : la réduction d'incidents induit la baisse de régulations et une activité concentrée sur l'essentiel, c'est-à-dire la fourniture du service attendu.

Un accompagnement éducatif complète nécessairement les mesures techniques et organisationnelles. Effectuer des campagnes de rappel aux bonnes pratiques de sécurité de l'information fait partie des règles absolues de la sécurité.

3 CONSEILS PRÉCIEUX

1. Éviter de brancher une clé USB ou un disque dur externe personnels ou inconnus sur son poste de travail. Ce sont des vecteurs de virus.
2. Ne pas ouvrir de pièces jointes provenant de sources inconnues, que cela soit par mail ou support tiers.
3. Ne pas cliquer sur des liens hypertextes quand l'expéditeur d'un e-mail est inconnu ou peu sûr.

VOS QUESTIONS

Comment dédramatiser le poids du risque de cyberattaque ?

La sensibilisation passe par une communication régulière de la part de l'autorité territoriale.

Conseil : donner des astuces pour protéger contre des risques qui touchent à la sphère privée en vue d'appliquer les bonnes pratiques dans la sphère professionnelle. L'exemple des mails frauduleux ou des sites non sécurisés.

Quelle attitude adopter en cas d'attaque par rançongiciel ?

Un message bloquant l'accès à votre site internet prétend détenir les données de votre système d'information et réclame une rançon pour ne pas divulguer ces données.

Même si chacun est libre d'agir comme il l'entend, il est fortement recommandé de ne pas payer la rançon. D'une part, rien ne garantit que vos données soient à nouveau accessibles, et, d'autre part, la rançon pourrait alimenter un système mafieux qui dépasse bien souvent les frontières d'un pays.

Se reporter aux conseils de Cybermalveillance.gouv.fr.

CONCLUSION

Se numériser, c'est faciliter la vie de ses administrés mais c'est également générer de nouveaux risques. La gestion d'un système d'information, même externalisé, implique :

- Des ressources financières permettant d'assurer l'identification des risques portant sur le système d'information et les services rendus aux citoyens, la mise en œuvre des mesures de sécurité nécessaires pour réduire les risques identifiés, la gouvernance des fournisseurs et prestataires à qui des délégations ont été attribuées. En moyenne, c'est 10 à 20 % du budget IT devant être dédié à la sécurité des systèmes d'information.
- Des ressources humaines et des compétences permettant d'assurer les responsabilités critiques liées à la sécurité de l'information et au respect des réglementations en vigueur ; ces ressources pouvant être internes aux collectivités, ou externalisées notamment par le biais de syndicats informatiques, dans l'optique de la mutualisation des compétences.

Toutes les préconisations de ce guide ne sauraient être appliquées correctement sans l'appui et le parrainage des élus et de la direction générale des services. C'est grâce à eux que la conduite du changement pourra se réaliser et que les équipes appliqueront les consignes du responsable de la sécurité des systèmes d'information et du délégué à la protection des données.

La mise en œuvre de ces mesures, qu'elles soient organisationnelles comme la réalisation d'une analyse de risques et l'accompagnement à la conformité, qu'elles soient techniques comme la réalisation de tests d'intrusion ou de scans de vulnérabilités, nécessite des compétences spécifiques ; CNPP Cybersecurity, partenaire de SMACL Assurances, est en capacité de vous accompagner sur ces sujets.

Dans la même collection :

- LA PRÉVENTION DU RISQUE MALVEILLANCE SUR LE PATRIMOINE DES COLLECTIVITÉS
- LE DOCUMENT UNIQUE DE VOTRE ASSOCIATION
- MENER UNE DÉMARCHE DE PRÉVENTION DE L'ABSENTÉISME

Disponibles sur smacl.fr

Suivez-nous sur @SmaclAssurances

SMACL ASSURANCES - *141, avenue Salvador Allende*
CS 20000 79031 Niort Cedex 9

LA MUTUELLE D'ASSURANCE DES TERRITOIRES

SMACL ASSURANCES
GROUPE VYV

01/2021 - Conception : Direction de la Marque et de la Communication de SMACL Assurances - Crédit photo : Gettyimages.