Hes·so
Haute Ecole Spécialisée
de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences and Arts
Western Switzerland

MSc HES-SO en Business Administration

Orientation :
Management des Systèmes d'information

Etude sur la cybersécurité des communes vaudoises

Création d'un outil d'auto-évaluation de la maturité

Réalisé par

Stéphane Olivier Paul Müller

Sous la direction de
Prof. Dr. Jean-Luc Beuchat

Lausanne, le 17.08.2022

Table des matières

Table des illustrations

Déclaration sur l'honneur

J'atteste que le travail rendu est le fruit de ma réflexion personnelle et a été rédigé de manière autonome. Je certifie que toute formulation, idée, recherche, raisonnement, analyse ou autre création empruntée à un tiers est correctement et consciencieusement mentionnée comme telle, de manière claire et transparente, de sorte que la source en soit immédiatement reconnaissable, dans le respect des droits d'auteur et des techniques de citations. Je suis conscient que le fait de ne pas citer une source ou de ne pas la citer clairement, correctement et complètement est constitutif de plagiat. Au vu de ce qui précède, je déclare sur l'honneur ne pas avoir eu recours au plagiat ou à toute autre forme de fraude.

Lausanne, le 17.08.2022

Stéphane Müller

Remerciements

Au Prof. Dr. Jean-Luc Beuchat pour son encadrement et ses conseils.

A Monsieur Eloi Fellay, directeur de l'UCV et à Madame Valérie Moreno, Webmaster de l'UCV, pour leurs précieux conseils dans la réalisation de mon questionnaire aux communes et pour m'avoir aidé à contacter les responsables communaux.

A Monsieur Marc Barbezat, pour m'avoir accordé un entretien me permettant d'avoir le point de vue des autorités cantonales.

Aux 72 responsables communaux qui ont pris le temps de répondre à mon questionnaire.

A Madame Sophie Müller pour ses corrections orthographiques.

Abréviations

UCV :	Union des Communes Vaudoises
AVRIC :	Association Vaudoise des Responsables Informatiques Communaux
NCSC :	Centre national pour la cybersécurité
ISO :	Organisation internationale de normalisation
NIST:	National Institute of Standards and Technology
TIC :	Technologies de l'information et de la communication
DDOS :	Distributed Denial of Service
CFC :	Certificat fédéral de capacité
CRUD :	Create, Read, Update, Delete

Résumé

En 2021, plusieurs communes du canton de Vaud ont fait l'objet d'articles dans les médias après avoir été victimes d'attaques informatiques ayant totalement ou partiellement affecté leur fonctionnement et ayant donné lieu à des vols de données des citoyens. L'annonce récente de la part des autorités Russes que la suisse était considérée comme un état hostile augmente encore ce risque.

Selon les recherches effectuées, il n'y a pas aujourd'hui de véritables données sur le mode de fonctionnement des communes au niveau de l'informatique et plus précisément de la sécurité. Ce manque de données sur la gestion de l'informatique dans les communes du canton de Vaud représente un problème pour la mise en place d'une politique sur le plan cantonal ou des faitières de communes.

Voici les questions que nous allons aborder dans ce travail de master : Comment les communes gèrent-elles leur informatique, quel est l'état actuel de la cybersécurité et comment envisagent-elles l'avenir ?

Grâce à ces données récoltées auprès des communes du canton, nous allons créer un outil qui sera utile aux responsables politiques locaux, leur permettant d'établir un premier audit de la situation, de se poser les bonnes questions et de faciliter la participation démocratique pour mettre en place une stratégie.

Mots clés : HES-SO, cybersécurité, communes vaudoises, administration publique, informatique

1 Introduction

1.1 Contexte

En 2021, plusieurs communes du canton de Vaud ont fait l'objet d'articles dans les médias après avoir été victimes d'attaques informatiques ayant totalement ou partiellement affecté leur fonctionnement et ayant donné lieu à des vols de données des citoyens.

Parmi ces dernières, la commune de Montreux a subi le 10 octobre 2021 une attaque informatique de type rançongiciel (Ransomware) durant laquelle des données ont été chiffrées [1]. Cette attaque a impacté les services de la commune de Montreux, de la commune de Villeneuve, de l'association Sécurité Riviera (en charge des services de secours de la région (police, pompiers et protection civile), de la commune de Veytaux ainsi que d'associations liées aux communes telles que l'ARAS en charge de la gestion des assurances sociales [1]. Selon le communiqué publié par les autorités compétentes, en collaboration avec les autorités cantonales, fédérales et avec l'aide de partenaires externes spécialisés, les infrastructures ont pu être rétablies dès le 19 octobre [2]. C'est ainsi que durant 9 jours les activités du service public de ces institutions ont été impactées par cette attaque.

Une autre attaque plus tôt dans l'année a également été largement médiatisée. La commune de Rolle a également subi une attaque de type rançongiciel durant laquelle des données confidentielles ont été chiffrées, volées et publiées sur le darknet. Parmi les données qui ont été publiées, on retrouve entre autres des données personnelles de citoyens, telles que des numéros AVS, des notes scolaires et diverses coordonnées. Selon les dernières estimations, 5395 habitants auraient été impactés par cette fuite de données [3]. Cette attaque a eu lieu le 30 mai 2021 mais son existence n'a été révélée par la presse nationale que le 20 août 2021, lorsque des journalistes du média Watson ont publié une enquête sur le sujet [4]. Plus que l'attaque en elle-même, ce qui a créé la polémique est le manque de transparence dont ont fait preuve les autorités communales, ainsi que leur manque de préparation et de réaction lorsque les données volées ont été mises en ligne sur le darknet.

Dans leur rapport de situation de 2021 [5], les services de renseignement suisses identifient un risque important d'attaques à cause notamment de la crise du Covid19. Les entreprises et les administrations publiques ont dû développer en urgence des solutions pour permettre le télétravail, ce qui a eu pour effet de faire passer la sécurité informatique au second plan. L'objectif à ce moment-là était de permettre aux gens de travailler depuis la maison tout en garantissant le bon fonctionnement des administrations publiques. Ces solutions de secours ont eu créé de nombreuses vulnérabilités dues notamment aux nombreux points d'accès pour se connecter aux réseaux internes à l'entreprise, la multiplication des applications pour le travail à distance et l'implication de nouveaux fournisseurs de services.

Les services de renseignement identifient également une forme de professionnalisation des cybercriminels travaillant potentiellement pour des entreprises étrangères en concurrence avec les entreprises suisses ou avec des gouvernements de pays hostiles. Ils prédisent un risque accru d'utilisation des technologies de l'information dans des activités de renseignement. Vu le contexte actuel de tension dans l'est de l'Europe et des sanctions prises par la Suisse à l'encontre de la Russie, le centre national pour la cybersécurité (NCSC) prédit une augmentation du nombre d'attaques en guise de représailles [6].

Finalement, les sociétés actives dans la manufacture d'équipements pour les infrastructures sensibles (fournisseurs de centrales électriques, installations nucléaires, etc.) seraient particulièrement susceptibles d'en faire les frais car ces sociétés fournissent des composants dans de nombreux pays, ce qui a une grande valeur stratégique pour un pays souhaitant impacter négativement un adversaire lors d'un conflit.

Toutes ces constatations nous permettent d'évaluer les enjeux entourant la problématique de la cybersécurité. Dans les cas que nous avons cités, nous pouvons déjà identifier un certain manque de préparation de la part des autorités communales, qui se retrouvent dépourvues devant des évènements de cybersécurité. En ce qui concerne la commune de Montreux, les services à la population ont été paralysés durant plus d'une semaine avant que les systèmes puissent être rétablis, ce qui pose la question de la préparation de la commune face à ce genre de situation. Dans le cas de la commune de Rolle, on se rend compte du manque de procédures en place et de connaissances pratiques pour gérer une crise de sécurité informatique de manière appropriée.

1.2 Les communes vaudoises

Dans le canton de Vaud, la responsabilité de la gestion des infrastructures informatiques pour la gestion des affaires communales est du ressort des communes elles-mêmes [7]. Partant de cette constatation, nous émettons l'hypothèse que la gestion des questions liées à l'informatique et de la cybersécurité diffère beaucoup entre ces dernières.

Selon les données publiées dans les statistiques officielles, le canton compte 300 communes (1er janvier 2022) dont voici la répartition par nombre d'habitants[1] :

- 161 ont moins de 1'000 habitants.
- 78 ont entre 1'000 et 3'000 habitants.
- 44 ont entre 3'000 et 9'999 habitants.
- 17 ont plus de 10'000 habitants.

Ces données nous donnent une meilleure vision de la situation. Ainsi la grande majorité des communes ont une faible population, 89 % des communes ayant moins de 5000 habitants.

Selon les recherches effectuées, il n'y a pas aujourd'hui de véritables données sur le mode de fonctionnement des communes au niveau de l'informatique et plus précisément de la sécurité. Ce manque de données sur la gestion de l'informatique dans les communes du canton de Vaud représente un problème pour la mise en place d'une politique sur le plan cantonal ou des faitières de communes. Voici les questions que nous allons aborder dans cette étude : Comment les communes gèrent-elles leur informatique, quel est l'état actuel de la cybersécurité et comment envisagent-elles l'avenir.

[1]Source : STATVD, Statistique annuelle de la population

1.3 Problématique

Les communes, comme toute institution privée ou publique, sont confrontées aux problématiques liées à la digitalisation. Le Conseil fédéral a adopté une stratégie concernant la cyberadministration pour les années 2020-2023 [8]. Dans cette dernière, il est mentionné ceci :

> « Par la présente stratégie, la Confédération, les cantons et les communes poursuivent une idée directrice qui se décline comme suit :
>
> a) La Confédération, les cantons et les communes donnent la priorité à l'interaction numérique sur l'offre analogique lorsqu'ils s'adressent à la population et aux entreprises, augmentant ainsi l'accès aux prestations et la transparence de leur action.
>
> b) La Confédération, les cantons et les communes misent sur des prestations administratives entièrement numériques pour accomplir leurs tâches, améliorant ainsi l'efficience et la qualité de l'exécution de leurs prestations.
>
> c) La Confédération, les cantons et les communes veillent à une mise en œuvre inclusive de façon à prévenir le risque d'une fracture numérique. Ils veillent également à limiter l'impact environnemental de la cyberadministration. »

Ainsi, les administrations communales sont de plus en plus dépendantes des outils informatiques dans leurs relations avec le citoyen et dans la réalisation de leurs tâches. Il en découle que les données des citoyens et les services qui leurs sont rendus sont gérés pour la plupart électroniquement. Comme chaque commune est responsable de la gestion de ses propres infrastructures [7], nous faisons l'hypothèse que cela peut créer de grandes inégalités entre ces dernières.

La sécurité informatique devient de plus en plus cruciale. Comme vu plus haut dans l'introduction, une attaque peut entraîner des répercussions importantes sur la qualité du service public. Dans le cas de la commune de Montreux, les services informatiques ont été bloqués pendant près de 8 jours, ce qui a mis à mal le niveau de service à la population. Dans le cas de la commune de Rolle, ce sont les données personnelles des citoyens qui ont été compromises, mettant en danger ces derniers, que ce soit du point de vue de leur vie privée ou de leur sécurité. En effet, la divulgation de ces données personnelles les rend utilisables par des personnes mal intentionnées. Cela peut déboucher sur des usurpations d'identité, elles peuvent être vendues à des sociétés réalisant du spam publicitaire et dans le cas de la commune de Rolle, qui abrite une école internationale prestigieuse, la divulgation de ces données peut potentiellement permettre de localiser des personnalités qui pourraient faire l'objet de menaces si leurs familles sont politiquement exposées dans leur pays d'origine. La mise en place de mesures de cybersécurité est un véritable challenge, car cette dernière nécessite des compétences qui aujourd'hui restent rares et des procédures nouvelles qui ne sont pas encore largement répandues.

Pour un responsable de commune élu par la population, il est aujourd'hui difficile de s'y retrouver. Le système suisse fonctionnant par gouvernance de milice (les citoyens sont élus mais exercent toujours leurs professions), la plupart des communes ne disposent pas des compétences internes leur permettant de gérer cette problématique de manière optimale. De plus, il n'existe pas de solutions clés en main leur permettant de réaliser un audit interne sans faire appel à des sociétés externes.

1.4 Questions de recherche

C'est ce premier échelon que nous voulons essayer de combler dans ce travail de Master. Créer un outil qui sera utile aux responsables politiques locaux, leur permettant d'établir un premier audit de la situation, de se poser les bonnes questions et de faciliter la participation démocratique pour mettre en place une stratégie. Pour cela, il nous faudra des informations préalables que nous préciserons ci-dessous :

Question de recherche 1

- Quels sont les défis rencontrés par les communes vaudoises dans leurs implémentations de mesures de cybersécurité ?
- Est-ce que ces défis sont les mêmes selon la taille de la commune ?

Question de recherche 2

Quelles sont les bonnes pratiques qu'une commune peut suivre pour mettre en place des mesures de sécurité informatique crédibles ?

A l'aide de cette élicitation des besoins et des bases théoriques que nous présentons dans notre revue de la littérature, nous établirons une solution permettant aux responsables politiques de se poser les bonnes questions et en définitive de mettre en place des mesures de protection de qualité, tant du point de vue organisationnel que du point de vue technique.

2 Revue de la littérature

Dans cette revue de la littérature, nous allons aborder deux grandes thématiques. Premièrement, il existe de nombreuses normes et standards qui ont été créés en Suisse et dans le monde pour mettre en place des mesures organisationnelles et techniques permettant une meilleure protection des systèmes d'information. C'est ce que nous allons aborder en premier. Ensuite, une seconde thématique de la littérature concerne les recherches sur des thèmes similaires, à savoir celles qui tentent de comprendre comment les institutions publiques et privées gèrent leurs infrastructures informatiques et mettent en place des mesures de cybersécurité. C'est ce que nous verrons dans la seconde partie. Grâce à cette revue de la littérature, nous serons capables de nous appuyer sur une base théorique pour analyser le fonctionnement actuel des communes vaudoises.

2.1 Cybersécurité

Avant de décrire les normes, standards et labels, il est nécessaire d'expliquer les bases de ce qu'est exactement la cybersécurité. Le Small Business Standard (SBS) en donne une bonne définition [9] :

« La cybersécurité concerne d'abord la protection des informations stockées et leur traitement. Elle se définit comme une solution dans laquelle les risques associés à l'utilisation des technologies de l'information, intégrant l'ensemble des risques et des vulnérabilités, sont réduits à un niveau acceptable au moyen de mesures appropriées. »

La norme ISO 27000:2018 donne également une bonne définition [10] : « Le terme *Sécurité de l'information* est basé sur le fait que l'information et les données d'une entreprise sont considérées comme un actif ayant une valeur. Cet actif requiert une protection appropriée, par exemple contre une perte de disponibilité, confidentialité et intégrité. »

La sécurité informatique se base sur 3 grands principes [11], [12] que l'on appelle la « CIA triad » :

1. *Confidentiality* : la confidentialité fait référence au principe que seules les personnes autorisées doivent avoir accès aux données et informations. Cela sous-entend également que ceux qui n'ont pas l'autorisation sont activement empêchés d'y accéder par des moyens techniques.
2. *integrity* : l'intégrité fait référence au principe selon lequel les données n'ont pas été modifiées par un tiers non-autorisé et qu'elles sont ainsi dignes de confiance.
3. *availability* : la disponibilité fait référence au principe selon lequel les données et les applications doivent être disponibles pour les utilisateurs autorisés dans des délais que l'on peut raisonnablement attendre d'un tel service.

Figure 1 - CIA Triad[2]

Ces principes sont la base sur laquelle reposent tous les modèles de cybersécurité car dans tout type d'incident pouvant mettre en péril les systèmes d'information, l'un de ces principes sera impacté.

Un dernier aspect de la cybersécurité concerne le concept de non-répudiation. Ce concept assure que le système est en mesure de garder une trace de toute transaction permettant de remonter à son origine. Ainsi une personne ne peut pas nier avoir effectuer une transaction de création, modification, visionnage ou de transmission en cas de conflit.[13]

2.2 Normes, standards et labels

2.2.1 En Suisse

Parmi les normes, standards et labels, nous distinguons tout d'abord les normes mises en place par des organismes suisses de celles émises par des organismes étrangers. Il existe une large littérature en Suisse et dans le monde avec de nombreux modèles permettant de mettre en place des systèmes d'information sécurisés.

En Suisse, le Conseil fédéral a adopté un plan stratégique pour les années 2018-2022 pour la gestion de la cybersécurité annonçant la vision suivante : « Tout en utilisant les chances offertes par le numérique, la Suisse est protégée de façon appropriée contre les cyberrisques et est

[2] https://blog.jamestyson.co.uk/tag/cia-triad

résiliente en cas de cyberincidents. La capacité d'agir et l'intégrité de sa population, de l'économie et de l'État face aux cybermenaces sont garanties. » [14].

Pour répondre à ce challenge, le Centre national pour la Cybersécurité (NCSC) a édité plusieurs publications à destination des entreprises et des institutions publiques, leur offrant des recommandations qui permettent de mettre en place des mesures de protection contre les cyberrisques. Parmi ces dernières, on peut citer la norme minimale pour améliorer la résilience informatique (norme minimale sur les TIC 2018) [15] qui se base sur le concept de « Defense-in-Depth » ou « défense en profondeur ». Cette stratégie de protection des systèmes d'information comprend plusieurs éléments qui doivent être mis en place en parallèle afin d'obtenir une sécurité avec un niveau de maturité élevé. Ainsi, le modèle comprend les éléments suivants : la gestion des risques, l'architecture de cybersécurité, la sécurité physique, l'architecture réseau, les périmètres de sécurité réseau, la sécurité de l'hôte, la surveillance de sécurité, la gestion des fournisseurs et les facteurs humains. C'est par cette succession de couches de protection que l'entreprise ou l'administration publique peut se protéger de manière optimale. La mise en place de cette norme se base sur les 5 fonctions du NIST Core Framework que nous abordons plus loin à savoir : identifier, protéger, détecter, réagir et récupérer. En lien avec cette norme, la Confédération a mis en ligne un outil permettant d'effectuer une évaluation au travers d'un tableau Excel[3].

La Confédération a également édité une circulaire sur les prescriptions de sécurité minimale. [16] Cette dernière énonce des mesures de protection à prendre dans l'organisation d'infrastructures informatiques d'unités administratives. Elle se base sur la norme ISO/IEC 27002:2013 que nous verrons également plus tard. Ce document informe sur les réglementations internes de la Confédération et peut servir de base intéressante pour la mise en place de standards pour la cybersécurité des communes. Un document Excel est disponible sur le site de la Confédération pour évaluer la mise en place de ces mesures.[4]

A l'international, de nombreuses normes ont été mises en place. Nous allons mentionner les plus importantes, telles que la norme NIST, la norme ISO 2700x ou encore la norme COBIT.

2.2.2 NIST Cybersecurity Framework

Le NIST Cybersecurity Framework a été publié par le U.S Department of Commerce [17]. Nous allons en expliquer le fonctionnement en détail car il fait partie des normes les plus mentionnées. Ce dernier se base sur 5 fonctions :

- *Identify* : Identifier les processus clés de l'entreprise, les données ayant le plus de valeur ou devant être protégées et les facteurs de risques de cybersécurité les plus importants. Cela permet à l'entreprise concernée de créer une priorisation de ses efforts en fonction de ses besoins.
- *Protect* : Mettre en place des mesures de prévention et de protection pour s'assurer que l'entreprise puisse délivrer ses services clés.

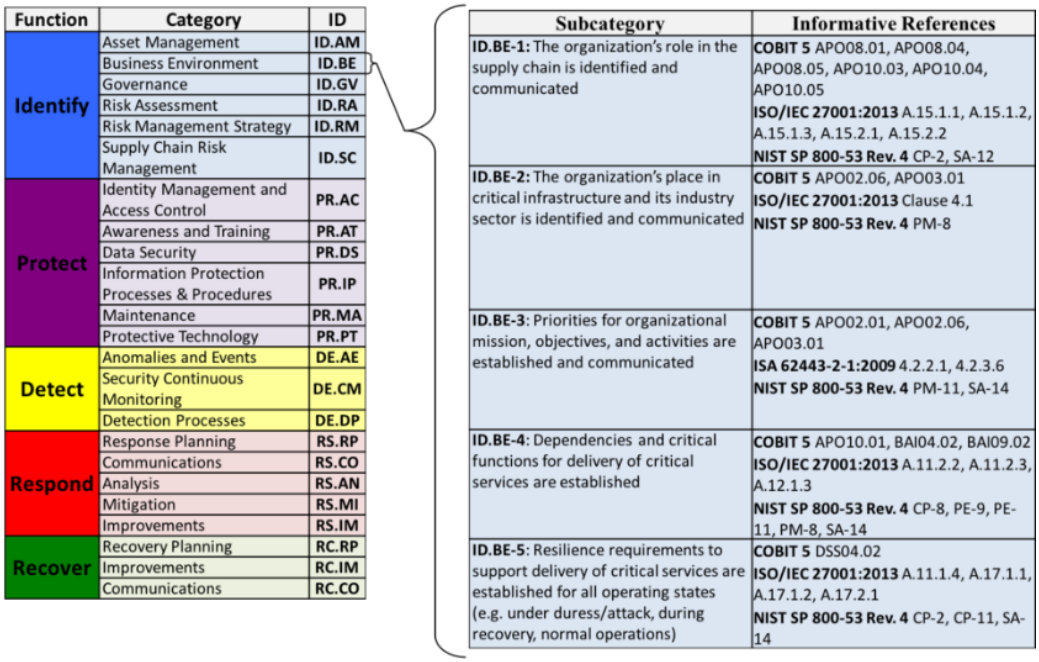
[3] https://www.bwl.admin.ch/dam/bwl/fr/dokumente/themen/ikt/excelblatt_minimalstandard.xlsx.download.xlsx/Norme.minimale.TIC-Outil.d.evaluation-2018-korr.xlsx
[4] https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/dokumentation/vorgaben/sicherheit/si001/Si001-Hi01-IT-Grundschutz_Umsetzung_V5-f.xlsx.download.xlsx/Si001-Hi01-IT-Grundschutz_Umsetzung_V5-f.xlsx

- *Detect* : Développer des outils permettant de détecter le plus rapidement des évènements en lien avec la cybersécurité. Le plus tôt l'entreprise détecte une anomalie, le plus rapidement elle peut la circonscrire et prendre des mesures correctives.
- *Respond* : Développer des procédures standardisées de réponse à un incident de cybersécurité (cellule de crise, communication, partenaires externes, etc.).
- *Recover* : Développer et planifier des procédures pour restaurer le plus rapidement possible les infrastructures informatiques impactées par l'évènement de cybersécurité.

Chacune de ces fonctions se décline en différentes subdivisions appelées catégories. Ces catégories sont elles-mêmes divisées en sous-catégories. Les sous-catégories sont des actions que l'entreprise peut prendre pour améliorer sa cybersécurité. Par exemple, la première sous-catégorie du modèle indique : « Les appareils et systèmes physiques au sein de l'organisation sont inventoriés ». Le manager peut aisément répondre par oui ou par non à cette question et comprend facilement les mesures qui doivent être prises pour que ce critère soit respecté. Le modèle offre pour chaque sous-catégorie des références à de la documentation spécialisée (ISO 27001, COBIT5, etc.) pour mettre ces dernières en place.

L'entreprise est amenée à réaliser une analyse de risques. Elle doit déterminer quels sont les processus et les données qu'elle souhaite protéger en priorité, quelles sont ses obligations légales et elle doit finalement identifier quels types d'attaques ont le plus de risque de survenir afin de s'y préparer au mieux. C'est après avoir réalisé cette analyse de risques que l'entreprise ou l'administration publique peut sélectionner, parmi les 108 sous-catégories, celles qui sont les plus importantes et dans quel domaine de la cybersécurité elle souhaite investir ses moyens financiers.

L'entreprise effectue ensuite une étude de sa situation actuelle sur la base des 5 fonctions, des catégories et des sous-catégories. Cette analyse permet de faire émerger les écarts avec ce qu'elle a établi dans sa liste de priorités et son état actuel. Cette méthodologie permet de communiquer clairement aux prestataires internes ou externes une liste détaillée d'exigences à mettre en place.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 2 - NIST Framework (Source : nist.gov)

2.2.3 ISO/CEI 2700x

Une seconde norme largement répandue dans le monde provient d'un partenariat entre l'Organisme international de normalisation (ISO) et la Commission électronique internationale (CEI). Cette dernière est connue sous le nom de suite ISO/CEI 2700x. Elle comporte une documentation pour la certification d'une entreprise dans le domaine de la sécurité de l'information. La figure 3 ci-dessous en donne un bon aperçu.

La norme qui est la plus souvent citée reste la norme ISO/CEI 27001:2013[18] qui « a été élaborée pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration d'un système de management de la sécurité de l'information (ISMS). » La norme ISO/CEI 27000:2018 définit un ISMS comme suit (traduit de l'anglais) [10] : « un ISMS consiste en des politiques, des procédures, des lignes directrices, et les ressources et activités associées, gérées collectivement par une organisation, dans le but de protéger ses actifs informationnels. Un ISMS est une approche systématique pour établir, mettre en œuvre, exploiter, surveiller, réviser, maintenir et améliorer la sécurité de l'information d'une organisation afin d'atteindre les objectifs commerciaux.» Parmi les points abordés dans cette norme, on trouve notamment :

1. Le contexte de l'organisation
2. Le leadership
3. La planification (gestion des risques)
4. Le support (financement et formation)
5. L'information documentée
6. Le fonctionnement
7. L'évaluation des performances
8. L'amélioration continue

Ce qui est intéressant avec cette norme, c'est qu'elle est à même de définir clairement le périmètre des services qui feront l'objet d'une protection particulière. Cela permet à l'entreprise de créer une liste de priorités et d'investir ses ressources là où cela fait le plus de sens. La norme ISO/CEI 27001 compte une annexe qui comporte une liste de mesures organisationnelles pouvant être mises en place par l'entreprise. Cette liste de mesures est détaillée pour une mise en œuvre facilitée dans la norme ISO/CEI 27002:2013 [19]. Simultanément à l'écriture de ce rapport, une nouvelle version des normes ISO/CEI 27001 et 27002 a été publiée. Les thématiques citées plus haut restent les mêmes, seule la liste de mesures organisationnelles de l'annexe A a été modifiée.

Finalement, la norme ISO/CEI 27005:2018 [20] propose une méthode pour faire une évaluation des risques liés à la sécurité de l'information.

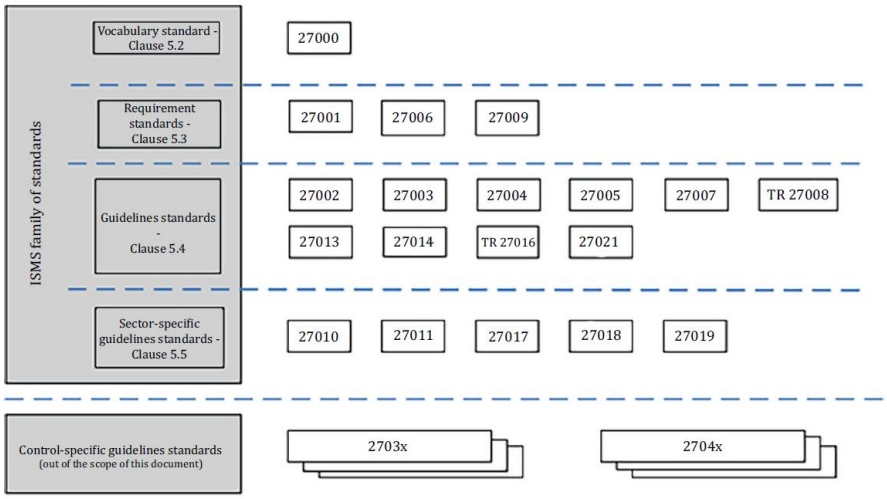


Figure 3 Architecture ISO 2700x [10]

2.3 Etudes similaires

Au niveau de la recherche scientifique relative à la maturité des institutions face à la problématique de la cybersécurité, nous pouvons mentionner deux grandes catégories. Premièrement, il existe un certain nombre d'études spécifiquement dirigées vers le mode de fonctionnement des institutions étatiques locales. Il existe également un grand nombre d'études concernant les entreprises plus largement. Bien que le statut juridique de ces entités soit différent, les difficultés rencontrées par les communes ou les entreprises privées sont sensiblement les mêmes.

2.3.1 Gouvernements locaux étrangers

Dans la littérature scientifique concernant la sécurité informatique des communes, on peut citer le travail du Dr. Donald F. Norris de l'université du Maryland qui a publié une série d'articles sur la thématique de la gestion de la cybersécurité dans le cadre des gouvernements locaux aux Etats-Unis. Dans un article publié en 2021 [21], il révèle les résultats d'une enquête effectuée en 2020 auprès de 14 responsables de la cybersécurité de 14 villes américaines. Dans sa publication, il identifie 4 raisons principales expliquant pourquoi les gouvernements sont une cible privilégiée des attaques informatiques :

1. Le grand nombre d'agences gouvernementales.
2. Les données personnelles identifiables qu'elles ont sur leurs serveurs ont de la valeur. Parmi ces dernières, les coordonnées des citoyens et leurs données financières/fiscales.
3. Les outils de piratages sont facilement utilisables et ne nécessitent plus de compétences spécifiques avancées. Le nombre de cybercriminels augmente.
4. Les gouvernements locaux ont des limites budgétaires.

Le manque de financement reste le facteur le plus important contribuant aux difficultés rencontrées par les gouvernements locaux américains dans la mise en place de mesures de cybersécurité solides. Ainsi dans le questionnaire de 2016 [22], trois barrières ont été identifiées :

1. Le manque de moyens pour engager des employés spécialisés en cybersécurité à des salaires attractifs.
2. Le manque de personnel spécialisé.
3. Le manque de financement.

Selon l'étude de 2020 [21], il a été démontré que 57,1% des gouvernements locaux interrogés consacraient un pourcentage moins élevé de leur budget informatique dans la cybersécurité que la moyenne des entreprises privées américaines (5-8%).

Différents types d'attaquants ont pu être identifiés par les gouvernements locaux dans les questionnaires de 2016 et de 2020 [21], [22]. Parmi ces derniers, on trouve par ordre d'importance :

1. Les organisations externes (groupes criminels)
2. Les hacktivistes/spammeurs
3. Les nations
4. Des individus externes

Parmi les objectifs identifiés de ces attaques, on trouve le plus souvent :

1. Les rançons
2. Le vol d'argent
3. Le vol de données personnelles
4. Le vol de données confidentielles
5. Hacktivisme

L'étude de 2016 mentionne également un grand nombre d'attaques dont le but est de provoquer des dégâts sans que l'objectif exact puisse être identifié.

Plus de 50% des gouvernements locaux ont rapporté avoir une ou plusieurs générations de retard en ce qui concerne les pratiques et politiques internes en matière de cybersécurité. Au niveau de la technologie, c'est 44% des répondants qui estiment être en retard [23]. Le rapport conclut que de manière générale les gouvernements locaux pratiquent mal la cybersécurité. Les raisons principales identifiée sont :

1. Le manque de sensibilisation des élus locaux.
2. Le manque de support de la part des élus locaux pour des projets liés à la cybersécurité.
3. La délégation de la responsabilité de la gestion de la cybersécurité à des techniciens.

Ainsi, sans support de la part du management et des responsables, une politique solide de cybersécurité ne peut être atteinte. La sensibilisation des élus a un impact direct sur leur volonté de consacrer du budget public et du support à la mise en place de mesures techniques et organisationnelles pour augmenter le niveau de maturité. Les élus doivent prendre le leadership sur les questions liées à la cybersécurité et ne plus déléguer cette thématique au personnel technique dans l'organisation.

Ces études du professeur Donald F. Norris nous permettent d'identifier un certain nombre de facteurs qui peuvent influencer notre étude des communes du Canton de Vaud. Il est probable que nos communes sont confrontées à des problématiques similaires et que ces études puissent nous éclairer sur notre problématique.

La littérature identifie également quels sont les incidents [24] en lien avec la cybersécurité qui affectent en majorité les gouvernements locaux. Ce sont, par ordre d'importance :

1. Violation des données (vol malicieux ou perte/vol de matériel).
2. Divulgation involontaire des données.
3. Perturbations (service non accessible ou détourné).
    a. Détournement ou blocage des infrastructures publiques.
    b. Attaques DDOS.
    c. Ransomware.
4. Violation de la vie privée (projet du gouvernement local ne respectant pas la législation).
5. Fraude et extorsion.
6. Erreur IT (bug).

Dans un rapport publié en 2021[25], l'ENISA estime que les principales tendances en termes de cybersécurité sont les suivantes :

- Les rançongiciels sont considérés comme la première menace.
- Les attaques de malware sont en déclin (à l'exception des ransomware).
- Fort développement du cryptojacking. Ce type d'attaque se définit comme l'utilisation non autorisée des infrastructures par un tiers dans l'objectif de miner des cryptomonnaies.
- Le développement de mails de phishing de plus en plus sophistiqués.

2.3.2 Communes suisses

Publié en 2021, un sondage de 2017 s'est intéressé à la situation des communes suisses [26]. Sur les 2255 communes recensées dans le pays, 1868 y ont participé, ce qui rend cette étude particulièrement représentative. Les auteurs de ce travail ont consenti à nous transmettre les données de l'étude, ce qui nous permet de réaliser une analyse pour les communes vaudoises. Dans ce questionnaire, toutes les communes participantes n'ont pas répondu à toutes les questions, les pourcentages sont relatifs au nombre de communes ayant répondu.

Selon le sondage (n=1795), 44,68% des communes offrent depuis plus de 5 ans des prestations pouvant être commandées sur leur site internet, 24,57 % depuis moins de 5 ans et 29,91% disent ne pas offrir ce genre de service à la population. Cela signifie qu'en Suisse, la majorité des communes contactées (69,25%) offre une forme de service digitalisé à la population.

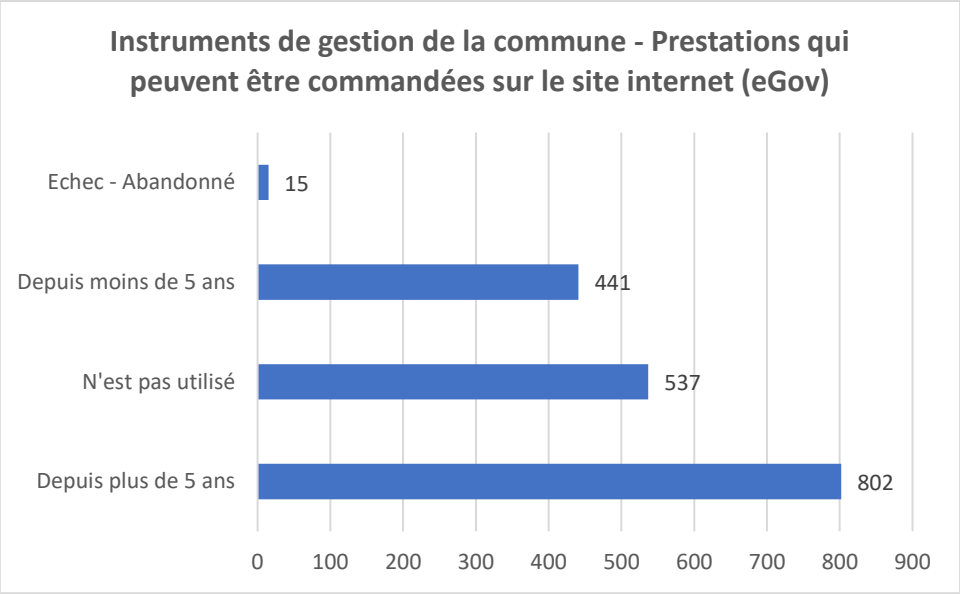


Figure 4 EGov - Utilisation en Suisse

Toutefois, à la question de savoir l'importance que ces dernières apportent à la stratégie fédérale de cyberadministration (n=1736), la majorité (58,21%) répondent qu'il s'agit d'un thème représentant peu/aucune importance. Seuls 31% des communes estiment cette thématique comme plutôt/importante. On peut ainsi établir que même si la majorité des communes offre des services en ligne à la population, cette thématique ne représente pas une priorité stratégique pour ces dernières.

L'une des données intéressantes ressortant de cette étude est que dans la gestion de leurs tâches, 18,2% des communes suisses s'estiment en manque de capacité pour gérer de manière optimale les questions liées à l'informatique. En Suisse romande plus spécifiquement, ce chiffre est légèrement plus bas avec 16,7 % des communes rencontrant des difficultés. Parmi les communes qui s'estiment le plus en difficulté, on retrouve les communes entre 2'000 et 4'999 habitants (21,4%), les communes entre 5'000 et 9'999 habitants (20,8%) et les communes entre 20'000 et 49'999 habitants (20%).

Parmi les communes interrogées (n=1764), 39,2% indiquent gérer leurs infrastructures informatiques en interne, 27,6% affirment travailler avec un prestataire privé externe et 32,36% en collaboration avec d'autres communes. L'informatique est d'ailleurs la tâche communale la plus externalisée auprès de partenaires privés. Au niveau de la taille des communes, l'étude remarque une différence significative dans la gestion de l'informatique selon la taille avec les communes de moins de 20'000 habitants gérant leur informatique en interne dans 40% des cas alors que les grandes communes disent gérer en interne dans 70,3% des cas.

Que les communes gèrent leur informatique en interne ou en externe, elles font beaucoup appel à des prestations de conseils auprès de partenaires externes. Selon l'étude, ce sont 61,8% des communes interrogées qui font appel à des prestataires externes pour du conseil en services informatiques, et 49,8% pour être conseillées dans l'achat de matériel.

Parmi les communes ayant répondu au questionnaire, 237 sont vaudoises. Ces données sont issues du dataset public lié à l'étude précitée [27]

- Les prestations de E-Gouvernement sont relativement peu utilisés : seuls 23,55% des communes disent offrir des prestations pouvant être commandées sur le site internet

(n=225). Ce chiffre est largement en dessous de ce qui se fait sur le plan national avec 69,25% des communes offrant ce genre de prestations.

- Elles sont 23,15% à déclarer porter de l'importance à la stratégie suisse de cyberadministration (n=216).
- 11,79% de ces communes estiment avoir atteint, voire avoir dépassé leurs capacités dans la gestion des questions liées à l'informatique (n=237). C'est légèrement en dessous de la moyenne suisse.
- 40% des communes vaudoises disent gérer en interne leurs infrastructures informatiques, 31,63% font appel à un prestataire externe et 26,04% ont des partenariats intercommunaux (n=215).
- La plupart d'entre elles (73,37% n=154) font appel à des prestataires externes de conseil informatique pour les services informatiques et 54,24% (n=153) pour des services de conseil d'achat.

Cette étude ayant été réalisée en 2017, ces données sont relativement anciennes. Il est fort probable que, à la suite des problématiques en lien avec la cybersécurité qui ont été révélées par les attaques des communes de Rolle et Montreux, les réponses au questionnaire seraient différentes s'il était répété en 2022. Ces données sont donc intéressantes en ce qui concerne la perception de la problématique en 2017, mais ne reflètent pas de manière précise la réalité de 2022.

Finalement, une étude réalisée en 2022 [28] indique que la population suisse a une perception négative de la protection des données et de la cybersécurité, indiquant à 44% n'avoir aucune confiance dans la protection des données et dans la sécurité des données.

2.3.3 Entreprises et PME

Une étude publiée en 2021 [29], [30] a interrogé 506 directeurs et directrices de PME suisses (4 à 49 collaborateurs) sur des thématiques comme la numérisation, le télétravail et la cybersécurité dans le contexte de la crise sanitaire de 2020. Ci-dessous les principales découvertes :

- 61 % des PME considèrent la modernisation de leurs infrastructures informatiques comme importante ou très importante. Ce sont notamment les sociétés actives dans le domaine des services et de la santé qui rapportent le plus ce besoin.
- 51% des répondants s'estiment bien ou très bien informés des cyberrisques.
- 30% des activités informatiques des PME sont effectuées par des prestataires externes.
- 36% des PME ont fait l'objet d'une attaque informatique.
- 66% des PME considèrent la cybersécurité comme importante ou très importante. Plus l'entreprise est grande, plus cette thématique est importante.
- Seules 15% des PME estiment qu'il y a un risque élevé ou très élevé qu'elles fassent l'objet d'une attaque paralysant leur activité pendant au moins 1 jour.
- 30 % des entreprises ont un budget dédié à la sécurité informatique.

- 40% estiment qu'il est probable qu'elles adoptent de nouvelles mesures de cybersécurité au cours des 3 prochaines années.
- 30% des PME ne forment pas ou peu leurs collaborateurs aux thématiques de cybersécurité.

Pour mettre ces résultats en perspective, une étude réalisée en 2021 par l'IFOP en France estime que bien que les patrons de PME soient conscients des problématiques liées à la cybersécurité, ils surestiment souvent leur niveau de protection face à cette menace et leur capacité à faire face à ce genre de situation. Ainsi, alors que 80% estiment être bien protégés, 25 % ont déjà subi une cyberattaque.[31]

2.4 Conclusion

De cette étude de la littérature nous pouvons retenir plusieurs éléments. Premièrement, il existe un nombre important de normes et standards reconnus internationalement offrant des recommandations et permettant de mettre en place des mesures et des stratégies en termes de cybersécurité. Nous pouvons également établir que pour les administrations publiques, le frein principal à la mise en place de mesures de cybersécurité reste le manque de ressources financières. En lien avec ce manque de ressources, vient ensuite la difficulté à recruter du personnel qualifié à des salaires suffisamment attractifs.

Ce que l'étude des PME démontre, c'est que de manière générale, les dirigeant se sentent sensibilisés aux risques liés à la cybersécurité, qu'ils considèrent la question comme importante mais estiment encore qu'ils ne seront pas impactés de manière significative, que ce soit sur le plan financier ou réputationnel en cas d'attaque. Il existe ainsi une surestimation de la capacité de leur entreprise à se protéger face à une attaque et à son impact.

Les administrations publiques détiennent sur leurs systèmes des données potentiellement sensibles (données fiscales, données personnelles sensibles) qui ont beaucoup de valeur pour un attaquant potentiel. La professionnalisation des groupes criminels, le développement du hacktivisme, la simplification des outils d'attaque et les tensions géopolitiques sont autant de facteurs qui augmentent le niveau de risque. Il est également important de noter qu'un risque non négligeable concerne les utilisateurs internes à l'entreprise ou l'institution publique qui peuvent de manière volontaire ou non causer de sérieux problèmes en matière de sécurité informatique.

3 Méthodologie

3.1 Population et échantillon

La population de cette étude comprend les communes du canton de Vaud. En 2022, elles sont au nombre de 300.

Pour l'échantillon de l'étude quantitative, un questionnaire est envoyé à tous les représentants des communes par email grâce à la liste de contacts fournie par l'Union des Communes Vaudoises.

Pour l'étude qualitative, les communes participantes sont sélectionnées selon une méthode d'échantillonnage stratifié. Différentes tailles de communes (grande, moyenne, petite, micro) de différentes régions du canton sont représentées dans l'étude.

3.2 Analyse quantitative et collection des données

Afin de réaliser l'analyse quantitative, un questionnaire comportant 41 questions a été réalisé en collaboration avec l'Union des Communes Vaudoises et le label Cybersafe. (Annexe 1)

À la suite de diverses itérations, ce dernier a été validé. Il se décline en 5 sections :

1. Identification de la commune : cette section n'est pas obligatoire. Nous avons décidé de laisser la possibilité aux communes de répondre anonymement. Cette décision est due à la sensibilité des données récoltées.
2. Démographie : l'objectif de cette section est de placer chaque commune dans son contexte. Nous souhaitons connaître le nombre d'habitants, le district et le nombre d'employés (exprimé en équivalents Temps Plein/ETP) travaillant dans la commune. Ces données nous permettent de déterminer s'il existe des différences significatives entre les différentes tailles de communes et la région dans laquelle elles se situent.
3. Organisation : cette section s'intéresse à l'organisation interne des communes. Sont abordés notamment les notions budgétaires, l'importance stratégique donnée à la digitalisation, les ressources humaines et le stockage des données.
4. Procédures et pratiques : cette section essaie de mettre en lumière les mesures et procédures qui sont mises en place dans la commune. Cela comprend par exemple la gestion des risques, la gestion de la relation avec les prestataires externes, la formation des collaborateurs et les procédures en place.
5. Attentes et remarques : dans cette section, nous laissons la liberté aux répondants d'inscrire quelles sont leurs attentes et leurs projets dans les mois à venir.

Lors du premier entretien avec l'Union des Communes Vaudoises, les responsables ont estimé un taux de réponse réaliste de 5%. Après la première campagne de mailing du 28.04.2021, 72 communes ont répondu au questionnaire. Cela représente 24% des communes.

A cause de la sensibilité des données récoltées, nous avons pris la décision de proposer deux solutions aux communes. Premièrement, nous avons établi un formulaire de réponse via Microsoft Forms. Les données sont stockées sur un serveur en Suisse et sont protégées par un mot de passe fort et une double authentification. Nous avons joint à l'email le questionnaire au format PDF. Ce

dernier peut être imprimé et retourné manuellement pour les communes qui ne souhaitent pas remplir un formulaire en ligne.

La décision a été prise que les données récoltées lors de cette étude resteront confidentielles et ne seront divulguées à personne. L'étude, elle, sera publiée publiquement.

Les données récoltées sont analysées à l'aide d'outils de visualisation de données (P.E : le logiciel Tableau ou encore Excel). L'objectif de ces dernières, comme expliqué plus haut, est d'établir un état de la situation, comprendre quelles sont les pratiques en cours dans les communes et déterminer quelles mesures font le plus de sens dans le cadre d'une mise en place d'une stratégie de renforcement de la cybersécurité.

3.3 Analyse qualitative et collection des données

Dans le cadre de cette étude, nous menons des entretiens semi-directifs avec des responsables communaux, afin d'approfondir les résultats obtenus lors de l'analyse quantitative. Les entretiens sont enregistrés à l'aide d'un dictaphone, ce qui permet la création de retranscriptions. Des entretiens sont également réalisés avec les responsables au niveau cantonal et à celui des associations de communes. Idéalement, il serait bien de rencontrer les représentants d'une commune de chaque taille (grande, moyenne, petite, micro).

3.4 Procédure, méthodologie et Research Design

Ce travail de Master est une étude transversale s'intéressant à l'état actuel de la gestion de l'informatique et de la cybersécurité des communes vaudoises. Elle a pour objectif de dresser un tableau de la situation actuelle et d'apporter des pistes afin de remédier aux manquements identifiés. Pour ce faire, une revue de la littérature est d'abord réalisée. Une étude des bonnes pratiques et des normes en cybersécurité est effectuée et des études de cas sur la situation à l'étranger sont mentionnées. Si le temps le permet, des experts du domaine sont interviewés pour confronter ce que nous dit la littérature à leur expérience du terrain. Un questionnaire est envoyé aux responsables politiques pour comprendre quel est leur ressenti vis-à-vis de la problématique de la cybersécurité, et des entretiens sont menés pour comprendre en détail le fonctionnement actuel des communes et l'étendue de leurs besoins.

3.5 Validité des données

Afin de s'assurer que les données récoltées sont valides, il est nécessaire de s'adresser aux mêmes acteurs dans la mesure du possible dans les différentes communes interrogées. Ainsi, pour le questionnaire, il faut absolument que ce soit le syndic ou un membre de la municipalité qui réponde au questionnaire. Pour l'interview, il doit s'agir de la personne en charge de l'infrastructure informatique. Cela est nécessaire car tous les acteurs n'ont pas la même vision et un fonctionnaire spécialisé ou un responsable informatique peut avoir un biais que n'aura pas un politicien.

4 Analyse

Afin de comprendre le mode de fonctionnement des communes vaudoises, nous avons envoyé un questionnaire par email aux communes. 72 communes sur 300 ont répondu (24%). Le questionnaire est disponible dans l'annexe 1.

4.1 Finances publiques

En premier lieu de cette analyse, revoyons les données précédemment citées dans l'introduction. Une grande majorité des communes du canton de Vaud ont moins de 5000 habitants (89% ou 267 communes sur 300) et plus de la moitié de ces dernières comptent moins de 1'000 habitants (53,66% ou 161 communes sur 300). Cette composition des communes vaudoises permet de déduire une grande disparité dans les besoins en infrastructures informatiques, entre les grandes villes et agglomérations et les communes plus éloignées des centres urbains.

Ces différences se répercutent logiquement sur les capacités financières des communes du canton. Selon les données disponibles sur le site du canton[5], en 2019, 50% des communes (sans Lausanne) avaient un revenu compris entre 2'067'887 (Q1) et 14'976'073 (Q3) de francs suisses avec des revenus médians de 4'908'973 de francs suisses. Nous avons fait le choix de sélectionner les données de 2019, car elles sont plus représentatives d'une situation normale, en dehors de la situation exceptionnelle que nous avons vécue durant la pandémie. Il est également intéressant de remarquer que dix grandes communes du canton perçoivent 50,62 % des revenus des communes cumulés.

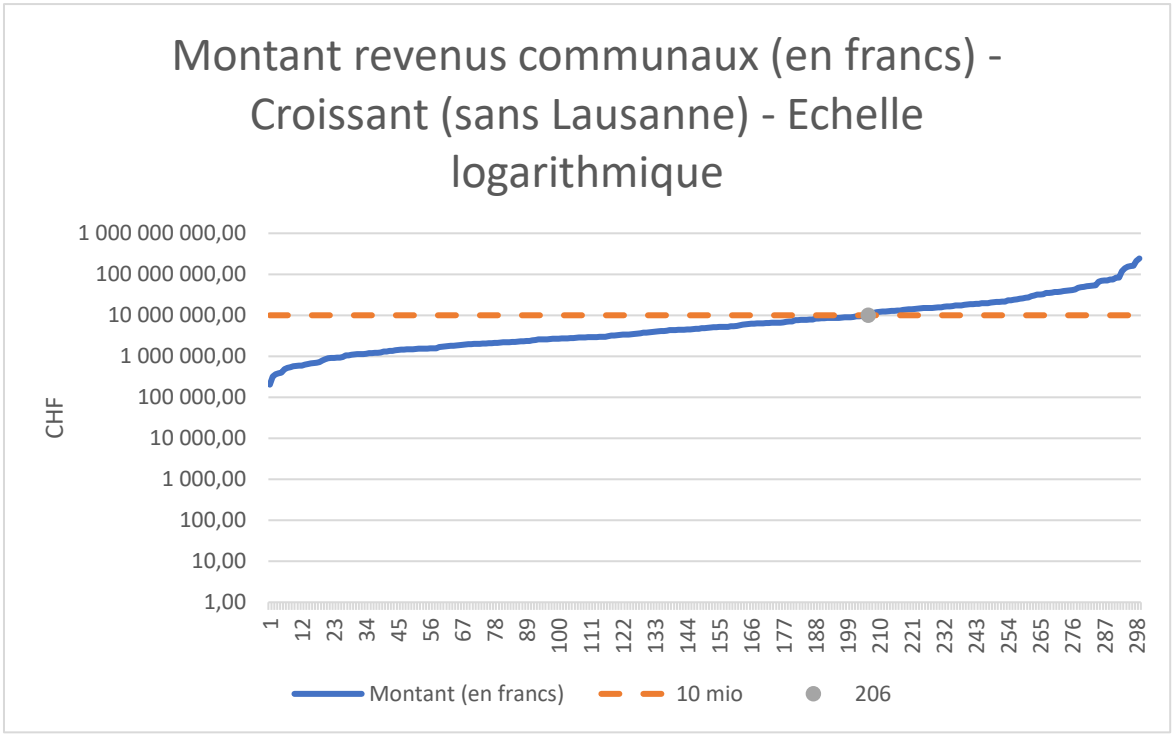


Figure 5 Montants revenus communaux (en francs) - Croissant (sans Lausanne) - Echelle logarithmique

[5] https://www.vd.ch/themes/etat-droit-finances/communes/finances-communales/ (consulté le 10.06.2022)

La figure 5 est tout à fait intéressante. Elle montre que près de deux tiers des communes du canton de Vaud disposent de revenus inférieurs à 10'000'000 de francs suisses pour couvrir leurs charges d'exploitation. Ce graphique ne comprend pas la ville de Lausanne, car ses revenus de 1,775 milliard de francs suisses (7x supérieurs à la seconde plus grande commune) entachent la lisibilité du graphique.

La population reste fortement demandeuse de services disponibles en ligne [28], ce qui peut être problématique dans le cas d'une petite commune ne disposant pas de moyens suffisants pour assurer la mise en place de ce type de prestations.

Dans notre revue de la littérature, parmi les facteurs importants identifiés aux Etats-Unis dans les freins à la mise en place de mesures de cybersécurité, le manque de ressources financières reste le plus important. La situation du canton de Vaud est comparable. Le canton compte un nombre important de communes, chacune responsable de la gestion de sa propre infrastructure informatique avec dans la plupart des cas des moyens limités.

Dans notre questionnaire, à la question 4.a « Est-ce que votre commune a un budget spécifiquement dédié à l'informatique ? » 73,61% ont répondu oui. Comme le montre la figure 6, ce sont principalement les petites communes de moins de 1000 habitants qui n'ont pas de budget dédié. Alors que plus de la moitié des communes vaudoises ont moins de 1000 habitants, ce résultat laisse penser que de nombreuses communes ne disposent pas de budget dédié. Cette absence de budget dédié à l'informatique a plusieurs significations : premièrement, cela signifie que la commune ne considère pas l'informatique et la numérisation des services communaux comme nécessitant une planification spécifique devant être budgétisée.

	Taille				
Budget IT	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	16	3			
Oui	23	13	12	4	1

Figure 6 - Budgets IT par taille de commune

Un bon exemple qui peut illustrer ce manque de moyens financiers pour la gestion de l'informatique est l'équipement informatique mis à disposition des élus. Ainsi, parmi les communes ayant indiqué avoir un budget spécifiquement dédié à l'informatique, seul un tiers fournit aux élus un ordinateur dédié pour l'exécution des tâches administratives (question 5.a). Comme le démontre la figure 7, plus une commune est petite, plus la proportion de mise à disposition d'ordinateurs professionnels est faible. Lors d'un entretien avec un responsable informatique d'une petite commune, la question budgétaire a été la raison principale pour expliquer cette situation. Les élus travaillent ainsi avec leurs propres machines pour accéder à leurs comptes email ou aux données des communes, ce qui peut avoir un impact sur la capacité du responsable informatique d'opérer des contrôles sur la manière dont sont utilisés ces machines et le niveau de sécurité de ces dernières (par exemple si le municipal utilise un gestionnaire de mots de passe, s'il effectue régulièrement des mises à jour ou s'il utilise un logiciel anti-virus).

	Taille				
Ordinateurs professionnels fournis aux municipaux	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	20	6	7	1	1
Oui	3	7	5	2	
Parfois				1	

Figure 7 - Ordinateurs professionnels pour municipaux

A la question de connaitre l'évolution de leur budget informatique au cours des 5 dernières années (question 4.c), la majorité des communes (71,70%) disposant d'un budget spécifique à l'informatique rapporte une faible (1-30%) ou grande augmentation (30% ou plus) de leurs dépenses dans ce département. Une seule commune répondante rapporte une grande diminution. Nous pouvons faire l'hypothèse qu'il s'agit d'une erreur de saisie de la part de la commune, qui indique plus loin dans le questionnaire un haut niveau de priorité pour la digitalisation des services communaux. Ces réponses semblent logiques, dans la mesure où la population a de plus en plus de demandes vis-à-vis de services digitalisés et où les communes, comme toute entreprise, dépendent des outils numériques dans la réalisation de leurs activités. La figure 8 montre les résultats de notre étude vis-à-vis de cette problématique. Ce sont à nouveaux les communes de moins de 1000 habitants qui ont la plus grande proportion de budget n'ayant pas augmenté.

	Taille				
Evolution du Budget IT 5 dernières années	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Grande augmentation (+30% ou plus)	4	2	5		
Petite augmentation (+1 % à + 30%)	9	8	5	4	1
Resté pareil	9	3	2		
Grande diminution (-30 % ou plus)	1				

Figure 8 - Evolution budget IT au cours des 5 dernières années

A la question de connaître l'évolution du budget pour la sécurité informatique (question 4.c), une majorité des communes interrogées (69,81%) rapporte une augmentation de leur budget. Comme pour la question précédente, une commune a rapporté une grande diminution. Ce qui est intéressant de remarquer, c'est la proportion de grande augmentation (14 sur 53). Cette proportion plus importante montre que si les budgets dédiés à l'informatique ont majoritairement évolué à la hausse, les budgets dédiés à la cybersécurité ont généralement plus augmenté. Cette augmentation plus importante est certainement à mettre sur le compte des attaques de plus en plus fréquentes que subissent les administrations publiques et les entreprises. Ces dernières ont fait prendre conscience à la population et aux décideurs de l'importance à donner à la protection des données. De plus, les législations sur la protection des données qu'elles soient européenne,

suisse ou vaudoise, mettent de plus en plus de pression pour la mise en place de mesures crédibles de cybersécurité.

	Taille				
Evolution du Budget Cybersécurité 5 dernières années	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Grande augmentation (+30% ou plus)	5		7	2	
Petite augmentation (+1 % à + 30%)	5	11	4	2	1
Resté pareil	12	2	1		
Grande diminution (-30 % ou plus)	1				

Figure 9 - Evolution budget sécurité

Nous avons également demandé aux communes d'estimer le pourcentage de leur budget qui est investi dans des mesures en lien avec la cybersécurité (question 4.b). Sur les 53 communes ayant un budget informatique, 42 ont répondu. Les autres communes ont indiqué soit ne pas savoir exactement le pourcentage, soit que les mesures en lien avec la sécurité informatique ne sont pas dissociées du budget.

Pour les communes qui ont répondu, voici les points à retenir :

- 13 communes (30%) indiquent investir 0 à 2% de leur budget informatique dans la cybersécurité.
- 6 communes (14,28%) indiquent investir entre 5 et 10%.
- 17 communes (40,47%) indiquent investir entre 10 et 20% du budget.
- 5 communes investissent de 20 à 50% de leur budget dans la cybersécurité (Max = 50%).

Finalement, nous nous sommes intéressés à la question des assurances pour la cybersécurité (question 13.a). De plus en plus de compagnies d'assurances proposent ce type de service. Dans un article publié en 2020 [32] , Jacques de Werra et Yaniv Benhamou décrivent trois principaux risques couverts par les assurances en Suisse. Premièrement, les dommages subis par le preneur d'assurance (p.e. : couverture des coûts liés à la non-disponibilité des données ou des systèmes d'information), les dommages causés par le preneur d'assurance (p.e : une fuite de données impacte les clients négativement. L'entreprise est couverte vis-à-vis des répercutions légales et des dédommagements) et dans certains cas une assistance en cas d'incident.

	Taille				
Assurance	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	33	13	10	2	1
Oui	6	3	2	2	

Figure 10 - Assurance

Selon notre étude, seule une minorité de communes (18.05%) a souscrit une telle assurance. Selon un sondage publié par l'institut GFS-Zurich en 2022 [33], la proportion des PME suisses ayant souscrit une cyber assurance est de 30%. La région lémanique n'arrive pas à ce niveau avec seulement 18% de ses entreprises ayant contracté ce genre d'assurance. Les données que nous trouvons sont ainsi en adéquation avec le marché de la cyber assurance dans la région. Il serait intéressant de comprendre la raison expliquant ce manque de couverture, et l'effet que cela a sur la résilience des entreprises de la région. La prise d'une assurance cybersécurité est également un signe que la commune ou l'entreprise a déjà étudié en profondeur la question car, dans la plupart des cas, les compagnies d'assurances, comme c'est le cas par exemple de la Bâloise[6], demandent dans les obligations contractuelles de la police la mise en place de mesures de cybersécurité crédibles.

Nous plaçons la souscription d'une assurance dans la partie financière, car nous souhaitons savoir si la commune s'est activement couverte contre les risques. Les communes ayant souscrit ce type d'assurance affirment à l'unanimité être couvertes contre les attaques de type ransomware (question 13.b).

En conclusion, comme vu précédemment dans la littérature, les difficultés budgétaires représentent un frein à la mise en place d'une stratégie crédible de cybersécurité. Les communes du canton de Vaud disposent de relativement petits budgets. Ce manque de moyens implique que des choix doivent être faits et que, pour certaines communes, l'informatique, la digitalisation et la cybersécurité ne sont pas des investissements prioritaires. Certaines petites communes n'ont pas de budget dédié à l'informatique. Ce manque de moyens se reflète dans le pourcentage de communes mettant à disposition des ordinateurs à leurs municipaux (32,69%). Toutefois, la problématique est reconnue. Durant les 5 dernières années, les budgets informatiques et de cybersécurité ont augmenté.

4.2 Leadership

La première information que nous avons essayé de récolter est de savoir si la commune a une personne désignée au sein de l'administration communale pour les questions en lien avec l'informatique (question 7.a). En effet, lors de nos discussions préparatoires avec l'Union des Communes Vaudoises (UCV), l'hypothèse a été émise que de nombreuses communes n'en disposent pas. Dans la base de données fournie par l'UCV, 159 communes sur 300 ont un responsable informatique répertorié. Cela signifie que 53% en disposent et que 47% n'en disposent pas. L'objectif est de confirmer cette proportion et de comprendre les différences selon la taille de communes. Nous souhaitons par la même occasion savoir qui au sein de

[6] https://www.baloise.ch/dam/baloise-ch/unternehmenskunden/documents/fr/vertragsbedingungen/140_1021_f.pdf (Consulté le 27.06.2022)

l'administration communale est responsable de cette tâche. Cette question est importante dans la mesure où la commune doit être capable de désigner qui est responsable au sein de l'administration communale de la question de la numérisation et de l'informatique, et cela signifie que cette thématique est considérée comme ayant une importance suffisamment importante pour être inscrite dans les fonctions d'un employé communal ou d'un élu. Cette question provient de l'étude du professeur Norris [23] qui a remarqué que les questions de cybersécurité sont souvent perçues comme étant de la responsabilité des professionnels techniques (informaticien de l'administration publique) et restent plus rarement traitées au niveau de la direction (au niveau des élus). Les normes ISO 2700x et NIST citées dans la revue de la littérature s'intéressent également à la question.

	Taille				
Responsable informatique	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	15	6	2		
Oui	24	10	10	4	1

Figure 11 - Responsable informatique

Selon nos résultats, 68.06% des communes disposent d'un responsable informatique. C'est ainsi proportionnellement supérieur aux données transmises par l'UCV. Il existe plusieurs hypothèses pour expliquer cette différence. Premièrement, dans la campagne de mailing, les responsables informatiques ont été contactés sur leur adresse email directe alors que dans le cas des communes répertoriées comme n'ayant pas de responsable informatique, c'est l'adresse générale de la commune qui a été utilisée. Nous pouvons également faire l'hypothèse que les communes disposant d'un responsable informatique ont un intérêt plus prononcé dans cette thématique et sont ainsi davantage prêtes à prendre le temps de répondre au questionnaire. Ce que nous montre notre questionnaire, c'est que ce sont les communes de moins de 2000 habitants qui ont la plus petite proportion de responsables informatiques avec 61% d'entre elles disposant de ce poste au sein de leur administration.

La figure 12 ci-dessous nous donne un bon aperçu du rôle de la personne responsable dans l'administration communale (questions 7.b et 7.c). Ainsi, dans la majorité des communes (69%), la personne responsable est un membre de la municipalité. Pour expliquer cette proportion importante, nous pouvons nous référer aux hypothèses explicitées plus haut, soit la nature de notre campagne d'emailing. Dans la partie de texte libre offerte aux répondants, certains expliquent travailler en partenariat avec des prestataires externes qui les conseillent dans leurs tâches pour la gestion de l'informatique. Ce type de réponse est attendu dans la mesure où dans la littérature, nous avons constaté que de nombreuses communes font appel à des prestataires externes pour les conseiller. Une commune explique également avoir deux personnes travaillant conjointement dans la gestion de cette tâche (membre de la municipalité et secrétaire communal). Ces données sont intéressantes car cela signifie que les questions liées à l'informatiques sont traitées au niveau de l'échelon de la direction de la commune et est considéré comme un enjeu d'importance stratégique.

Role	Taille				
	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Boursier	1	1	2	3	
Cadre spécialisé répondant à la municipalité	2		1		1
Membre de la municipalité	20	8	6		
Secrétaire communal	1	1	1	1	

Figure 12 - Position du responsable informatique dans l'organisation

Nous avons ensuite souhaité savoir si la commune avait parmi ses employés une personne disposant de compétences en informatique (question 8.a). Par compétences en informatique, nous entendons une personne ayant effectué des études supérieures en informatique ou ayant obtenu un CFC d'informaticien. Cette question a pour but de savoir si les communes ont investi dans l'engagement d'une personne spécialisée dans le domaine. Il est important de préciser qu'il est possible que, dans les communes ayant répondu positivement, il y ait, parmi les élus, une personne disposant de ce genre de qualification. Cela signifie que les communes ayant répondu positivement n'ont pas forcément activement recherché à engager un expert en informatique. Parmi les 72 communes ayant répondu au questionnaire, seules 12 (16,6%) disposent de ce type de compétences. Cela représente bien la réalité des communes vaudoises. Comme expliqué précédemment, avec une majorité d'entre elles de petite taille et disposant d'un budget limité, l'investissement dans du personnel qualifié reste compliqué.

Comp IT	Taille				
	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	34	13	9	4	
Oui	5	3	3		1

Figure 13 - Compétences IT

Nous avons ensuite souhaité comprendre quel était, du point de vue politique, le niveau de priorité donné à la digitalisation des services communaux au travers de services en ligne et à la problématique de la sécurité informatique (question 6).

	Taille				
Importance stratégique de la digitalisation des services communaux	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
1	3	1	1		
2	3	3			
3	7	6	6	1	
4	7	3	3	3	
5	3		2		1

Figure 14 - Importance stratégique digitalisation services communaux

L'échantillon de données est issu des communes ayant un budget dédié. 37,73 % de ces dernières indiquent une importance moyenne (3) vis-à-vis de cette problématique. Elles sont 30,18 % à décrire une importance élevée (4).

En ce qui concerne la cybersécurité, l'échantillon estime que cette thématique est importante. 30,17% des communes décrivent une importance élevée (4) et 47,16% parlent d'une importance très élevée (5). Ces résultats sont à mettre dans le contexte. L'année 2021 a été particulièrement agitée en ce qui concerne les attaques informatiques contre les communes avec l'exposition médiatique qui en a résulté. C'est pourquoi cette thématique a pris une grande importance. Il serait intéressant de répéter cette étude dans quelques années afin de savoir comment évolue cette perception de l'enjeu stratégique de la cybersécurité.

	Taille				
Importance stratégique de la cybersécurité	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
1		1			
2	3	1	1		
3	5	1			
4	5	5	5	1	
5	10	5	6	3	1

Figure 15 - Importance stratégique sécurité informatique

Que nous ont appris les données récoltées à propos de la gestion stratégique de la cybersécurité dans les communes ? Premièrement, que dans certaines communes de petite taille, un poste de responsable informatique n'existe pas. Quand il existe, il s'agit dans la majorité des cas d'un membre de la municipalité. Une minorité de communes compte parmi ses employés des personnes disposant de compétences spécialisées en informatique. Au niveau de l'importance stratégique donnée à la digitalisation des services communaux, la majorité des communes indiquent une importance moyenne ou élevée. En ce qui concerne la problématique de la cybersécurité, les communes reconnaissent majoritairement une importance élevée à très élevée.

4.3 Gestion des prestataires externes

Lors de notre entretien avec l'Union des Communes Vaudoises (UCV), les responsables nous ont expliqué que la majorité des communes font appel à des prestataires de services externes pour les assister dans la gestion de leurs infrastructures informatiques. La première question que nous avons posée à chaque commune cherche à savoir si cette dernière a dressé une liste des prestataires avec lesquels elle travaille. La création d'une liste de fournisseurs de services informatiques fait partie des recommandations de la norme NIST et nous donne une première vision sur le niveau de maturité des communes dans la gestion de leurs fournisseurs. Les communes étant soumises à la Loi sur la Protection des Données (LPD) et à la Loi vaudoise sur la Protection des Données personnelles (LPrD), il est nécessaire pour elles de s'assurer que les prestataires avec lesquels elles travaillent répondent aux exigences légales.

Dans un rapport publié en 2022 dans le cadre de la guerre en Ukraine [34], Microsoft a étudié les méthodes utilisées par les services de renseignements russes lors de l'offensive en Ukraine. Les hackers ont pris pour cible notamment des entreprises actives dans le domaine IT fournissant des services aux autorités ukrainiennes et aux pays de l'OTAN. Ce que nous apprend cette guerre, c'est que les communes doivent non seulement s'occuper de connaître les enjeux de la cybersécurité, mais également s'assurer que leurs prestataires en amont sont également bien préparés. C'est pourquoi nous nous intéressons particulièrement à cette thématique.

Parmi les communes ayant répondu au questionnaire, 73,61% disent avoir établi une liste de leurs prestataires informatiques (question 11). Ce sont les communes de moins de 1000 habitants qui procèdent le moins à ce type de listing (64,10%), suivies par les communes entre 1000 et 1999 habitants (68,75%). Les communes de plus de 2000 habitants ayant répondu au questionnaire ont toutes établi une telle liste.

	Taille				
Liste des prestataires informatiques	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	14	5			
Oui	25	11	12	4	1

Figure 16 - Liste prestataires informatiques

Nous avons ensuite souhaité savoir avec combien de prestataires informatiques les communes travaillent (question 12.b). Cette information est importante car plus le nombre de prestataires augmente, plus la gestion des systèmes d'information peut devenir complexe. Cela s'explique dans la mesure où chaque produit doit pouvoir s'intégrer avec les autres dans un écosystème et que les liens entre les différentes applications et les données qui leur sont associées peuvent représenter des vulnérabilités potentielles. Plus le nombre de prestataires différents est important plus la gestion de ces derniers doit être faite de manière méthodique. Dans notre échantillon, 35% des communes travaillent avec un prestataire informatique et 36,6% des communes travaillent avec 2 prestataires. Une grande commune assure travailler avec plus d'une centaine de prestataires.

	Taille				
Nombre de prestataires	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
0	1				
1	14	8	2	1	
2	16	3	7		
3	6	3			
4	1		1	1	
5		1	2	1	
6				1	
100+					1
je ne sais pas		1			

Figure 17 - Nombre de prestataires informatiques

Nous avons ensuite souhaité savoir si, dans leurs négociations avec leurs prestataires informatiques, les communes ont établi une liste d'exigences en lien avec la cybersécurité (question 12.c). 54,16% des communes répondent avoir établi une telle liste. Cela signifie que pour le reste des communes, la thématique n'a pas été abordée lors des négociations de leurs contrats. Il est également intéressant de remarquer que toutes les communes entre 5000 et 9999 habitants ont répondu non. On trouve ainsi une inégalité dans la manière dont les contrats sont conclus entre les différentes communes.

	Taille				
Liste d'exigences cybersécurité	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Oui	17	13	8		1
Non	21	3	4	4	
Nous ne faisons pas ..	1				

Figure 18 - Liste d'exigences de cybersécurité établie lors de la signature du contrat

Malgré avoir indiqué qu'elles ont établi une liste d'exigences, les communes qui l'ont fait ne se basent généralement pas sur des normes nationales et reconnues. A la question « Est-ce que cette liste d'exigences se base sur une norme nationale (norme minimale pour les TIC) ou internationale ? (NIST Framework, ISO 2700x) » (question 12.d) 51,28% des communes répondent non. 30,76% indiquent travailler sur la base de recommandations de prestataires externes. Cela signifie que dans la majorité des cas, les listes d'exigences envoyées aux prestataires ne reposent pas sur des bases standardisées.

	Taille				
Norme exigence	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non;	25	10	7	3	1
Recommandation partenaire externe (P.E: Cyber-safe - Merci de préciser) ;	4	4	4		
Autre (merci de préciser);	3	1	1		
ISO 27001;	1				
NIST Framework;	2	1			
Norme nationale;	2				
Je ne sais pas	2			1	

Figure 19 - Exigences Normes

La question suivante détermine si les communes ont convenu des accords de niveau de service (SLA) (question 12.f) spécifiques à la cybersécurité avec leurs prestataires externes. Cette question a pour objectif de savoir si les communes se sont posé la question de savoir si leur prestataire est disponible en cas de problème et s'il peut être atteint par exemple en dehors des heures conventionnelles de bureau. Ce que nous montrent les données, c'est que 83% des communes ont répondu ne pas avoir conclu de SLA spécifique à la cybersécurité ou ne pas le savoir.

	Taille				
SLA	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Je ne sais pas	14	4	6	1	
Non	23	7	2	2	1
Oui	2	5	4	1	

Figure 20 - Cybersecurity Service Level Agreement (SLA)

Finalement, nous avons souhaité savoir où les communes stockent leurs données (question 9.a). 52,78% des communes interrogées indiquent que leurs données sont stockées sur les serveurs de leurs prestataires informatiques. 27,78% stockent leurs données sur un serveur interne et 19,44% stockent leurs données sur un service cloud. Ce que l'on peut tirer comme conclusion, c'est que dans la grande majorité des cas, les communes stockent des données sur les serveurs d'entreprises tierces. Afin de respecter les législations suisse et vaudoise sur la protection des données, il est nécessaire pour elles de négocier avec leurs prestataires les conditions de ce stockage, notamment le lieu de stockage et la gestion des accès.

Stockage Données	Taille				
	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Serveur interne	7	2	8	2	1
Sur les serveurs de votre prestataire informatique	23	10	3	2	
Sur un service cloud	9	4	1		

Figure 21 - Stockage des données

A la question de savoir si les communes procèdent à des sauvegardes régulières de données, 94,44% des communes répondent positivement. 4 communes répondent ne pas savoir si des sauvegardes sont régulièrement effectuées. La régularité de ces sauvegardes est variable en fonction des contrats conclus par les communes avec leurs prestataires de services informatiques. Elles sont 77,77% à indiquer que leurs sauvegardes sont enregistrées sur les serveurs de leurs partenaires informatiques ou sur un service cloud.

En conclusion, comme nous en avions fait l'hypothèse, les communes du canton de Vaud dépendent de prestataires externes pour gérer leurs infrastructures informatiques. En raison de la doctrine vaudoise de libre marché, chaque commune négocie de manière indépendante les conditions et les services fournis. Cette méthode a des avantages : en cas d'attaque réussie contre un prestataire, le nombre de communes impactées est limité car le système est décentralisé. Cela a également pour avantage de pousser les prestataires à proposer des conditions intéressantes afin d'être compétitifs sur le marché. Il existe toutefois des inconvénients : Il n'existe pas de liste d'exigences en termes de cybersécurité similaire pour toutes les communes. Il en résulte que le niveau de protection peut être très différent. Le niveau de service peut également être impacté par ces différences au niveau des exigences. Alors qu'une commune pourra contacter son prestataire 24h/24 7j/7 en cas de problème, une autre ne le pourra pas. Nous verrons plus tard quels types de solutions pourraient répondre à cette problématique.

4.4 Procédures et gestion

Notre analyse des procédures internes des communes commence par s'intéresser à la question de savoir si la municipalité a considéré le risque lié à la cybersécurité dans sa politique de gestion des risques (question 11). En effet, la gestion des risques est un point central, que ce soit dans la norme NIST ou dans la norme ISO 27001, qui sont les références dans le domaine de la cybersécurité. Etablir une analyse de risque est souvent la première étape pour mettre en place une politique crédible de sécurité informatique. Parmi les communes ayant répondu au questionnaire, 58,33% indiquent avoir établi une analyse de risque. Cela signifie aussi que près de la moitié des communes n'ont pas établi ce type d'analyse.

	Taille				
Analyse Risque	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	20	7	2	1	
Oui	19	9	10	3	1

Figure 22 - Analyse de risques

Nous avons ensuite souhaité savoir quelles procédures ont été mises en place par les communes dans l'éventualité d'un évènement en lien avec la cybersécurité (question 14.a). Mettre en place des procédures permet à chacun de savoir comment réagir en cas d'incident et de répartir les responsabilités. Cela évite de se retrouver pris par surprise et de commettre des erreurs. 17 communes (23,61%) indiquent n'avoir pas de procédures. 11 communes (15,27%) indiquent être en train de travailler pour créer ce genre de procédures. De manière générale, il existe une grande inégalité dans les procédures et pratiques mises en place dans les différentes administrations. Cela pose la question de la capacité de résilience des communes et de leur capacité à prendre les bonnes décisions en cas d'incidents.

	Taille				
Procedure	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	10	5	2		
En cours	4	2	3	2	
Externe	2		2		
Plan de communication	5	3		1	
Procédure d'alerte auprès de la police	6	5	1	1	
Procédure d'Identification de l'attaque	3	3	1		1
Procédure d'isolation des systèmes du réseau	4	3	3	1	1
Procédure de cellule de crise	6	3	3		
Procédure de récupération des données	7	1	3	1	1
Autre (Merci de préciser)	3	3			

Figure 23 - Procédures

À la suite de notre discussion avec les autorités cantonales, il a été établi que dans la procédure actuelle[7], lors d'un incident, les communes sont invitées à informer les autorités au travers de la police (117) et de son unité cybercrime. Une fois la police contactée, les experts du centre opérationnel de sécurité (SOC) du canton, en collaboration avec l'état-major cantonal de conduite, prennent position pour soutenir la commune impactée. Elles doivent également être en mesure d'isoler leurs systèmes informatiques dans des courts délais afin de s'assurer que l'attaque ne se propage pas dans une trop grande mesure. C'est pourquoi nous estimons qu'il est important que

[7] https://www.vd.ch/fileadmin/user_upload/organisation/dinf/dsi/ussi/Annexe_ConseilsCyberattaque.pdf

les communes soient au courant et aient mis en place des procédures d'alerte à la police et qu'elles soient en capacité d'isoler leurs systèmes en cas d'urgence.

Elles ne sont malheureusement que 13 communes à avoir mis une procédure en place pour l'appel à la police et 12 communes à avoir mis en place une procédure d'isolation du réseau.

L'attaque de la commune de Rolle a révélé qu'il est primordial d'avoir une procédure en place pour assurer la communication avec le public. Le pire qui puisse arriver pour une commune, c'est qu'une fuite de données soit révélée par la presse, ce qui peut mettre à mal sa réputation et la confiance que lui confèrent ses citoyens.

Nous avons voulu savoir si les employés des communes ont reçu une formation sur la thématique de la cybersécurité au cours des deux dernières années. En effet, de nombreuses attaques se basent sur des méthodes d'ingénierie sociale où les collaborateurs sont invités à ouvrir des fichiers infectés, cliquer sur des liens ou transmettre des données d'identification (phishing). L'une des manières les plus efficaces pour prévenir ce genre d'attaque est la formation et la prévention auprès des collaborateurs des communes. Il est également important que la direction et les municipaux suivent cette formation car des attaques de plus en plus sophistiquées (spear phishing) s'intéressent aux dirigeants des entreprises (whaling). Parmi les communes ayant répondu au questionnaire, 2/3 ont proposé ce genre de formation à leurs collaborateurs. Cela signifie également que de nombreuses communes n'ont pas procédé à ce genre de formation. Une question qu'il serait pertinente de poser lors d'une prochaine étude, serait de savoir quels sont les sujets abordés lors de ces formations et si la qualité de ces dernières est équivalente entre les différentes communes. Nous n'avons malheureusement pas de données concernant la formation des municipaux.

	Taille				
Formation	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	15	4	3	1	
Oui	24	12	8	3	1

Figure 24 - Formation des employés communaux

Lors de notre discussion avec l'UCV et les autorités cantonales, la question de la mise en place de l'authentification à 2 facteurs a été abordée comme une mesure majeure permettant de protéger les infrastructures informatiques des communes. En effet, comme nous le verrons plus tard dans notre analyse de risque, la protection des accès aux informations est un point central dans la protection des données. 54,71% des communes interrogées indiquent avoir mis en place ce type de mesure de protection pour accéder à leurs données. Cela signifie que dans 45% des cas, les communes sont uniquement protégées par des mots de passe, ce qui les rendent plus vulnérables à des attaques de type force brute ou d'attaques de phishing.

	Taille				
Double authentification	Moins de 1000 habitants	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habitants
Non	12	7	2	3	
Oui	11	6	10	1	1

Figure 25 - Double Authentification

Nous avons finalement voulu savoir si les communes faisaient appel à des sociétés externes pour tester régulièrement leur capacité à résister à divers types d'attaques (ethical hacking – question 17). Parmi les communes ayant répondu au questionnaire, elles sont 27,77% à faire appel à ce type de service. Cela signifie que dans la majorité des cas, les communes n'ont pas de moyens et d'indicateurs (KPI) pour mesurer l'efficacité des systèmes mis en place, ni la sensibilisation de leurs collaborateurs à la problématique.

	Taille				
Ethical hacking	Moins de 1000 habitan..	1000 - 1999 habitants	2000 - 4999 habitants	5000 - 9999 habitants	10'000 - 19'999 habit..
Non	32	11	6	3	
Oui	7	5	6	1	1

Figure 26 - Ethical Hacking

En conclusion, les communes restent indépendantes dans la mise en place de leurs procédures de gestion de la cybersécurité et de réponses en cas d'incident. Alors que certaines semblent s'être préparées à l'éventualité d'une attaque, d'autres n'ont pas de procédures en place. Comme expliqué plus haut, les autorités cantonales souhaitent avoir le lead en cas de problème, car elles estiment que la crise ne peut pas être gérée par les seules autorités communales. Une question plusieurs fois abordée, que ce soit par l'Union des Communes Vaudoises (UCV) ou par les autorités cantonales, concerne la gestion des ressources en cas d'incident et le développement du SOC (Security Operation Center) capable à la fois de répondre aux demandes des communes tout en assurant les besoins des systèmes de l'administration cantonale. Cette question est politique, car il y a des décisions en lien avec le financement de cette infrastructure, nous pourrons toutefois tenter de donner des pistes d'améliorations dans la partie suivante.

4.5 Réseau

Dans la presse, il a été révélé que dans un grand nombre de cas, les responsables municipaux se retrouvent démunis face à la problématique de la cybersécurité qui n'est pas leur spécialité. Nous avons souhaité comprendre quels sont les réseaux existant pour les responsables communaux et avec qui ces derniers entrent en contact lorsqu'ils ont une question. Lors d'un entretien avec un responsable de commune, ce dernier nous a indiqué que lorsqu'un municipal est nommé en tant que responsable informatique, il ne reçoit pas d'informations particulières, que ce soit de la part du canton ou de l'Union des Communes Vaudoises. Il n'avait pas connaissance de réseau de partage de connaissances intercommunal.

Selon nos recherches, il existe un réseau de responsables informatiques communaux, l'Association vaudoise des Responsables informatiques communaux (AVRIC). Cette dernière regroupe les communes de plus de 7000 habitants avec la possibilité que les petites communes soient représentées collectivement par un délégué[8]. De fait, cela signifie que plus de 90% des communes n'ont pas accès à ce réseau.

Parmi les communes ayant répondu au questionnaire, la majorité (94,44%) dit ne pas avoir développé de réseau de partage d'informations (question 15.a) et de connaissances avec d'autres

[8] https://www.ucv.ch/fileadmin/documents/pdf/Communication/PC/PC41-2012_MAG_UCV.pdf

communes. Certaines (8,33%) citent travailler avec l'UCV, les autorités cantonales ou encore l'association Cybersafe (Question 15.b). Cela reste ainsi assez anecdotique.

Que nous expliquent ces données ? Que le système vaudois reste encore très cloisonné et que les communes travaillent chacune de leur côté, ne partageant que peu les unes avec les autres. Cela a pour conséquence que les municipaux peuvent se retrouver seuls lorsqu'ils sont confrontés aux questions de cybersécurité et ne savent pas exactement vers qui se tourner. Les communes doivent, chacune de leur côté, créer des règles et des procédures, ce qui pourrait potentiellement être standardisé par la création d'un guide de bonnes pratiques et de procédures standards à destination des communes. Comme nous le verrons plus tard, nous estimons qu'il est possible de développer un modèle de partage de bonnes pratiques au moyen des nouvelles technologies.

4.6 Remarques

La dernière section de notre questionnaire laisse les communes libres de nous communiquer leurs remarques concernant la thématique de la cybersécurité. Nous avons décidé d'inclure cette partie afin que toutes les thématiques pertinentes pour les communes puissent être abordées, même si elles ne sont pas couvertes par le questionnaire.

Un répondant exprime sa frustration concernant le poids des petites communes sur les fournisseurs de services informatiques. Il propose de créer une forme de consortium de clients d'un même prestataire afin d'avoir de meilleures conditions dans le domaine de la cybersécurité.

De nombreuses communes parlent de la nécessité de former leurs collaborateurs régulièrement. 8 communes mentionnent cette thématique en commentaire. Il existe ainsi une grande demande en ce sens.

La deuxième thématique la plus mentionnée concerne la question de la centralisation des procédures et règles internes. Ainsi, un répondant explique que dans la grande majorité des communes, le type de données enregistrées sur les serveurs est similaire. Il souhaiterait que le canton ou l'Union des Communes édicte un document officiel sur le niveau de confidentialité de ces différentes données et des prescriptions pour la sécurisation de ces différents niveaux de confidentialité. Aujourd'hui, chaque commune doit réaliser cette analyse de son côté. Elles sont 6 à mentionner cette thématique. Il y a donc une demande pour un plus grand partage d'informations et pour une meilleure communication entre les communes, les autorités cantonales et les associations de communes sur la thématique. Un répondant demande par exemple une check-list ou un document similaire permettant de s'assurer que la commune a mis les bonnes mesures en place. Une autre demande concerne une plus grande information concernant les types d'attaques et de risques qui sont actuellement les plus importants.

Finalement, certaines communes demandent plus de soutien financier de la part du canton ou de la Confédération pour la mise en place de mesures de cybersécurité. Elles se plaignent de leur manque de moyens dû à leur taille. Une commune propose par exemple un subside de la part du canton pour réaliser un audit de cybersécurité.

4.7 Conclusion

En conclusion de cette analyse, voici les points que nous estimons les plus importants à retenir :

- Les difficultés budgétaires représentent un frein à la mise en place d'une stratégie crédible de cybersécurité. Les communes du canton de Vaud, dans leur grande majorité, disposent de relativement petits budgets. Ce manque de moyens implique que des choix doivent être faits et que, pour certaines communes, l'informatique, la digitalisation et la cybersécurité ne sont pas des investissements prioritaires. Certaines petites communes n'ont pas de budget dédié à l'informatique. Ce manque de moyens se reflète dans le pourcentage de communes mettant des ordinateurs à la disposition de leurs municipaux (32,69%). Toutefois, la problématique est reconnue. Durant les 5 dernières années, les budgets informatiques et de cybersécurité ont augmenté (voir figures 8 et 9).

- Dans certaines communes de petite taille, un poste de responsable informatique n'existe pas. Lorsqu'il existe, il s'agit dans la majorité des cas d'un membre de la municipalité. Une minorité de communes compte parmi ses employés des personnes disposant de compétences spécialisées en informatique. Au niveau de l'importance stratégique donnée à la digitalisation des services communaux, la majorité des communes indiquent une importance moyenne ou élevée. En ce qui concerne la problématique de la cybersécurité, les communes reconnaissent une importance stratégique importante. (Voir figure 14 et 15)

- Les communes du canton de Vaud dépendent de prestataires externes pour gérer leurs infrastructures informatiques. Dans une majorité des cas, les communes stockent et sauvegardent leurs données sur des serveurs externes, qu'il s'agisse de ceux de leurs prestataires ou de services cloud. Du fait de leurs activités, elles stockent des données personnelles, sensibles et financières sur les résidents. En raison de la doctrine vaudoise de libre marché, chaque commune négocie de manière indépendante les conditions et les services fournis. Cette méthode a des avantages : en cas d'attaque réussie contre un prestataire, le nombre de communes impactées est limité car le système est décentralisé. Cela a également pour avantage de pousser les prestataires à proposer des conditions intéressantes afin d'être compétitifs sur le marché. Il existe toutefois des inconvénients : il n'existe pas aujourd'hui de liste d'exigences en termes de cybersécurité similaire pour toutes les communes. Il en résulte que le niveau de protection peut être très différent selon le prestataire et le contrat conclu avec la commune. Cela peut poser des problèmes au niveau du respect des prescriptions de la loi vaudoise sur la protection des données qui implique que celles-ci soient stockées dans des pays dont la législation est compatible avec le niveau de protection suisse. Le niveau de service peut également être impacté par ces différences relatives aux exigences. Alors qu'une commune pourra contacter son prestataire 24h/24 7j/7 en cas de problème, une autre ne le pourra pas. Un autre inconvénient relevé dans les remarques concerne le faible pouvoir de négociation des petites communes pour obtenir des conditions intéressantes auprès de leurs prestataires externes.

- Les communes restent indépendantes dans la mise en place de leurs procédures de gestion de la cybersécurité et de réponses en cas d'incident. Alors que certaines semblent s'être préparées à l'éventualité d'une attaque, d'autres n'ont pas de procédures en place. Les autorités cantonales souhaitent garder le contrôle en cas de problème, car elles estiment que la crise ne peut pas être gérée par les seules autorités communales. Elles estiment que la gestion de crise nécessite des compétences spécifiques et ne peut pas s'improviser. Une question plusieurs fois abordée, que ce soit par l'Union des Communes Vaudoises (UCV) ou par les autorités cantonales, concerne la gestion des ressources en cas d'incident et le développement d'un SOC (Security Operation Center) capable à la fois de répondre aux demandes des communes tout en assurant les besoins des systèmes de

l'administration cantonale. Cette question est politique, car il y a des décisions en lien avec le financement de cette infrastructure.

- La formation semble être un point très important pour les communes. Elles sont 2/3 à avoir offert des formations à leurs collaborateurs. Il est important de noter que les élus devraient également recevoir une telle formation, afin qu'ils ne soient pas victimes de tentatives de phishing ou autre.

- Le système vaudois reste encore très cloisonné et les communes travaillent chacune de leur côté, ne partageant que peu les unes avec les autres. Cela a pour conséquence que les municipaux peuvent se retrouver seuls lorsqu'ils sont confrontés aux questions de cybersécurité et ne savent pas exactement vers qui se tourner. Les communes doivent, chacune de leur côté, créer des règles et des procédures.

- Les communes, dans leurs remarques, appellent à des mesures de centralisation pour certaines compétences et souhaitent mieux partager les bonnes pratiques entre elles. Du fait de la similitude des processus et des données gérées par les communes, elles souhaitent pouvoir bénéficier d'un guide de classification de la confidentialité des données et des mesures nécessaires à mettre en place pour les protéger.

5 Etude qualitative

5.1 Point de vue des communes

Lors de l'écriture de notre planification du travail de master, nous avions prévu de rencontrer plusieurs responsables de communes pour des entretiens semi-directifs. Malheureusement, la contrainte temporelle ne nous a pas permis de réaliser autant d'entretiens que nous l'aurions désiré. Nous avons toutefois eu la chance d'interviewer un responsable communal d'une petite commune (moins de 1000 habitants) qui nous a décrit les problématiques et les attentes qu'il a vis-à-vis de la cybersécurité. Il est important de préciser que cette commune est dans un état d'avancement relativement élevé dans la mesure où elle travaille depuis plusieurs mois sur un projet de certification Cyber-safe et que le municipal en charge est lui-même spécialisé dans les questions de cybersécurité dans le cadre de sa profession.

Le responsable communal interrogé est en charge des services industriels et, travaillant professionnellement dans le domaine de l'informatique, il a souhaité intégrer cette thématique dans son dicastère après les élections de 2021. Il s'occupe de planifier le budget, le suivi des comptes, également du coaching avec les employés communaux pour les former et les accompagner au changement lors de l'installation de nouvelles applications ou la mise en place de nouvelles procédures. Il s'occupe ainsi plutôt de la gestion financière et stratégique et laisse les questions techniques et opérationnelles à son prestataire externe.

La commune a eu la chance de profiter du soutien de la Confédération dans le cadre d'un projet pilote pour le financement d'audits de sécurité. Ainsi pour cette commune, l'audit sur l'état actuel de la situation des systèmes d'information en matière de cybersécurité a été gratuit. Les mesures techniques et organisationnelles qui seront implémentées à la suite de cet audit doivent quant à elles être financées par la commune. Comme la thématique de la cybersécurité était nouvelle au moment où le municipal responsable l'a présentée à ses collègues (avant les évènements de 2021) et que, de manière générale l'informatique coûte de plus en plus cher, cette aide de la Confédération a été un facteur important pour que le projet soit approuvé par la municipalité.

Il estime ainsi qu'un soutien financier ou organisationnel de la part du canton pour « booster les communes » serait une bonne chose afin de leur permettre de réaliser un audit de cybersécurité de manière facilitée et à moindres frais. Il imagine la création d'un fond pour la cybersécurité des communes qui permettrait de financer des mesures ciblées pour les aider à évoluer dans le bon sens. Il est important de préciser que cette commune travaille avec l'association Cyber-Safe. NDLA : des échos reçus de la part d'autres communes indiquent qu'il est nécessaire de laisser le choix du prestataire réalisant l'audit.

Les données sont sauvegardées toutes les heures sur un disque dur externe dans les locaux de la commune, dans un local sécurisé et non accessible sans autorisation. Les données sont également envoyées par canal chiffré chez le prestataire pour avoir une seconde copie.

Il nous indique que sur les serveurs de sa commune sont stockées des données très sensibles, notamment des données personnelles des citoyens, ainsi que des données financières qu'il est nécessaire de protéger.

Comme la commune est en train de chercher à obtenir le label Cyber-Safe, elle a déjà mis des mesures en place permettant d'assurer une plus grande sécurité de ses données. Entre autres, elle dispose d'un pare-feu qui protège son réseau interne des menaces venant de l'internet. Les municipaux, comme nous l'avons vu dans notre étude quantitative, travaillent avec leurs propres

machines. Afin de régler le fonctionnement de cette problématique, ils ont établi une charte indiquant des règles pour la sauvegarde de documents sur les machines privées. Les services de mails sont stockés en Suisse et protégés par des mots de passe forts. Notre interlocuteur n'a pas d'information quant à l'utilisation par les municipaux de gestionnaires de mots de passe.

La commune n'a pas beaucoup de services digitalisés. Elle a un site internet disponible sur mobile où les citoyens peuvent trouver les formulaires administratifs. Il n'y a ainsi pas réellement de services offerts à la population disponibles en ligne. Il y a toutefois un projet de digitalisation des processus du contrôle des habitants qu'il souhaite mettre en place dans un second temps, une fois que ce projet de labélisation Cyber-safe sera complété. Le problème avec la digitalisation des services communaux revient au rapport coût/bénéfice, avec des outils qui seraient en fin de compte peu utilisés selon la taille de la commune. Il souhaite finalement mettre en place un système de gestion électronique des documents.

Au niveau de la labélisation, toutes les mesures techniques et de gestion de prestataires ont déjà été mises en place par la commune. Le plus gros challenge que la commune rencontre concerne toute la documentation nécessaire (politique de sécurité, plan de reprise, cartographie des données, inventaire, chartes diverses) qui prend énormément de temps pour un municipal travaillant à 10-20% pour sa commune.

Nous avons voulu savoir comment un municipal fraîchement élu en tant que responsable informatique était accueilli par le canton ou les associations de communes pour lui permettre de prendre pleine possession de ses fonctions. Selon son expérience, il n'a pas reçu de mail ni d'invitation, que ce soit de la part du canton ou de l'UCV. Il est au courant que l'UCV propose régulièrement des formations et évènements en lien avec la thématique, mais rien n'est fait proactivement pour contacter les municipaux en charge de l'informatique et leur proposer une journée d'introduction ou de formation. Il nous indique que dans les petites communes il faut « apprendre sur le tas », car il n'y a pas de personnel pouvant faire de transition. Il n'existe également pas à sa connaissance des groupes d'intérêts intercommunaux où les responsables informatiques partagent entre eux les bonnes pratiques.

L'analyse de risque que la commune a effectuée repose sur deux critères :

- Le type de données (données sensibles, données personnelles, données financières)
- La valeur des données (nombre de données, valeur sur le marché si volées)

En fin d'entretien, nous avons demandé à notre répondant quelles étaient ses attentes pour les autorités cantonales :

- Support financier pour la cybersécurité
- Clarification des procédures en cas d'évènement
- Bibliothèque documentaire (procédures standards, modèles de charte informatique, etc.)
- Coaching

Voici ses attentes concernant l'entraide intercommunale :

Création d'une commission intercommunale où les responsables informatiques se rencontreraient régulièrement pour discuter des problématiques et faire connaissance.

5.2 Point de vue du canton

Durant l'écriture de ce travail de Master, nous avons également eu la chance de nous entretenir avec Monsieur Marc Barbezat, directeur de la sécurité numérique de l'Etat de Vaud, afin d'avoir le point de vue des autorités cantonales sur la problématique de la cybersécurité des communes.

Aujourd'hui, les autorités cantonales interviennent dans le cas de situations de crise, lorsque des systèmes d'information publics sont touchés par une attaque. Comme la problématique de la cybersécurité a commencé à réellement être abordée en 2021 pour donner suite aux attaques qui ont été mentionnées dans la presse, des discussions sont en cours avec les faitières de communes pour savoir comment canton et communes peuvent collaborer sur cette problématique et sur quel périmètre. Ainsi des discussions sont en cours entre les conseillères d'Etat Rebecca Ruiz et Christelle Luisier, les associations de communes (l'UCV et l'ADCV) ainsi que l'AVRIC qui regroupe les responsables informatiques des grandes communes, pour définir les conditions de cette coordination, que ce soit au niveau financier ou au niveau organisationnel.

Un scénario probable selon les discussions actuelles voudrait que les communes puissent se reposer sur l'expertise du canton en cas de crise. Trois acteurs cantonaux travaillent en collaboration avec la commune :

- L'EMCC (Etat Major Cantonal de Conduite) disposant de méthodologies prouvées de gestion de crise qui peut intervenir afin de soutenir les communes en cas d'évènement en lien avec la cybersécurité. Il est nécessaire d'avoir une organisation bien huilée pour permettre aux communes de communiquer avec leurs citoyens, permettre de continuer à fournir des services à la population.
- L'entité cybercrime de la police.
- Le SOC du canton (équipe spécialisée en charge de la supervision des systèmes d'informations cantonaux pour les protéger contre les cyberattaques).

Le canton n'a toutefois pas l'intention de se substituer à la commune, il fournit des conseils et des recommandations, les décisions restant du domaine des responsables communaux.

Au niveau de la réponse plus technique en lien avec l'infrastructure informatique en elle-même, le scénario en discussion privilégie un partenariat public/privé, où les services du SOC du canton travaillent avec le prestataire informatique de la commune impactée.

Il n'existe pas aujourd'hui de procédures de gestion de crise partagées avec les communes car, selon notre interlocuteur, la gestion de crise ne s'improvise pas et il est nécessaire de faire appel à des professionnels en cas de problème, que ce soit dans le cadre d'un plan de communication ou de continuité des opérations. Le canton communique toutefois avec les responsables communaux sur différents points :

- Lorsque de grandes vulnérabilités (Log4shell par exemple) sont découvertes afin que les communes prennent des mesures pour mieux protéger leurs systèmes d'information.
- Rappel des bonnes pratiques basées sur le NCSC.
- Le canton a également organisé au début de la législature des soirées de formation en collaboration avec la police cantonale sur les thématiques de la sécurité où la question de la cybersécurité a été abordée.

L'équipe de notre interlocuteur est avant tout en charge de répondre aux besoins du canton en matière de cybersécurité. L'utilisation des ressources en personnel pour des problématiques communales pourrait impacter négativement les services rendus au canton. C'est pourquoi les discussions en cours essaient de définir exactement comment s'organiser pour que le canton ait cette capacité de réponse lors d'évènements communaux, tout en pouvant continuer à opérer avec ses propres systèmes d'information. Il y a bien sûr des considérations financières en jeu. Un projet serait de renforcer le SOC avec plus de ressources, ce qui permettrait d'absorber les crises au niveau communal et d'augmenter le niveau de prévention auprès des communes.

En conclusion de notre entretien, M. Barbezat se reconnaît chanceux d'avoir comme conseillers d'Etat des personnes qui soutiennent activement la problématique avec des investissements importants dans la digitalisation et qui sont sensibles à la question de la cybersécurité. Cette année, le canton est dans une démarche de certification ISO 27001.

5.3 Conclusion

Ce que cette analyse nous permet de conclure, c'est que l'ensemble des acteurs avec qui nous avons été en contact sont au courant de la problématique que représente la cybersécurité. Pour un responsable travaillant à temps partiel pour sa commune, la charge que représente la création d'un plan de protection ainsi que toute la documentation nécessaire à la mise en place de ce dernier est un frein à l'évolution de la maturité des communes. Les limitations budgétaires sont également un facteur qui peut pousser certaines communes à faire l'impasse sur des investissement dans la numérisation des services communaux ainsi que dans le développement de la cybersécurité.

Pour les responsables cantonaux, la situation est similaire. L'équipe du centre opérationnel de sécurité est en charge des besoins du canton et doit également intervenir régulièrement pour soutenir les communes lorsque des incidents de cybersécurité arrivent. Aujourd'hui la capacité en ressources humaines reste limitée, ce qui a pour effet de prétériter les services du canton au profit des communes.

Communes et cantons sont ainsi en train de travailler ensemble pour définir la répartition des compétences et du niveau d'implication que devraient avoir les différentes parties prenantes dans la gestion d'une crise en lien avec la sécurité informatique. Il est également question de savoir comment faire en sorte que les élus disposent d'informations et de ressources nécessaires à la mise en place d'une infrastructure informatique crédible et sécurisée.

Le sentiment qui ressort de ces entretiens est que ces collaborations, tant avec le canton qu'intercommunales, sont demandées et qu'elles vont se développer dans l'avenir.

6 Bonnes pratiques

Maintenant que nous avons étudié la situation actuelle des communes, nous allons nous pencher sur les solutions et les bonnes pratiques qui peuvent être mises en place du point de vue organisationnel afin d'améliorer le niveau de cybersécurité des communes dans le canton de Vaud.

6.1 Analyse de risques

Nous allons commencer par établir une analyse de risques afin de déterminer quels scénarii et types d'attaques sont probables et quelles mesures doivent être mises en place en priorité. Nous nous baserons sur la liste des mesures issue des normes NIST et ISO 27001 pour établir un profil cible qui pourra être adapté aux différentes communes selon leurs besoins spécifiques.

Afin de créer une cartographie de risques, il faut d'abord définir quels sont les services communaux qui doivent être sécurisés en priorité. La norme ISO 27001 nous invite à réaliser un périmètre qui énonce clairement quels processus et bases de données font l'objet d'un plan de protection. Cela permet d'investir les ressources dans les services qui comptent le plus. Pour notre étude, nous identifions deux classes à sécuriser :

1. Les services et processus essentiels à la population (contrôle des habitants, gestion des déchets, sécurité publique, police, pompiers, eau, gaz et électricité). Sont exclus de cette analyse de risques les services non essentiels tels que la comptabilité de la commune, la gestion des parcs et jardins ou tout processus n'impactant pas la qualité de vie des citoyens.
2. Les données personnelles des habitants et des entreprises de la commune.

L'objectif de cette étude de risques est de s'assurer que les communes répondent aux exigences de la loi vaudoise sur la protection des données (LPrD). Elle souhaite également être une base permettant la description des exigences en termes de sécurité des systèmes d'information communaux.

Reprenons ce que dit la littérature [24] vis-à-vis des types d'incidents de cybersécurité rencontrés par les communes aux USA. Par ordre d'importance nous trouvons :

1. Violation des données (vol malicieux ou perte/vol de matériel)
2. Divulgation involontaire des données
3. Perturbations (service non accessible ou détourné)
    a. Détournement ou blocage des infrastructures publiques
    b. Attaques DDOS
    c. Ransomware
4. Violation de la vie privée (projet du gouvernement local ne respectant pas la législation)
5. Fraude et extorsion
6. Erreur IT (bug)

Sur cette base, nous pouvons réaliser une analyse de risques, en évaluant l'impact que chaque type d'incident aurait sur la commune, ainsi que la probabilité qu'un tel incident se produise. Nous définissons l'impact comme la mesure des dommages encourus par l'administration communale, que ce soit en termes d'image, d'impact financier ou encore d'impact légal. Afin de réaliser cette analyse, nous nous basons sur la matrice de Mehari[35] qui nous permet de mieux visualiser la problématique. Cette matrice a pour avantage de montrer quels sont les risques qu'il faut traiter en priorité (cases rouges), quels risques sont à inclure dans le plan de gestion des risques (cases jaunes) et quels risques sont acceptables (cases vertes). Nous allons analyser ces risques au niveau des trois critères de la cybersécurité énoncés dans la CIA Triad citée plus haut, à savoir la confidentialité, l'intégrité et la disponibilité.

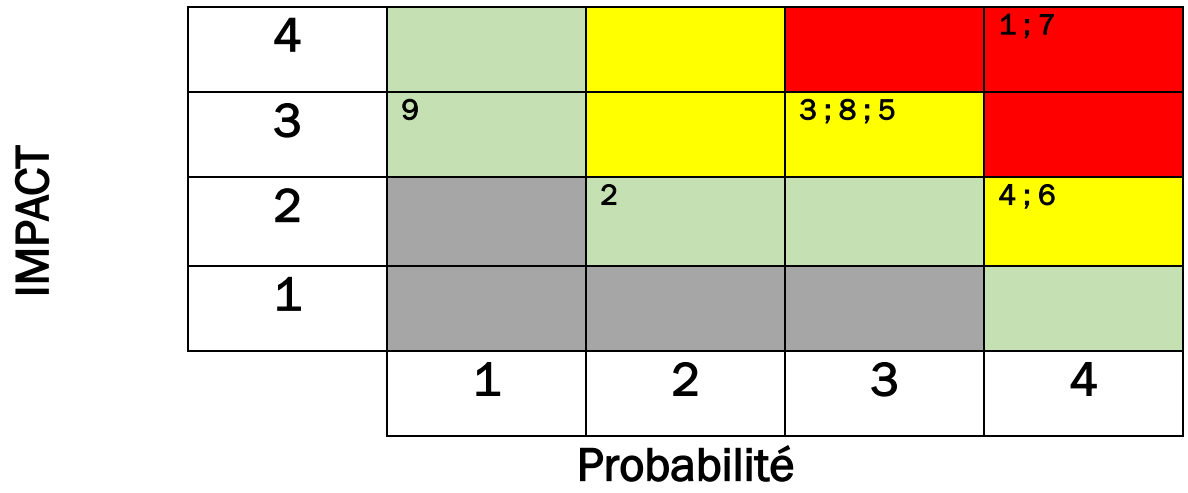


Figure 27 - Analyse de risques communes

Risques identifiés :

1. **Vol de données (Confidentialité) :** les données stockées sur les serveurs des communes ont une grande valeur. En effet, on trouve par exemple des documents officiels tels que des copies de pièces d'identité ou des informations sur la situation financière des personnes et des entreprises. Ces données peuvent être exploitées pour créer des campagnes de phishing ciblées adressées à la population ou pour des usurpations d'identité. Pour une personne mal intentionnée ou une organisation criminelle organisée, il existe ainsi une grande motivation à voler ces données à des fins financières. Nous estimons ainsi que la probabilité d'un tel type d'attaque est élevée. Au niveau de l'impact qu'une telle attaque a sur la commune, sa réputation et la relation de confiance avec les citoyens peuvent être impactées négativement. Comme expliqué précédemment, cela a également un impact sur les habitants et les entreprises qui sont plus susceptibles d'être elles-mêmes la cible d'attaques. C'est pourquoi nous donnons le score de 4 : 4 à ce type d'attaque.

2. **Perte de données (Disponibilité, Intégrité) :** la commune, comme toute entreprise, est sujette à des erreurs de la part de ses collaborateurs, à la défaillance de son matériel informatique et aux attaques d'acteurs internes ou externes mal intentionnés. Une perte de données a le potentiel de mettre à mal la disponibilité d'un service en ligne et/ou de créer des dysfonctionnements à cause des informations manquantes. Ce que notre questionnaire a démontré, c'est que la majorité des communes procède régulièrement à

des sauvegardes de données à des fins de récupération en cas de problème. Nous estimons ainsi qu'une perte de données reste un scénario peu probable et que s'il se produit, il aura un impact relativement faible.

3. Vol de matériel/hardware (Confidentialité, Disponibilité) : toute entreprise est susceptible de faire l'objet de cambriolages de la part de personnes mal intentionnées ou qu'un employé soit victime d'un vol lorsqu'il travaille à distance, par exemple dans le train. Ces dernières ont un intérêt particulier pour l'équipement informatique qui a une grande valeur sur le marché du recel de marchandises. Les données contenues sur ces équipements vont alors disparaitre lors du formatage des disques durs. Le vol de matériel informatique peut également avoir pour objectif le vol de secrets industriels ou des données confidentielles par des concurrents ou des organisations externes mal intentionnées. Nous estimons qu'il existe un réel risque de vol de matériel (probabilité 3) et que ce dernier si non-traité aura un impact important sur l'entreprise (Impact 3). Nous estimons ainsi qu'il est nécessaire de l'inclure dans notre plan de gestion des risques.

4. Divulgation involontaire de données (Confidentialité) : la divulgation involontaire de données est malheureusement un type d'incident fréquent qui peut mettre en péril la réputation d'une institution publique. Voici un bon exemple pour illustrer ce type d'évènement : en 2021, l'office du médecin cantonal vaudois a divulgué par erreur les adresses électroniques de 300 personnes non-vaccinées [36], ce qui lui a valu des articles dans la presse et des potentielles poursuites légales. Ce type d'erreur humaine représente 84,7% des fuites de données [37] et a ainsi une grande probabilité de se produire. Son impact reste difficile à évaluer, car chaque incident reste unique. Nous estimons toutefois que dans la mesure où ces divulgations ne sont pas volontaires, leur impact reste limité mais doit faire l'objet d'un travail continu de sensibilisation.

5. Détournement d'infrastructures publiques (Disponibilité, Intégrité) : les infrastructures publiques représentent un grand potentiel. Avec le développement des infrastructures d'IOT (caméras de surveillances, capteurs, etc.) il existe de plus en plus de vulnérabilités potentielles. L'utilisation de ces nouvelles technologies interroge sur la question de la protection des données des citoyens. En effet, ces derniers risquent de voir celles-ci récoltées par des personnes non autorisées à des fins malveillantes. Finalement, selon le rapport des services de renseignement de la Confédération cité en introduction, les fournisseurs de machines utilisées dans les infrastructures critiques sont de plus en plus victimes de tentatives de piratage, ceci afin d'obtenir un accès stratégique aux infrastructures d'un pays. Les objets connectés sont également de plus en plus exploités sous la forme de botnets dans le cadre d'attaques en déni de service [38]. Nous estimons que pour cette catégorie de risques, l'impact est moyen (score 3) sur les autorités communales. En effet, la sécurisation des outils de IOT doit être considérée comme importante car il faut considérer les nombreux points d'accès aux réseaux de la commune.

   Également de plus en plus fréquent, le détournement par des organisations criminelles d'infrastructures d'entreprises et d'institutions publiques dans l'objectif de miner des cryptomonnaies. C'est ce que l'on appelle le cryptojacking. Concernant le risque lié au cryptojacking, il peut impacter les performances des services numériques, ce qui peut péjorer les services à la population. Encore une fois, l'impact sur la commune est moyen. Nous estimons toutefois que la probabilité d'une telle attaque reste élevée (score de 3) car les cryptomonnaies sont un marché très rentable.

6. **Attaque DDOS (Disponibilité) :** une attaque en déni de service compromet la disponibilité d'un service en ligne. On peut facilement imaginer une entreprise dont les clients et les collaborateurs sont incapables d'accéder aux applications nécessaires à la réalisation de leurs transactions. Il peut en résulter un grand manque à gagner pour une entreprise dépendant de ses services en ligne pour son chiffre d'affaires. Dans le cadre d'une commune, ce type d'attaque est fortement probable. Ces attaques peuvent avoir diverses motivations, qu'elles soient d'ordre criminel, politique ou dans certain cas militaire. Nous estimons toutefois que ce type d'attaque a un impact limité (score 2), car elle agit peu sur le chiffre d'affaires ou sur la réputation de la commune. Il ne faut toutefois pas sous-estimer le risque que ce type d'attaque représente dans le cadre de services essentiels tels que les services d'urgence de la police, des ambulances ou des pompiers. C'est pourquoi il est classé dans la matrice comme devant être inclus dans le plan de gestion des risques.

7. **Chiffrement des données et extorsion (Disponibilité, Intégrité) :** les attaques par ransomware deviennent de plus en plus courantes. En effet, ces dernières permettent aux attaquants de réclamer une rançon aux personnes affectées. Dans les cas répertoriés en 2021 dans les communes vaudoises, ce type d'attaque a eu pour effet de bloquer pendant plusieurs jours les services informatiques communaux. Une attaque de ce type peut avoir plusieurs phases. Tout d'abord, les attaquants bloquent les services de la commune et lui demandent de payer une rançon, souvent en cryptomonnaies. Si cette dernière décide de ne pas payer, l'étape suivante consiste à menacer de diffuser les données sur le darkweb. Finalement, si cela ne marche toujours pas, les attaquants peuvent tenter de se retourner vers une ou plusieurs personnes ou entreprises impactées par le vol de données (par exemple un contribuable fortuné) et de le menacer de diffuser ses données personnelles sur le web. Cela représente ainsi un risque important pour les communes (Score 4). De plus, ce type d'attaque a une haute probabilité de survenir (Score 4), c'est pourquoi nous lui donnons un score élevé. Ce type de risque est ainsi classé comme à traiter en priorité.

8. **Fraude (Intégrité) :** les communes sont susceptibles d'être victimes de fraudes de la part d'organisations criminelles. Les auteurs de ce type d'arnaques commencent par obtenir l'accès à des comptes email et étudient les relations que la commune entretient avec ses fournisseurs. Au moment opportun, ils tentent de se faire passer pour le fournisseur en indiquant un changement dans les coordonnées bancaires afin de recevoir l'argent. Un article de la BBC [39] décrit le procédé comme suit : « "L'arnaqueur recueillait des détails contextuels, en observant le flux de courriels légitimes", explique Crane Hassold, directeur principal de la recherche sur les menaces chez Agari. L'arnaqueur redirigeait les courriels vers un autre compte de courriels, rédigeait des courriels au client qui semblaient provenir de la bonne entreprise, indiquait que "l'entreprise" avait un nouveau compte bancaire, fournissait des informations "mises à jour" sur le compte bancaire et l'argent disparaissait à ce moment-là" ». Nous estimons la probabilité qu'une commune soit la cible de fraude comme élevée (Probabilité 3) avec un impact important sur les finances de la commune (Impact 3). Nous considérons ainsi qu'il est nécessaire d'inclure ce risque dans le plan de gestion des risques.

9. **Erreur IT (Bug) / Zero-Day exploit (Disponibilité, intégrité et confidentialité) :** tout système informatique est susceptible d'avoir des défauts qui peuvent causer des problèmes de disponibilité, d'intégrité ou de confidentialité. Dans la mesure ou la majorité des communes fait appel à des sociétés externes spécialisées dans l'informatique, nous estimons que ce type de risque reste faible dans sa probabilité. Il n'est toutefois pas à négliger dans l'impact

qu'il peut avoir pour la commune (Impact 3). C'est pourquoi nous classons ce risque comme acceptable, dans la mesure où il peut être externalisé chez le fournisseur.

Nous allons maintenant tenter de comprendre plus en détail quelles sont les causes de ces différents types d'attaques. Dans la colonne de gauche, nous retrouvons les différents types cités plus haut. Nous souhaitons savoir si l'origine d'un tel incident est due à un acte délibéré (D), un acte accidentel (A) ou s'il est la conséquence d'un manque de procédure (P). Nous essayons également de déterminer si la cause de l'incident est interne à la commune (I) ou externe (E). Ce tableau d'analyse s'inspire de l'annexe C de la norme ISO 27005:2018 [20]. Les causes identifiées sont issues de diverses sources [40] [41] [42] [25] [43], [44].

Type	Causes	Origine
Vol de données	Collaborateur mal intentionné/ Whistleblower	DI
	Phishing / Whaling	DE
	Ransomware	DE
	Faiblesse des mots de passe et absence d'authentification à deux facteurs	PI
	Vulnérabilité du logiciel	AI
	Vol de matériel	DE
	Données non-cryptées	PI
	Fournisseur de services compromis	DE
Perte de données	Erreur d'un collaborateur	AI
	Collaborateur mal intentionné	DI
	Défaillance technique (panne)	AI
	Ransomware	DE
	Bug logiciel	AI
Divulgation involontaire de données	Erreur d'un collaborateur	AI
	Erreur de paramétrage logiciel	AI
	Erreur dans la gestion des accès	AI
	Perte de matériel non-crypté	AI
	Règles internes pas claires / Pas appliquées	PI
Détournement d'infrastructures publiques	Faiblesse des points d'accès aux infrastructures publiques – Mots de passes faibles / Absence d'authentification à deux facteurs	PI
	Fournisseur de services mal protégé (IOT)	PE
	Malware	DE
	Absence de contrôle interne d'utilisation des ressources CPU/GPU.	PI
Attaque DDOS	Choix d'un prestataire d'hébergement mal préparé	PI
	Site/services obsolètes (pas mis à jour) et peu sécurisés	PI
Fraude	Faiblesse des mots de passe et absence d'authentification à deux facteurs	PI
	Phishing	DE
Erreur IT/Zero Day Exploit	Logiciels obsolètes (pas mis à jour)	PI
	Choix de prestataires mal préparé (Due Diligence)	PI
	Absence de test de vulnérabilité	PI
	Phishing	DE

Cryptage des données et extorsion :	Absence de sauvegardes	PI
	Pas de procédure standard pour le cas	PI

Figure 28 - Analyse des causes d'incidents

Ci-dessous nous allons tenter d'analyser quels types d'acteurs sont susceptibles d'avoir un intérêt à causer des incidents de cybersécurité. Comprendre qui se tient derrière une attaque permet de comprendre quelles sont leurs motivations et comment se préparer au mieux.

Origine	Motivation	Conséquence
Organisations criminelles	Attaque en nom propre	Extorsion
	Hacking As A Service	Vol de données
	Argent	Perturbations
		Cryptojacking
Hacker isolé	Argent	Perturbations
	Prestige	Vol de données
	Défi	Cryptojacking
	Vengeance	
Hacktivistes	Politique	Perturbation – Diffusion de messages politiques
		Déstabilisation politique
		Vol de données / Whistleblowing
Acteurs étatiques	Informations stratégiques	Perturbation des services à la population / Militaire
	Avantage militaire	Vol de données confidentielles
	Espionnage	Vol de propriété intellectuelle / secrets de fabrication
		Destruction
	Argent	Renseignement militaire
		Déstabilisation politique
		Extorsion
Employé	Erreur	Accès à des informations confidentielles
	Vengeance	Destruction de données / perturbation des services
	Corruption (Argent)	Vol de données (Espionnage industriel)
	Curiosité	Whistleblowing
	Politique	
Terroristes	Récolte d'informations	Récolte d'informations dans la préparation d'un attentat
	Politique	Diffusion de messages politiques / menaces
	Perturbation	Perturbation des services de secours / Militaires
	Argent	Extorsion

Figure 29 - Analyse des origines d'attaques

Sur la base de cette analyse de risques nous allons pouvoir établir un profil cible selon les recommandations de l'Annexe A de la norme ISO 27001:2013 [18] et de la liste des mesures de la norme NIST [17].

6.2 Recommandations - mesures de protection

Sur la base de notre analyse de risques, nous allons procéder à des recommandations ciblées sur les risques les plus importants que nous avons identifiés dans la matrice de Mehari. Nous allons détailler les mesures que les communes peuvent prendre afin de trouver les ressources clés, protéger les systèmes d'informations, détecter les incidents, réagir et restaurer. Nous nous référons aux normes NIST[9] comme source pour ces recommandations. Cette norme est également la source des recommandations de la norme Minimale TIC mise en place par la Confédération[10]. Dans les recommandations suivantes, nous proposons des mesures simples, permettant aux responsables communaux de se protéger face aux risques identifiés.

La cybersécurité n'est pas une chose qui s'improvise. Il est recommandé de faire appel à un prestataire spécialisé qui mènera un audit spécifique de l'état de maturité de la commune en matière de cybersécurité et pourra établir avec les responsables communaux une liste personnalisée de mesures à prendre. Toutefois, ce type d'audit n'est pas gratuit, c'est pourquoi nous proposons une liste de mesures qui peuvent être utiles aux responsables de communes pour améliorer leur niveau de sécurité rapidement.

Voici tout d'abord quelques recommandations générales, qui sont importantes indépendamment du type d'attaque.

1. **Détermination des responsabilités – Qui fait quoi ? :** un point central dans la gestion des systèmes d'information et de la cybersécurité est de nommer une ou plusieurs personnes responsables de la thématique. Notre étude a démontré que, en 2022, toutes les communes du canton de Vaud ne disposent pas d'une personne désignée pour les questions en lien avec l'informatique.

   Il est important qu'au sein de l'administration communale, et plus largement chez le prestataire externe, il y ait une formalisation des rôles afin que chaque intervenant sache quel est son rôle, que ce soit pour prévenir un incident ou pour savoir à qui s'adresser en cas de problème. Déterminer les rôles permet également de s'assurer qu'au moins une personne soit officiellement reconnue responsable, qu'elle puisse recevoir une formation adéquate et qu'elle doive rendre des comptes concernant l'avancement des projets de développement des systèmes d'information et de leur sécurisation.

   Nous recommandons ainsi que dans les communes vaudoises, une personne soit nommée responsable et que cette information soit publiée et mise à la disposition de l'ensemble des parties prenantes afin de s'assurer de la transparence et la clarté des responsabilités au sein de l'administration communale.

   Se référer aux sous-catégories NIST ID.AM-6, ID,GV-2

[9] https://doi.org/10.6028/NIST.CSWP.04162018fr

[10] https://www.bwl.admin.ch/dam/bwl/fr/dokumente/themen/ikt/broschuere_minimalstandard.pdf.download.pdf/IKT_FR_2018_Web.pdf

2. **Créer un budget dédié à l'informatique :** la création d'un budget dédié à l'informatique dans le cadre de l'administration communale aura pour effet que cette thématique sera gérée de manière active et sera abordée au niveau de la municipalité comme une thématique d'importance stratégique.

3. **Définition des processus clés :** la première étape dans l'établissement d'une stratégie de cybersécurité consiste à définir quels sont les processus qui doivent être protégés en priorité. Comme nous l'avons vu, les communes ont des budgets limités, c'est pourquoi il est primordial d'effectuer cette sélection des priorités stratégiques. Comme chaque commune a ses propres particularités, cette détermination doit se faire au niveau communal.

   Le rôle des municipaux est ainsi de sélectionner les processus et les services qu'ils estiment essentiels au bon fonctionnement de la commune, et ceux qui représentent un risque moindre et ne nécessitant pas d'actions immédiates. Pour notre étude, nous avons choisi les services essentiels à la population (contrôle des habitants, gestion des déchets, hôpitaux, sécurité publique, police, pompiers, eau, gaz et électricité) ainsi que les données personnelles des personnes morales et physiques résidant dans la commune. Pour réaliser cette analyse, nous préconisons d'étudier les points pour chaque processus :

   - Qui est impacté par l'incident de cybersécurité ?
   - Quel impact a l'incident sur ces parties prenantes ?
   - Quel impact a l'incident sur les finances de la commune ?
   - Quel impact a l'incident sur l'image de la commune ?

   Une fois les priorités établies, les responsables communaux, en collaboration avec leurs prestataires externes, peuvent commencer la planification des mesures à prendre pour sécuriser les systèmes d'information de la commune.

4. **Cartographie des systèmes d'information – connais-toi toi-même :** la deuxième étape du processus de sécurisation des systèmes d'information consiste à réaliser une cartographie générale des systèmes d'information. Cela comprend entre autres :

   - Un inventaire des données que la commune possède sur ses serveurs et sur ceux de ses prestataires externes.
   - Un inventaire du matériel physique (hardware) de la commune.
   - Un inventaire des prestataires avec lesquels la commune travaille.
   - Un inventaire des applications et licences qu'elle utilise dans la réalisation de ses activités.
   - Une liste des flux de données à l'intérieur de la commune et avec ses prestataires externes.

   Grâce à cette cartographie des systèmes d'information, la commune sera en mesure d'avoir une vue d'ensemble de son système d'information et de prioriser les données et les processus qu'elle souhaite protéger. Cela lui permet d'identifier les vulnérabilités potentielles et facilite la restauration des systèmes en cas d'incidents. Elle sera aussi en mesure de détecter plus aisément les problèmes potentiels lorsqu'ils surviennent.

Grâce à cette cartographie, elle sera également à même d'identifier les ressources qui sont les plus importantes de protéger dans le cadre de son plan de gestion des risques.

Se référer aux sous-catégories NIST ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5

5. **Gestion des risques :** les communes doivent intégrer les risques en lien avec la cybersécurité dans leur politique de gestion des risques. Dans notre étude, nous avons découvert que seulement 58,33 % des communes interrogées procèdent à une telle analyse. Comme chaque commune a ses propres particularités avec un système d'information qui lui est unique et potentiellement son propre système de gestion des risques, nous recommandons de réaliser cette analyse afin d'avoir une vision des impacts financiers ou d'image résultant de divers types d'évènements.

   Se référer aux sous-catégories NIST ID.GV-4

6. **Gestion des relations avec les prestataires de service :** comme nous l'a démontré notre étude, les communes vaudoises font dans la grande majorité appel à des prestataires externes pour leurs services informatiques. Il n'existe aujourd'hui pas de normes contractuelles standardisées.

   Nous recommandons que les communes procèdent à l'établissement d'une liste des fournisseurs de services informatiques avec lesquels elles travaillent. Ce listing leur permet de s'assurer que l'ensemble de leur chaîne de valeur numérique est sous contrôle et respecte des exigences similaires dans leur prestations.

   Nous recommandons que, soit au niveau du canton soit au niveau des associations de communes, soit créée une forme de standardisation des exigences en termes de cybersécurité que les communes puissent inclure dans leurs contrats avec leurs prestataires de services respectifs. Il existe déjà un modèle de conditions générales pour les prestations TIC publié par la conférence suisse[11] sur l'informatique, disponible sur le site administration-numérique-suisse.ch. Nous recommandons la création d'un modèle similaire avec les exigences standards en matière de cybersécurité devant être mises en place par les prestataires.

   Se référer aux sous-catégories NIST ID.SC-2 ID.SC-3, ID.SC-5

7. **Information sur les menaces :** la personne en charge de l'informatique, conjointement avec son/ses prestataires externes se tient informée des menaces actuelles. Le canton de Vaud a mis en place une newsletter[12] mensuelle disponible sur une plateforme en ligne informant des vulnérabilités et évènements qu'il estime d'importance. Nous recommandons que les responsables informatiques restent informés des dernières actualités.

   Se référer aux sous-catégories NIST ID.RA-2

8. **Garder des traces :** un point central dans la cybersécurité est la détection de comportements sortant de l'ordinaire sur les réseaux. Afin de faciliter cette détection, nous recommandons que toutes les transactions effectuées sur les systèmes d'information de la commune soient enregistrées dans des fichiers de journalisation (logs). Ces derniers, couplés à des algorithmes de Machine Learning, pourront aider à détecter ces

[11] https://www.administration-numerique-suisse.ch/fr/mise-en-oeuvre/programme-de-travail-TIC-CSI/conditions-generales-pour-les-prestations-TIC (Consulté le 09.08.2022)
[12] https://www.vd.ch/fileadmin/user_upload/organisation/dinf/dsi/ussi/vd_secure/ (Consulté le 08.08.2022)

comportements sortant de l'ordinaire. Nous vous recommandons d'en parler à votre prestataire dans le cadre des mesures de détections des anomalies.

Ces journaux ont également l'avantage de pouvoir être utilisés pour comprendre les causes d'un incident et d'en retrouver la source.

9. **Réaliser des tests :** un bon moyen pour tester l'efficacité des mesures de cybersécurité consiste à réaliser régulièrement des tests. Ces derniers pourront être la base pour identifier les manquements, les vulnérabilités non identifiées et les collaborateurs ou élus nécessitant une meilleure sensibilisation.

6.2.1 Vol de données

Afin de prévenir les vols de données, voici quelques mesures qui peuvent être mises en place :

1. **Identification des niveaux de confidentialité :** pour les différentes données stockées sur les serveurs de la commune. La norme ISO 27002 :2013 [19] propose 4 niveaux de confidentialité :
    a. « La divulgation ne cause aucun préjudice .»
    b. « La divulgation cause une gêne mineure ou un léger désagrément de fonctionnement .»
    c. « La divulgation a, sur le court terme, des répercussions importantes sur les opérations ou les objectifs tactiques .»
    d. « La divulgation a, sur le long terme, des répercussions graves sur les objectifs stratégiques ou compromet la pérennité de l'organisation. »

    La Confédération, dans l'ordonnance du 4 juillet 2007 concernant la protection des informations, identifie 3 échelons de classification [45] :

    - Public
    - Interne
    - Confidentiel
    - Secret

    Comme les communes ont toutes sensiblement les mêmes données sur leurs serveurs du fait de leurs activités similaires, il serait intéressant de mettre en place une identification du niveau de confidentialité centralisée à l'échelle du canton ou de l'UCV ainsi que les mesures de protection organisationnelles et techniques qui leur sont attribuées.

    Se référer aux sous-catégories NIST ID.AM-5

2. **Formation des collaborateurs et des élus :** la plus grande vulnérabilité dans un système d'information reste souvent l'utilisateur qui tombe dans un piège que lui ont tendu des individus ou organisations malveillants. Il est ainsi central que les gens soient mis au courant régulièrement de différents types d'attaques et de procédés afin qu'ils puissent les identifier et éviter de se faire piéger (phishing, arnaque au faux patron, etc.). Les collaborateurs peuvent également manquer de connaissances concernant la génération de

mots de passe et sur les procédures de sécurisation des différents types de données (chiffrement, gestion des secrets, etc.).

Dans le contexte des communes, il serait intéressant de mettre en place au niveau du canton ou de l'Union des Communes Vaudoises un module de formation centralisé, ceci afin de s'assurer que tous les collaborateurs et élus disposent d'une formation standardisée d'une qualité jugée suffisante.

Ces mesures permettent de prévenir :

- Tentatives de phishing/Whaling
- Fraudes
- Faiblesse des mots de passe

Se référer aux sous-catégories NIST PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5

3. **Principe du Need-to-Know :** une fois les différentes données classifiées selon leur degré de confidentialité, il est important de mettre en place une politique d'accès à l'information selon le principe du « Need-to-Know ». Andrew Wolter, senior program manager chez Microsoft, décrit ce principe comme suit (traduit de l'anglais) [46]: « un utilisateur n'a accès qu'aux informations que sa fonction requiert, indépendamment de son niveau d'habilitation de sécurité ou d'autres approbations. ». Ce principe s'applique également aux applications qu'exploite la commune qui doivent avoir accès uniquement aux données nécessaires à leur bon fonctionnement et à rien d'autre.

   Ce principe permet de prévenir un certain nombre de vols de données de la manière suivante :

   - En cas de tentative de phishing réussie, l'attaquant n'aura accès qu'à une partie limitée des données de la commune.
   - En cas d'application piratée, l'attaquant aura accès uniquement aux données nécessaires à cette dernière.
   - Un collaborateur mal intentionné ne pourra voler que les données auxquelles il a accès.

   Se référer aux sous-catégories NIST PR.AC-4

4. **Utilisation de gestionnaires de mots de passe / identification à deux facteurs :** l'une des failles les plus importantes dans la cybersécurité concerne l'authentification des utilisateurs des services en ligne. Malheureusement, il n'est pas rare que certains utilisateurs se servent du même mot de passe dans différentes situations (personnelles et professionnelles). De plus, la mémorisation de mots de passe sécurisés avec chiffres, lettres (avec majuscules et minuscules) et caractères spéciaux devient un exercice complexe dans la mesure où ils sont nécessaires pour chaque service en ligne.

   C'est pourquoi, nous recommandons dans le cadre des administrations communales l'utilisation de gestionnaires de mots de passe. Ces derniers offrent les avantages suivants :

   - Génération de mots de passe forts automatique.
   - Un seul mot de passe complexe à retenir pour les utilisateurs (mot de passe maître).

Il est important que les collaborateurs soient informés de la nécessité de créer un mot de passe maître fort, et qu'ils reçoivent des conseils pour le générer.

Un second niveau de sécurité qu'il est nécessaire d'ajouter concerne l'identification à deux facteurs qui requiert l'utilisation de deux formes d'identification distinctes pour accéder à un service en ligne. Dans la plupart des cas, un utilisateur devra inscrire son nom d'utilisateur et son mot de passe et confirmer sa connexion à l'aide d'un SMS reçu sur son téléphone portable ou l'utilisation d'une application d'authentification telle que Microsoft Authenticator ou SwissID. Cette méthode d'authentification permet de rendre plus complexes les tentatives de phishing car la seconde méthode d'identification est aléatoire et dépend de l'utilisateur.

Ces mesures permettent de prévenir :

- Les attaques de type force brute
- Les attaques de phishing

Nous pensons également de mentionner qu'un nouveau type de plateforme commence à devenir de plus en plus populaires, les logiciels SSO (Single Sign On) permettant d'assurer une connexion sécurisée pour accéder à plusieurs types systèmes et applications. Avec cet outil, les collaborateurs se connectent à une seule plateforme sécurisée pour avoir accès aux logiciels et données dont ils ont besoin pour leur travail.

Se référer aux sous-catégories NIST PR.AC-1

5. **Chiffrement des données :** les données classées comme confidentielles dans la commune doivent être chiffrées sur les supports physiques de l'entreprise et chez ses prestataires externes. Qu'il s'agisse d'un ordinateur portable, d'un serveur ou d'un support externe de stockage de données, ces dernières doivent faire l'objet d'un chiffrement afin de n'être pas lisibles par tout le monde.

   Ce chiffrement permet d'éviter que, dans le cas d'un vol de matériel, la personne ou l'organisation mal intentionnée puisse avoir accès aux données stockées sur le support physique.

   Afin de gérer au mieux cette mesure, il est nécessaire que la commune mette en place avec son prestataire des procédures de gestion des clés cryptographiques (permettant de chiffrer et déchiffrer les données) afin que ces dernières soient uniquement accessibles aux personnes qui en ont l'autorisation du fait de leur fonction.

   Se référer aux sous-catégories NIST PR.DS-5

6. **Mises à jour, logiciels anti-virus, anti-spam et filtre DNS :** les communes sont susceptibles d'être victimes de virus et malwares. Les développeurs d'applications découvrent régulièrement des failles de sécurité et mettent à disposition des utilisateurs des patchs de correction. C'est pourquoi il est important pour les communes de mettre régulièrement à jour leurs logiciels et systèmes d'exploitation afin de s'assurer une protection optimale contre tout type d'attaque. L'investissement dans un logiciel anti-virus est également fortement recommandé.

   L'utilisation d'un filtre anti-spam moderne permet de limiter le nombre d'emails de phishing ou contenant des virus parvenant aux collaborateurs d'une entreprise. Nous recommandons l'utilisation d'un tel dispositif.

Un employé peut aisément être trompé et cliquer par erreur sur un lien le menant vers une page web infectée par des malwares. Il existe des logiciels qui mettent en place des filtres limitant les sites internet que les employés sont habilités à visiter. Nous recommandons ainsi l'utilisation de ce type de filtres qui ajoutent une protection supplémentaire afin de se prémunir d'une attaque de ransomware.

Ces recommandations permettent à la commune de se prémunir au mieux contre les divers malwares tels que les ransomwares qui sont très problématiques. Elles permettent également de se prémunir des attaques Zero-day et des vulnérabilités logicielles.

Se référer aux sous-catégories NIST PR.MA-1

7. **Pseudonymisation des données :** comme un vol de données reste une grande probabilité malgré les différents niveaux de protection, nous proposons de mettre en place des mesures réduisant l'impact de tels incidents. Afin de réduire l'impact des vols de données, il existe des méthodes permettant de rendre plus compliquée l'identification des propriétaires de données, ce qui a pour effet de réduire grandement la valeur des données pour un attaquant potentiel.

   Le CNIL définit le procédé comme suit [47] : « La pseudonymisation est un traitement de données personnelles réalisé de manière qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire. En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.) »

   Nous recommandons ainsi que dans le cadre de la gestion des données au sein des administrations publiques du canton de Vaud, un modèle de pseudonymisation des données soit mis en place. Un modèle de ce type existe aujourd'hui dans le cadre de la gestion des dossiers électroniques des patients.

8. **Sécurisation du réseau :** le télétravail se développant de plus en plus depuis la crise Covid, et les communes faisant de plus en plus usage de services cloud, il est primordial que ces dernières adoptent des bonnes pratiques quant à la sécurisation des accès à leurs réseaux depuis l'extérieur. Voici quelques mesures qui peuvent être mises en place pour réaliser cette sécurisation :

   - Utilisation d'un VPN pour les collaborateurs souhaitant se connecter au réseau depuis l'extérieur.
   - L'utilisation de services cloud ayant mis en place des mesures techniques de chiffrement côté client. Grâce à cette méthode, les données sont déjà chiffrées chez le client avant même l'envoi sur le serveur cloud.
   - Etudier l'opportunité de la mise en place d'une architecture de réseau selon le principe « Zero-Trust » en collaboration avec les prestataires informatiques.

6.2.2 Perte de données

1. **Limitation des droits des utilisateurs (CRUD) :** comme vu précédemment dans la recommandation du Need-To-Know, les collaborateurs de la commune ainsi que les applications doivent avoir un accès restreint aux données. Ces restrictions doivent

également se porter sur leur capacité à créer, modifier et supprimer les données. La municipalité doit établir une cartographie CRUD (Qui dans la commune a le droit de créer, lire, modifier et supprimer les données, s'applique également aux applications) pour tous les processus et limiter au maximum la possibilité qu'auraient les collaborateurs ou les applications de modifier ou supprimer des données par erreur.

Cette mesure permet de prévenir les causes de pertes de données suivantes :

- Erreur d'un collaborateur
- Collaborateur mal intentionné

Se référer aux sous-catégories NIST PR.AC-4

2. **Procédure de sauvegardes des données – collaborateurs et élus :** il peut arriver que, dans les entreprises ou les communes, des collaborateurs stockent des données sur leur poste de travail. Les données sont ainsi non accessibles pour le reste de l'organisation. Il est donc important de sensibiliser les collaborateurs et les élus à l'importance de stocker leurs données professionnelles sur le serveur partagé dans leurs activités afin d'éviter qu'en cas d'absence du collaborateur, de défaillance ou de vol du poste de travail, les données enregistrées localement soient perdues.

   Cette mesure permet de prévenir les causes de pertes de données suivantes :

   - Défaillance technique
   - Erreur d'un collaborateur

   Se référer aux sous-catégories NIST PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5

3. **Sauvegardes et tests de restauration :** une bonne pratique permettant d'éviter une perte trop importante de données comprend la réalisation régulière de sauvegardes de données. La régularité de ces sauvegardes doit être définie par la municipalité et être comprise comme l'évaluation de l'impact de la perte des données ajoutées, modifiées ou supprimées entre chaque sauvegarde. Il est conseillé de réaliser plusieurs copies d'une même sauvegarde réparties sur plusieurs localisations géographiques pour les données nécessitant une protection particulière.

   Il est également recommandé de réaliser régulièrement des tests de restauration des données afin qu'en cas de problème, les systèmes d'information puissent être remis en service le plus rapidement possible.

   Dans la mesure où les communes font appel à des prestataires externes, qu'elles traitent sensiblement les mêmes types de données et utilisent des processus similaires, nous proposons de centraliser les conditions de sauvegardes au niveau des associations de communes ou du canton. Cela permettrait aux communes de se présenter devant leurs prestataires de services avec des conditions standards, assurant ainsi un niveau de qualité similaire dans tout le canton.

   Cette mesure permet de prévenir les causes de pertes de données suivantes :

   - Erreur d'un collaborateur
   - Collaborateur mal intentionné
   - Ransomware

- Défaillance technique

Se référer aux sous-catégories NIST PR.IP-4

6.2.3 Chiffrement des données (Ransomware)

Le NIST a publié un rapport en février 2022 présentant un modèle de profil spécifiquement dirigé pour la prévention et la réaction face aux attaques de Ransomware[13] [48]. Ce document donne une liste extrêmement exhaustive de mesures techniques et organisationnelles que les entreprises et les administrations publiques peuvent mettre en place pour se protéger face à cette menace.

1. **Procédure de réaction et travail en mode dégradé :** lorsqu'une commune se retrouve face à une situation de chiffrement des données due à un ransomware, il est important qu'elle s'y soit préparée à l'avance afin de ne pas se retrouver prise par surprise. Notre sondage a montré que peu de communes ont mis en place des procédures standards opérationnelles leur permettant de réagir rapidement.

   C'est pourquoi, nous recommandons la mise en place de procédures standardisées au niveau des associations de communes ou du canton auxquelles les responsables peuvent se référer en cas d'incident. Les responsables informatiques communaux doivent être mis au courant de ces procédures.

   Nous recommandons également que les communes étudient la mise en place de procédures afin de pouvoir travailler en mode dégradé le temps du rétablissement des infrastructures informatiques afin de pouvoir répondre quand même aux besoins de la population.

   Cette mesure permet de prévenir les effets suivants :

   - Réaction inadaptée lors d'un incident
   - Interruption des services à la population

   Se référer aux sous-catégories NIST ID.GV-1, PR.IP-9, PR.IP-10

2. **Mises à jour et logiciels anti-virus :** cette recommandation a déjà été mentionnée dans la partie sur les vols de données, qui vont souvent de pair avec les ransomwares. Il est toutefois nécessaire de rappeler l'importance de maintenir les logiciels et les infrastructures à jour et d'investir dans des logiciels anti-virus qui permettront d'éviter, de détecter ou du moins de réduire l'impact d'une attaque de type ransomware.

   Cette mesure permet de prévenir les effets suivants : Attaque de ransomware

3. **Sauvegardes et tests de restauration :** se référer au point 5.2.2.3

4. **Mise en place de filtres DNS :** un employé peut aisément être trompé et cliquer par erreur sur un lien le menant vers une page web infectée par des malwares. Il existe des logiciels qui mettent en place des filtres limitant les sites internet que les employés sont habilités à visiter. Nous recommandons ainsi l'utilisation de ce type de filtres qui ajoutent une protection supplémentaire afin de se prémunir d'une attaque de ransomware.

[13] https://doi.org/10.6028/NIST.IR.8374 (Consulté le 13.08.2022)

6.2.4 Fraude

1. **Sécurisation des accès aux boites mails :** comme expliqué plus haut, les attaques de phishing deviennent de plus en plus sophistiquées. En obtenant accès à une/des boîtes mails, des arnaqueurs étudient les relations qu'entretient la commune avec ses fournisseurs. Ils peuvent ainsi par exemple intercepter une facture légitime d'un fournisseur et transmettre de fausses coordonnées bancaires afin de voler de l'argent. C'est pourquoi il est primordial pour les communes de mettre en place des mesures de protection de leurs boites mails afin de limiter ce type d'incident.

   Pour sécuriser une boite mail, il existe plusieurs solutions que nous détaillons ci-dessous :

   1. Utilisation de mots de passe complexes et de gestionnaires de mots de passe.
   2. Authentification à deux facteurs.
   3. Détection et notification des connections suspectes (localisation géographique, nouvel appareil, etc.) par SMS ou sur une adresse tierce.

2. **Sensibilisation des employés :** les employés doivent être sensibilisés aux cybercrimes tels que les arnaques et les fraudes. Par exemple, ils doivent être particulièrement attentifs à l'adresse de provenance d'un email ou encore demander confirmation si les coordonnées de paiement d'un fournisseur semblent étranges (paiement à l'étranger par exemple).

3. **Utilisation de moyens sécurisés pour la transmission des factures :** Afin d'augmenter la sécurité des communications avec les fournisseurs, nous recommandons d'utiliser des solutions de facture sécurisée tel que le service ebill. Plus compliqué mais également envisageable, il serait intéressant d'étudier la mise en place de signatures électroniques pour sécuriser l'intégrité des emails.

6.2.5 Détournement des infrastructures publiques

1. **Sélection de prestataires crédibles pour les installations d'objets connectés:** la première étape dans la sécurisation des infrastructures publiques consiste à s'assurer que le fournisseur d'objets connectés (caméras de surveillances, infrastructures connectées) dispose des compétences techniques et organisationnelles suffisantes pour fournir un produit répondant à un haut niveau de sécurité. Nous recommandons une étude approfondie et un audit régulier de la capacité des prestataires à répondre aux exigences en matière de cybersécurité.

   Nous incluons cette recommandation dans cette partie, car les objets connectés sont un cas particulier qu'il est nécessaire de prendre en compte. Les fournisseurs de ces objets ne sont pas nécessairement des experts dans les technologies de l'information, c'est pourquoi il est nécessaire de s'assurer qu'ils sont en mesure d'assurer un niveau de protection suffisant. Il est ainsi nécessaire d'inclure dans les contrats de maintenance que les objets connectés doivent régulièrement être mis à jour par le prestataire afin que les vulnérabilités identifiées soient patchées.

2. **Sécurisation des points d'accès aux objets connectés :** les objets connectés exploités par les communes doivent faire l'objet d'une sécurisation des points d'accès. Ainsi les mots de passe standards configurés lors de l'installation de ces objets doivent impérativement être

modifiés afin de présenter un niveau de complexité suffisant. L'utilisation de gestionnaires de mots de passe ainsi que l'authentification à deux facteurs sont recommandées.

3. **Contrôle d'utilisation des ressources :** comme expliqué précédemment, de plus en plus d'attaquants cherchent à exploiter les ressources en CPU/GPU des entreprises et des administrations publiques afin de miner des cryptomonnaies. Il est ainsi nécessaire d'investir dans des solutions de contrôle d'utilisation des ressources, en partenariat avec son/ses prestataires informatiques afin de s'assurer que ces dernières sont effectivement utilisées pour l'objectif qui leur est donné.

6.2.6 Attaque DDOS

1. **Choix d'un prestataire crédible :** la première manière de se protéger face à une attaque de type DDOS est de faire appel à un prestataire d'hébergement crédible pour ses services en ligne (site internet, applications mobiles, etc.) ayant suffisamment de ressources et de connaissances pour faire face à ce type d'attaques. Nous recommandons de choisir un prestataire Suisse disposant de suffisamment de ressources. Ces prestataires sont en règle générale experts de ce type d'attaques et disposent de moyens techniques (Pare-feu applicatifs web par exemple) et organisationnels (surveillance 24h/24) pour y faire face.

2. **S'assurer que son site internet est à jour :** les sites internet et les applications doivent régulièrement être mis à jour afin de s'assurer qu'ils ne soient pas vulnérables à des attaques d'acteurs malveillants. Comme une attaque de type DDOS a pour effet de mettre à mal la disponibilité du site et de mobiliser beaucoup de ressources, elle fragilise par la même occasion les mesures de sécurité. C'est pourquoi il est nécessaire d'avoir un site qui soit mis à jour régulièrement.

3. **Utilisation du Pare-feu d'application Web :** si votre commune gère en interne son site internet, une application web ou une API, l'utilisation d'un Pare-feu d'application Web est recommandé afin de se prémunir d'une attaque DDOS impactant cette ressource. Le Pare-Feu bloquera les requêtes identifiées comme frauduleuse et préservera votre serveur.

6.3 Recommandations – Collaborations

Une thématique que notre étude a plusieurs fois mentionnée concerne le manque de communication et de collaboration entre les différents acteurs, qu'ils se trouvent au niveau des communes, du canton ou des faitières de communes. Les responsables de communes se retrouvent parfois bien seuls pour prendre en charge les questions en relation avec l'informatique et la cybersécurité. Voici ainsi nos recommandations et idées concernant les collaborations qui pourraient être mises en place afin de renforcer le niveau global de la cybersécurité des communes.

- **Modules de formations pour les élus et des collaborateurs :** nous proposons qu'en début de législature, les nouveaux élus au poste de responsable communal de l'informatique soient invités proactivement à participer à une formation leur permettant d'acquérir les connaissances nécessaires à la bonne conduite de leur dicastère. Cette formation peut prendre plusieurs formes, soit au travers d'une plateforme de E-learning, soit en présentiel. Les collaborateurs des communes doivent également être régulièrement formés aux différents types d'attaques qu'ils sont susceptibles de rencontrer dans leur travail.

- **Création de groupes d'intérêts :** nous proposons de créer sous l'égide des associations faitières de communes des groupes d'intérêts se réunissant régulièrement, afin que les responsables communaux pour un même dicastère puissent se rencontrer et discuter des problématiques qui les concernent. L'objectif ici est que les élus élargissent leur réseau de connaissances et puissent collaborer sur des thématiques et problématiques similaires. Il serait potentiellement intéressant de créer une plateforme en ligne permettant une collaboration plus directe, sur le modèle d'un forum, permettant aux élus d'interagir entre eux pour poser des questions ou simplement pour partager des idées ou des documents.

- **Création d'une bibliothèque documentaire :** lors de nos discussions avec les élus, l'un des principaux freins à la mise en place de mesures de cybersécurité concerne la charge importante de travail administratif que représente le fait de créer des règlements internes et diverses documentations nécessaires à la mise en place d'une cybersécurité crédible. Comme les communes ont des activités similaires les unes aux autres, nous recommandons la création d'une bibliothèque documentaire afin que les élus disposent de documents et procédures standardisés (par exemple : charte informatique, niveau de classification de confidentialité des données, conditions générales pour un prestataire informatique ou procédure de réaction en cas d'incident) qu'ils puissent appliquer sans trop de modifications dans leur propre administration.

- **Création d'exigences standardisées pour les prestataires informatiques :** comme nous l'avons vu dans notre étude, les communes font toutes appel à des prestataires externes pour la gestion de leurs infrastructures informatiques. Aujourd'hui, chaque commune conclut ses contrats selon les conditions qu'elle a négociées elle-même avec ses prestataires. Nous proposons de mettre à la disposition des communes une liste d'exigences standardisées pour les mesures de cybersécurité et les standards que le prestaire doit pouvoir mettre en place dans le cadre de son travail avec la commune. Il serait par exemple également question du niveau de service, à savoir la disponibilité du prestataire pour réagir en cas d'incident.

- **Fond cantonal de soutien aux communes pour la cybersécurité :** nous proposons que le canton envisage la création d'un fond a destination des communes pour encourager les mesures en lien avec la cybersécurité. Ce que l'un des conseiller municipaux que nous avons interrogé propose est par exemple une participation de la part du canton aux coûts liés à la réalisation d'un audit de cybersécurité par un prestataire indépendant.

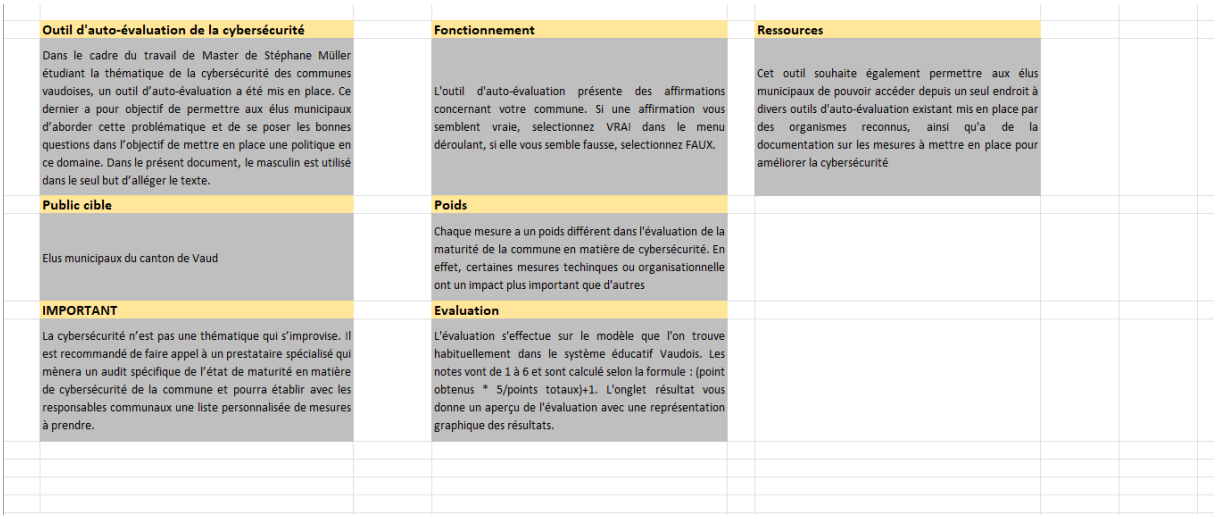
7 Création d'un outil d'auto-évaluation

Comme expliqué précédemment dans les recommandations, la mise en place de mesures de cybersécurité nécessite la participation de professionnels spécialisées dans le domaine. C'est pourquoi l'outil que nous avons mis en place à la suite de cette étude se place à un haut niveau, avec une faible complexité afin qu'il puisse être accessible à un public le plus large possible, notamment à un public de non-initiés. Cet outil a un objectif : permettre aux responsables politiques de commencer à aborder cette thématique et de se poser les bonnes questions pour mettre en place une politique crédible de cybersécurité. Il ne veut pas et ne peut pas se substituer à un audit effectué par un prestataire indépendant professionnel dans le domaine.

Cet outil reprend les recommandations que nous avons émises dans la précédente partie et permet sur un seul document de trouver les meilleures ressources identifiées dans ce rapport actuellement disponibles sur différents sites et plateformes de références.

7.1 Page de garde

Sur la page de garde, les municipaux trouvent les informations générales en lien avec le questionnaire et son fonctionnement.



Outil d'auto-évaluation de la cybersécurité	Fonctionnement	Ressources
Dans le cadre du travail de Master de Stéphane Müller étudiant la thématique de la cybersécurité des communes vaudoises, un outil d'auto-évaluation a été mis en place. Ce dernier a pour objectif de permettre aux élus municipaux d'aborder cette problématique et de se poser les bonnes questions dans l'objectif de mettre en place une politique en ce domaine. Dans le présent document, le masculin est utilisé dans le seul but d'alléger le texte.	L'outil d'auto-évaluation présente des affirmations concernant votre commune. Si une affirmation vous semblent vraie, selectionnez VRAI dans le menu déroulant, si elle vous semble fausse, selectionnez FAUX.	Cet outil souhaite également permettre aux élus municipaux de pouvoir accéder depuis un seul endroit à divers outils d'auto-évaluation existant mis en place par des organismes reconnus, ainsi qu'a de la documentation sur les mesures à mettre en place pour améliorer la cybersécurité
Public cible	**Poids**	
Elus municipaux du canton de Vaud	Chaque mesure a un poids différent dans l'évaluation de la maturité de la commune en matière de cybersécurité. En effet, certaines mesures techinques ou organisationnelle ont un impact plus important que d'autres	
IMPORTANT	**Evaluation**	
La cybersécurité n'est pas une thématique qui s'improvise. Il est recommandé de faire appel à un prestataire spécialisé qui mènera un audit spécifique de l'état de maturité en matière de cybersécurité de la commune et pourra établir avec les responsables communaux une liste personnalisée de mesures à prendre.	L'évaluation s'effectue sur le modèle que l'on trouve habituellement dans le système éducatif Vaudois. Les notes vont de 1 à 6 et sont calculé selon la formule : (point obtenus * 5/points totaux)+1. L'onglet résultat vous donne un aperçu de l'évaluation avec une représentation graphique des résultats.	

Figure 30 - Outil d'auto-évaluation - page de garde

Cette page de garde donne le contexte de la création de l'outil et ses objectifs : permettre aux élus municipaux d'aborder la problématique de la cybersécurité et de se poser les bonnes questions dans l'objectif de mettre en place une politique dans ce domaine. Elle explique également le mode de fonctionnement du questionnaire. Ce dernier propose des affirmations auxquelles la commune est invitée à répondre par Vrai ou Faux. Par exemple, la première affirmation est : « Votre commune a désigné une personne responsable de l'informatique. ». Pour chaque affirmation, nous avons déterminé une pondération différente, en fonction notamment de l'impact immédiat qu'ont les différents types de mesures sur la cybersécurité des communes. Ainsi pour la question précitée, nous donnons une pondération de 4 car la désignation d'un responsable est centrale pour toute

organisation utilisant des outils numérique pour effectuer son travail et est d'autant plus importante lorsqu'elle souhaite mettre en place une stratégie et des mesures de sécurité informatique.

Un disclaimer est ajouté pour expliquer aux utilisateurs que cet outil ne peut se substituer à un audit effectué par un prestataire professionnel et que ce type d'audit est recommandé.

7.2 Questionnaire

Le questionnaire est disponible dans l'Annexe 3. Le questionnaire est divisé en 6 parties :

- Organisation
- Identifier
- Protéger
- Détecter
- Répondre
- Récupérer

Cinq de ces parties sont issues de la norme NIST. Nous avons décidé d'en ajouter une, la partie organisation, plus spécifique au contexte des communes vaudoises. Le questionnaire est composé de 52 questions sur ces différentes thématiques. Comme expliqué précédemment, chaque question a une pondération différente, en fonction de l'impact que la mise en place de celle-ci aura immédiatement sur la protection des données et les processus de la commune. Nous avons tenté de créer un outil abordant les thématiques principales de la cybersécurité tout en restant compréhensible pour un public de non-initié.

7.3 Résultat

Une fois que les communes ont rempli le questionnaire, elles peuvent se rendre sur la page résultat. Ces derniers sont exprimés de la façon suivante. Tout d'abord, un tableau indique aux responsables communaux le nombre de points totaux (somme des pondérations) qu'ils pourraient obtenir s'ils répondaient « VRAI » à toutes les questions. La seconde colonne présente les points obtenus (les pondérations pour lesquelles le répondant a répondu « Vrai » s'additionnent). Finalement, le tableau calcule une note sur le modèle du système éducatif vaudois, allant de 1 à 6 calculée selon la formule : (Points obtenus x 5 / Points totaux) + 1.

Thématique	Points Totaux	Points obtenu	Evaluation
Organisation	21	12	3,86
Identifier	35	20	3,86
Protéger	57	41	4,60
Détecter	16	11	4,44
Répondre	18	11	4,06
Rétablir	14	7	3,50

Figure 31 - Outil d'auto-évaluation - Résultat - Tableau

Nous avons également souhaité ajouter une représentation graphique pour permettre une visualisation plus aisée de la situation de la commune sur les différentes thématiques de la cybersécurité. Pour cela nous avons choisi de réaliser un graphique Radar. Cette dernière permet de visualiser quels sont les thématiques qui obtiennent la meilleure note et où la commune a encore besoin de travailler pour s'améliorer et ainsi obtenir un niveau de maturité plus élevé.

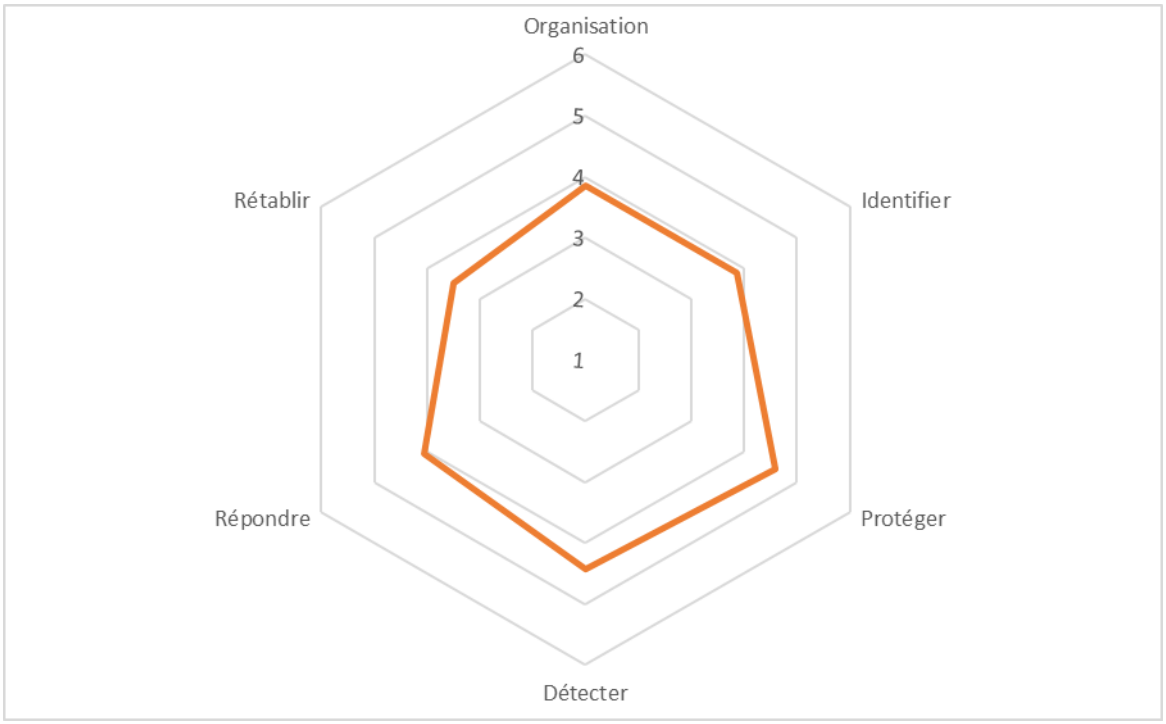


Figure 32 - Outil d'auto-évaluation - Résultats - graphique Radar

7.4 Ressources

Comme expliqué précédemment, notre outil d'auto-évaluation a pour objectif de permettre aux élus de se poser les bonnes questions et de commencer à aborder la thématique de la cybersécurité. Il ne peut pas et ne veut pas se substituer à un audit effectué par un professionnel. Lors de la réalisation de ce travail de master, nous avons découvert de nombreuses ressources qui sont actuellement disponibles gratuitement sur internet, mais qui ne sont pas forcément connues de tous. Ces ressources ont été créées par des professionnels chevronnés disposant d'années d'expériences dans la cybersécurité. C'est pourquoi nous avons décidé d'ajouter cette page, afin que les élus souhaitant traiter cette thématique aient plus de documentation et d'autres outils à leur disposition si tel est leur souhait d'approfondir leurs recherches.

Ressources
Cette section regroupe un ensemble de ressources librement disponibles en ligne qui vous permettront d'approfondir la thématique et permettront à votre commune d'effectuer diverses analyses pour évaluer votre maturité au niveau de la cybersécurité.

Documentation	Auteur	URL
Norme minimale sur les TIC	Confédération, Suisse	Lien
Prévenir les cybercrimes, guide à destination des communes	NEDIK / UCV	Lien
Conseil en cas de cyberattaques	Canton de Vaud / UCV	Lien
Aide-mémoire des premières mesures à prendre en cas d'attaque informatique	Cybersafe / UCV	Lien
Cadre pour l'amélioration de la cybersécurité des infrastructures critiques	NIST	Lien
Conditions générales pour les prestations TIC	Administration numérique, Suisse	Lien
Cybersécurité Vaud	Canton de Vaud	Lien
Si001 - Protection informatique de base dans l'administration fédérale	Confédération, Suisse	Lien
Ransomware Risk Management: A Cybersecurity Framework Profile (en anglais)	NIST	Lien
Outils d'auto-évaluation	**Auteur**	**URL**
Norme minimale sur les TIC - Outil d'auto-évaluation	Confédération, Suisse	Lien
Si001 - Hi01 - Mise en œuvre des mesures de protection informatique de base dans l'administration fédérale	Confédération, Suisse	Lien

Figure 33 - Outil d'auto-évaluation – Ressources

7.5 Conclusion

De nombreux outils existent actuellement en ligne pour réaliser une auto-évaluation de la cybersécurité. Le nôtre souhaite se placer à un haut niveau tout en présentant une moindre complexité afin de se présenter comme une porte d'entrée à la création d'une réflexion en lien avec la problématique de la cybersécurité. Nous espérons qu'il pourra servir aux élus municipaux du canton de Vaud et peut-être encore plus largement.

8 Conclusion

La problématique de la cybersécurité, en Suisse en général et dans le canton de Vaud en particulier, reste un sujet extrêmement important car les menaces qui planent sur les entreprises et les administrations publiques sont permanentes. L'annonce récente de la part des autorités Russes que la suisse était considérée comme un état hostile augmente encore ce risque. L'accroissement de la fréquence des attaques et l'augmentation de leur impact rendent nécessaire la mise en place de mesures de sécurité.

Pour les communes vaudoises, c'est un point essentiel dans le maintien de la confiance entre les institutions publiques et la population qui font le succès de notre système étatique suisse.

Ce travail de master a permis d'analyser comment les communes vaudoises gèrent la thématique de la cybersécurité. Dans notre introduction, nous partions de l'hypothèse que « la gestion des questions liées à l'informatique et à la cybersécurité diffère beaucoup entre ces dernières ». Cette hypothèse s'est révélée exacte

Notre première question de recherche aspirait à découvrir quels étaient les défis rencontrés par les communes dans la mise en place de mesures de cybersécurité crédibles et si la taille de la commune avait un impact. Voici ce que notre étude a permis de découvrir :

- Les difficultés budgétaires représentent un frein à la mise en place d'une stratégie crédible de cybersécurité. Les communes du canton de Vaud, dans leur grande majorité, disposent de relativement petits budgets. Ce manque de moyens implique que des choix doivent être faits et que, pour certaines communes, l'informatique, la digitalisation et la cybersécurité ne sont pas des investissements prioritaires. Certaines petites communes n'ont pas de budget dédié à l'informatique. Ce manque de moyens se reflète dans le faible pourcentage de communes mettant des ordinateurs à la disposition de leurs municipaux (32,69%). Toutefois, la problématique est reconnue. Durant les 5 dernières années, les budgets informatiques et de cybersécurité ont augmenté (69,81%) (voir figures 8 et 9).

- Dans certaines communes de petite taille, un poste de responsable informatique n'existe pas. Lorsqu'il existe, il s'agit dans la majorité des cas d'un membre de la municipalité. Une minorité de communes compte parmi ses employés des personnes disposant de compétences spécialisées en informatique. Au niveau de l'importance stratégique donnée à la digitalisation des services communaux, la majorité des communes indiquent une importance moyenne ou élevée. En ce qui concerne la problématique de la cybersécurité, les communes reconnaissent une importance stratégique importante (voir figure 14 et 15).

- Un point intéressant soulevé par l'un des conseillers municipaux que nous avons interrogé, concerne le rapport coût/bénéfice pour la mise en place de services digitalisés dans la mesure où l'utilisation des services en ligne reste extrêmement limitée dans le cas d'une petite commune, alors que l'investissement est important. L'offre de services en ligne à la population entre les centres urbains et les petites communes diffère ainsi grandement. Cette question du rapport coût/bénéfice peut également s'appliquer à la question de l'investissement dans la cybersécurité qui peut se révéler important pour une petite commune.

- Les communes du canton de Vaud dépendent de prestataires externes pour gérer leurs infrastructures informatiques. Dans une majorité des cas, les communes stockent et

sauvegardent leurs données sur des serveurs externes, qu'il s'agisse de ceux de leurs prestataires ou de services cloud. Du fait de leurs activités, elles stockent des données personnelles et financières sur leurs résidents. En raison de la doctrine vaudoise de libre marché, chaque commune négocie de manière indépendante les conditions et les services fournis. Cette méthode a des avantages : en cas d'attaque réussie contre un prestataire, le nombre de communes impactées est limité car le système est décentralisé. Cela a également pour avantage de pousser les prestataires à proposer des conditions intéressantes afin d'être compétitifs sur le marché. Il existe toutefois des inconvénients : il n'existe pas aujourd'hui de liste d'exigences en termes de cybersécurité équivalentes pour toutes les communes. Il en résulte que le niveau de protection peut être très différent selon le prestataire et le contrat conclu avec la commune. Cela peut poser des problèmes au niveau du respect des prescriptions de la loi vaudoise sur la protection des données qui implique que celles-ci soient stockées dans des pays dont la législation est compatible avec le niveau de protection suisse. Le niveau de service peut également être impacté par ces différences relatives aux exigences. Alors qu'une commune pourra contacter son prestataire 24h/24 7j/7 en cas de problème, une autre ne le pourra pas. Un autre inconvénient relevé dans les remarques concerne le faible pouvoir de négociation des petites communes pour obtenir des conditions intéressantes auprès de leurs prestataires externes.

- Les communes restent indépendantes dans la mise en place de leurs procédures internes de gestion de la cybersécurité et de réponse en cas d'incident. Alors que certaines semblent s'être préparées à l'éventualité d'une attaque, d'autres n'ont pas de procédures en place. Les autorités cantonales souhaitent garder le contrôle en cas de problème, car elles estiment que la crise ne peut pas être gérée par les seules autorités communales.et que la gestion de crise nécessite des compétences spécifiques et ne peut pas s'improviser. Une question plusieurs fois abordée, que ce soit par l'Union des Communes Vaudoises (UCV) ou par les autorités cantonales, concerne la gestion des ressources en cas d'incident et le développement d'un SOC (Security Operation Center) capable à la fois de répondre aux demandes des communes tout en assurant les besoins des systèmes de l'administration cantonale. Cette question est politique, car il y a des décisions en lien avec le financement de cette infrastructure.

- La formation semble être un point très important pour les communes. Parmi les communes ayant répondu, elles sont 2/3 à avoir offert des formations à leurs collaborateurs. Il est important de noter que les élus devraient également recevoir une telle formation, afin qu'ils ne soient pas victimes de tentatives de phishing ou autre.

- Le système vaudois reste encore très cloisonné et les communes travaillent chacune de leur côté, ne partageant que peu les unes avec les autres. Cela a pour conséquence que les municipaux peuvent se retrouver seuls lorsqu'ils sont confrontés aux questions de cybersécurité et ne savent pas exactement vers qui se tourner. Les communes doivent, chacune de leur côté, créer des règles et des procédures.

- Les communes, dans leurs remarques, appellent à des mesures de centralisation pour certaines compétences et souhaitent mieux partager les bonnes pratiques entre elles. Du fait de la similitude des processus et des données gérées, elles souhaitent pouvoir bénéficier d'un guide de classification de la confidentialité des données et des mesures nécessaires à mettre en place pour les protéger.

- Les grandes communes ont créé une association où les responsables informatiques se rencontrent régulièrement pour traiter des sujets en lien avec l'informatique et la

cybersécurité (l'AVRIC) à laquelle l'ensemble des responsables de petites communes peuvent envoyer un représentant.

Notre seconde question de recherche s'intéressait aux bonnes pratiques que les communes peuvent mettre en place pour une stratégie de cybersécurité crédible. Notre section de recommandations a tenté d'y répondre sur la base d'une analyse de risque générale. Voici quelques points à retenir :

- **Nommez une personne responsable de l'informatique :** la création de cette position au sein de l'administration communale permet de s'assurer qu'une personne gère de manière active les questions en lien avec l'informatique, qu'elle est la personne de référence pour les prestataires externes et qu'elle peut recevoir des formations en cas de besoin.
- **Créez un budget dédié à cette thématique :** la création d'un budget dédié à l'informatique permet de garder un œil sur les dépenses liées à cette thématique et la place comme un enjeu stratégique au niveau de l'administration communale.
- **Définissez vos processus clés :** il est important de définir quels sont les processus et les données de votre administration communale que vous voulez protéger en priorité.
- **Faites appel à un prestataire indépendant pour la réalisation d'un audit :** la cybersécurité ne s'improvise pas. L'idéal est de faire appel à un prestataire indépendant pour la réalisation d'un audit de l'état actuel de la cybersécurité de la commune.
- **Intégrez la cybersécurité dans votre analyse de risque :** la cybersécurité doit être comprise dans votre analyse de risque.
- **Sélectionnez vos mesures de protection en fonction de votre analyse de risque :** il existe des centaines de mesures de protection. Faites votre sélection selon vos priorités identifiées dans votre analyse de risque et votre définition des processus clés.
- **Formation avant tout :** la formation des collaborateurs et des élus est centrale dans la prévention des évènements de cybersécurité.
- **Soyez proactifs dans la création de collaborations :** les collaborations et les partages intercommunaux et avec le canton sont de plus en plus demandés par les responsables communaux. Soyez proactifs !

Il reste beaucoup de travail pour faire en sorte que les communes du canton de Vaud soient en mesure d'atteindre un niveau de maturité élevé en matière de cybersécurité. Nous espérons toutefois que notre étude pourra être une pierre à l'édifice de cette thématique et qu'elle puisse servir de référence pour de futurs projets, que ce soit sur le plan académique ou politique.

8.1 Perspectives de recherche

Il serait intéressant de répéter cette étude dans quelques années afin de voir l'évolution de la situation au point de vue communal et d'observer si les mesures prises au niveau du canton et des faitières de communes ont commencé à porter leurs fruits.

Une autre étude qu'il serait pertinente de mener concerne le mode de fonctionnement des communes d'autres cantons romands et plus largement en Suisse alémanique. Cette recherche

permettrait de faire une comparaison des solutions envisagées par les différentes régions du pays et pourrait servir de base pour un partage des bonnes pratiques sur le plan national.

8.2 Conclusion personnelle

En tant qu'étudiant à la HES-SO, la réalisation de ce travail de master a été pour moi l'occasion de pouvoir participer activement à la protection de ma région. Lorsque j'ai eu à choisir ma thématique, j'avais envie de travailler sur quelque chose qui ait un sens. C'est en lisant un article de journal que j'ai décidé de ma problématique. Je ressentais un sentiment d'impuissance face à ces attaques de plus en plus fréquentes, c'est pourquoi j'ai choisi cette thématique. J'ai ainsi eu l'opportunité de me plonger dans un domaine qui me passionne, la cybersécurité, et ai pu l'appliquer dans un contexte réel.

Les différents acteurs avec qui j'ai eu l'occasion de discuter se sont montrés ouverts pour répondre à mes questions et intéressés à obtenir le résultat de cette étude. Je les remercie chaleureusement pour leur participation et le temps qu'ils m'ont accordé. J'espère que, dans un futur proche, mon étude pourra servir de référence pour la mise en place de politiques permettant de développer la thématique de la cybersécurité dans les communes du canton de Vaud.

Merci pour votre lecture

9 Bibliographie

[1] Association Sécurité Riviera, “Communiqué de presse - Point de situation du 11 octobre 2021, 13h00 - Cyberattaque contre la Commune de Montreux et ses partenaires.” Oct. 11, 2021. Accessed: Apr. 05, 2021. [Online]. Available: https://www.securite-riviera.ch/getmedia/16848b2b-b218-443a-afcb-11070283989f/018_ASR_Comm-presse_Cyberattaque_2.pdf

[2] Association Sécurité Riviera, “Communiqué de presse - Point de Situation du 18 octobre 2021, 18h00 - Cyberattaque contre la commune de Montreux et ses partenaires.” Oct. 18, 2021. Accessed: Apr. 05, 2022. [Online]. Available: https://www.securite-riviera.ch/getmedia/67e9a277-61d8-40a8-8cb9-3a2eabe6fbe4/ASR_Comm-presse_Cyberattaque_6.pdf

[3] Yannick Chavanne, “Cyberattaque contre Rolle: la commune appelle ses résidents à la vigilance (update),” *ICT Journal*, Aug. 30, 2021. Accessed: Jan. 17, 2022. [Online]. Available: https://www.ictjournal.ch/news/2021-08-30/cyberattaque-contre-rolle-la-commune-appelle-ses-residents-a-la-vigilance-update

[4] Daniel Schurter and Oliver Wietlisbach, “Internet-Erpresser veröffentlichen Gigabyte an vertraulichen Daten der Gemeinde Rolle VD,” *watson.ch*, Zurich, Aug. 20, 2021. Accessed: Apr. 05, 2022. [Online]. Available: https://www.watson.ch/!987644812

[5] Service de renseignement de la Confédération SRC, “La Sécurité de la Suisse 2021 - Rapport de situation du Service de renseignement de la Confédération,” Confédération Suisse, Berne, 2021. Accessed: Feb. 01, 2022. [Online]. Available: https://www.vbs.admin.ch/content/vbs-internet/fr/vbs/organisation-des-vbs/die-verwaltungseinheiten-des-vbs/-der-nachrichtendienst-des-bundes.download/vbs-internet/fr/documents/servicederenseignement/rapportsdesituation/SRC_Rapport_de%20situation_Suisse_2021.pdf

[6] Claude-Olivier Volluz, “Cyberattaques attendues en Suisse après les sanctions contre la Russie,” *rts.ch*, Genève, Mar. 10, 2022. Accessed: Apr. 05, 2022. [Online]. Available: https://www.rts.ch/info/suisse/12928839-cyberattaques-attendues-en-suisse-apres-les-sanctions-contre-la-russie.html

[7] Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK), “Prévenir les cybercrimes, Guide à l’intention des communes.” Police cantonale Zurichoise. Accessed: Apr. 06, 2021. [Online]. Available: https://www.ucv.ch/fileadmin/documents/pdf/Th%C3%A8mes/04-Securite/Cybersecurite-Guide-communes-NEDIK_GUI.pdf

[8] Conseil Fédéral, “Stratégie suisse de cyberadministration 2020–2023.” Confédération Suisse, Nov. 20, 2019. Accessed: Apr. 14, 2022. [Online]. Available: https://www.newsd.admin.ch/newsd/message/attachments/59198.pdf

[9] European DIGITAL SME Alliance, “Guide de mise en oeuvre de la norme de gestion de la sécurité des informations ISO/CEI 27001 à l’intention des PME.” Small Business Standards (SBS). Accessed: Apr. 23, 2022. [Online]. Available: https://www.sbs-sme.eu/sites/default/files/publications/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min%20%281%29.pdf

[10] International Organization for Standardization (ISO) and International Electrotechnical Commission (CEI), “Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000:2018(E)).” 2018.

[11] M. Cabric, “Chapter 11 - Confidentiality, Integrity, and Availability,” in *Corporate Security Management*, M. Cabric, Ed. Butterworth-Heinemann, 2015, pp. 185–200. doi: https://doi.org/10.1016/B978-0-12-802934-3.00011-1.

[12] Debbie Walkowski, “What Is The CIA Triad?,” *F5 Labs*, Jul. 09, 2019. https://www.f5.com/labs/articles/education/what-is-the-cia-triad (accessed Apr. 19, 2022).

[13] J. Fruhlinger, “The CIA triad: Definition, components and examples,” *CSO Online*, Feb. 10, 2020. https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html (accessed Jun. 04, 2022).

[14] Le Conseil fédéral, “Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022.” Unité de pilotage informatique de la Confédération UPIC, 2018. Accessed: Feb. 02, 2022. [Online]. Available: https://www.ncsc.admin.ch/ncsc/fr/home/strategie/strategie-ncss-2018-2022.html

[15] Office fédéral pour l’approvisionnement économique and du pays, “Norme minimale pour améliorer la résilience informatique.” 2018. Accessed: Feb. 01, 2022. [Online]. Available: https://www.bwl.admin.ch/dam/bwl/fr/dokumente/themen/ikt/broschuere_minimalstandard.pdf.download.pdf/IKT_FR_2018_Web.pdf

[16] Centre national pour la cybersécurité NCSC, “Si001 - Protection informatique de base dans l’administration fédérale.” Confédération Suisse, Dec. 19, 2013. Accessed: Feb. 02, 2022. [Online]. Available: https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/dokumentation/vorgaben/sicherheit/si001/Si001-IT-Grundschutz-V5-0-f.pdf.download.pdf/Si001-IT-Grundschutz-V5-0-f.pdf

[17] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[18] International Organization for Standardization (ISO) and International Electrotechnical Commission (CEI), “Technologies de l’information — Techniques de sécurité — Systèmes de management de la sécurité de l’information — Exigences (ISO/IEC 27001:2013(F)).” 2013.

[19] International Organization for Standardization (ISO) and International Electrotechnical Commission (CEI), “Technologies de l’information — Techniques de sécurité — Systèmes de management de la sécurité de l’information — Exigences (ISO/IEC 27002:2013(F)).” 2013.

[20] International Organization for Standardization (ISO) and International Electrotechnical Commission (CEI), “Technologies de l’information — Techniques de sécurité — Gestion des risques liés à la sécurité de l’information (ISO/IEC 27005:2018(F)).” 2018.

[21] Donald F. Norri, “A New Look at Local Government Cybersecurity in 2020,” *pm magazine*, Jul. 14, 2021. https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020 (accessed Feb. 05, 2022).

[22] Donald F. Norris, Laura Mateczun, Anupam Joshi, and Tim Finin, “Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity”.

[23] D. F. Norris, L. Mateczun, A. Joshi, and T. Finin, “Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity,” *J. Urban Aff.*, vol. 43, no. 8, pp. 1173–1195, Sep. 2021, doi: 10.1080/07352166.2020.1727295.

[24] J. P. Kesan and L. Zhang, “An Empirical Investigation of the Relationship between Local Government Budgets, IT Expenditures, and Cyber Losses,” *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 2, pp. 582–596, Apr. 2021, doi: 10.1109/TETC.2019.2915098.

[25] European Union Agency for Cybersecurity (ENISA), “ENISA THREAT LANDSCAPE 2021 - April 2020 to mid-July 2021,” Oct. 2021, doi: 10.2824/32479.

[26] Reto Steiner, Andreas Ladner, Claire Kaiser, Alexander Haus, Ada Amsellen, and Nicolas Keuffer, *Zustand und Entwicklung der Schweizer Gemeinden : Ergebnisse des nationalen Gemeindemonitorings 2017*, Somedia Buchverlag. Glaris, 2021. Accessed: May 23, 2022. [Online]. Available: https://digitalcollection.zhaw.ch/bitstream/11475/22601/2/2021_Steiner-etal_Zustand-und-Entwicklung-der-Schweizer-Gemeinden.pdf

[27] C. Kaiser, A. Ladner, J. Machljankin, and R. Steiner, “Sondaggio Nazionale Per I Segretari ComunaliGemeindemonitoring der Schweizer GemeindenLes Communes SuissesData Monitoring Local Communities in Switzerland.” FORS - Swiss Centre of Expertise in the Social Sciences, 2019. doi: 10.23662/FORS-DS-1116-1.

[28] Dr. Michael Buess, Helen Amberg, and Chiara Büchle, “Étude nationale sur la cyber-administration 2022,” Administration numérique suisse, DemoSCOPE AG/Interface Politikstudien Forschung Beratung GmbH, Adligenswil/Lucerne., 2022. Accessed: Aug. 02, 2022. [Online]. Available: https://www.administration-numerique-suisse.ch/application/files/3416/5216/3445/Etude_nationale_sur_la_cyberadministration_2022_compte_rendu.pdf

[29] Marc K. Peter, Andreas Hölzli, Andreas W. Kaelin, Karin Mändli Lerch, Patric Vifian, and Nicole Wettstein, “Numérisation, télétravail et cybersécurité dans les PME.” La Mobilière, digitalswitzerland, FHNW Hochschule für Wirtschaft, SATW, gfs-zürich, Dec. 2020. Accessed: May 23, 2022. [Online]. Available: https://www.mobiliere.ch/assurances-et-prevoyance/tout-pour-votre-pme/numerisation-teletravail-et-cybersecurite-dans-les-pme/telechargement-du-livre-blanc-relatif-a-l-etude-2020-sur-les-pme

[30] Karin Mändli Lerch and Mara Tanner, “Auswirkungen der Corona-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU,” *Schweiz. Mobiliar Versicherungsgesellschaft AG Digit. Allianz Digit. Sicherh. Schweiz Fachhochsch. Nord. FHNW Kompetenzzentrum Digit. Transform. Schweiz. Akad. Tech. Wiss. SATW*, Nov. 2021.

[31] “Les TPE/PME et la cybersécurité,” *IFOP*, Dec. 15, 2021. https://www.ifop.com/publication/les-tpe-pme-et-la-cybersecurite/ (accessed Jun. 05, 2022).

[32] J. de Werra and Y. Benhamou, “Cyberassurance : instrument utile pour la cybersécurité des entreprises ? Analyse juridique et recommandations des mesures étatiques concernant les cyberassurances visant à protéger les entreprises (PME),” *Jusletter*, no. 24 août, 2020, Accessed: Jun. 20, 2022. [Online]. Available: https://archive-ouverte.unige.ch/unige:140819

[33] Karin Mändli Lerch and Mara Tanner, “Auswirkungen der Corona-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU - Befragung von Geschäftsführenden kleiner Unternehmen in der Schweiz,” *Schweiz. Mobiliar Versicherungsgesellschaft AG Digit. Allianz Digit. Sicherh. Schweiz Fachhochsch. Nord. FHNW Kompetenzzentrum Digit. Transform. Schweiz. Akad. Tech. Wiss. SATW*, Jun. 2022.

[34] Microsoft’s Digital Security Unit, “Special Report: Ukraine - An overview of Russia’s cyberattack activity in Ukraine,” Microsoft, Apr. 2022. Accessed: Jul. 07, 2022. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[35] Clusif, “Les fondamentaux de Méhari - Clusif,” *https://clusif.fr/*. https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/ (accessed Aug. 02, 2022).

[36] Jacqueline Favez, “Covid-19 – Vaud fait fuiter des centaines d’e-mails,” *20 minutes*, Oct. 27, 2021. https://www.20min.ch/fr/story/vaud-fait-fuiter-des-centaines-de-mails-999365614486 (accessed Jul. 23, 2022).

[37] Mahmood Sher-Jan, “Data indicates human error prevailing cause of breaches, incidents,” Jun. 26, 2018. https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/ (accessed Jul. 23, 2022).

[38] D. Radcliff, “How a new generation of IoT botnets is amplifying DDoS attacks,” *CSO Online*, Apr. 25, 2022. https://www.csoonline.com/article/3657738/how-a-new-generation-of-iot-botnets-is-amplifying-ddos-attacks.html (accessed Aug. 15, 2022).

[39] “Comment des cyber criminels nigérians ont été arrêtés par les USA ?,” *BBC News Afrique*. Accessed: Jul. 26, 2022. [Online]. Available: https://www.bbc.com/afrique/monde-53334654

[40] M. Campbell, “What Causes Data Loss?,” *Unitrends*, Jul. 05, 2010. https://www.unitrends.com/blog/backup-what-causes-data-loss (accessed Aug. 16, 2022).

[41] Abi Tygas Tunggal, “What is an Attack Vector? 16 Common Attack Vectors in 2022 | UpGuard,” *UpGuard*, Aug. 15, 2022. https://www.upguard.com/blog/attack-vector (accessed Aug. 16, 2022).

[42] Rob Sobers, “166 Cybersecurity Statistics and Trends [updated 2022],” *Varonis*, Jul. 08, 2022. https://www.varonis.com/blog/cybersecurity-statistics (accessed Aug. 16, 2022).

[43] “What is an Cyber Attack Vector? Types & How to Avoid Them,” *Fortinet*. https://www.fortinet.com/resources/cyberglossary/attack-vector (accessed Aug. 16, 2022).

[44] A. Sutcliffe, “8 Most Common Causes of Data Breach,” *Sutcliffe Insurance*, Dec. 21, 2017. https://www.sutcliffeinsurance.co.uk/news/8-most-common-causes-of-data-breach/ (accessed Aug. 16, 2022).

[45] Le Conseil fédéral, *Ordonnance concernant la protection des informations de la Confédération*. 2007, p. 14. Accessed: Aug. 04, 2022. [Online]. Available: https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/2007/414/20210101/fr/pdf-a/fedlex-data-admin-ch-eli-cc-2007-414-20210101-fr-pdf-a.pdf

[46] Andreas Wolter, “Security: The Need-to-know principle,” *TECHCOMMUNITY.MICROSOFT.COM*, Feb. 03, 2021. https://techcommunity.microsoft.com/t5/azure-sql-blog/security-the-need-to-know-principle/ba-p/2112393 (accessed Aug. 04, 2022).

[47] CNIL, “L’anonymisation de données personnelles | CNIL,” May 19, 2020. https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles (accessed Aug. 05, 2022).

[48] William C. Barker, William Fisher, Karen Scarfone, Murugiah Souppaya, and National Institute of Standards and Technology, “Ransomware Risk Management: A Cybersecurity Framework Profile,” Gaithersburg, MD, NISTIR 8374, Feb. 2022. Accessed: Aug. 08, 2022. [Online]. Available: https://doi.org/10.6028/NIST.IR.8374

Annexe 1 – Questionnaire

Cybersécurité des communes vaudoises

Dans le cadre de mon travail de Master à la HES-SO, je réalise une étude sur la gestion de la cybersécurité dans les communes du canton de Vaud. Ce questionnaire a été réalisé en collaboration avec l'Union des Communes Vaudoises et du Label Cybersafe.

L'objectif de cette étude est de mieux comprendre l'état des lieux dans la gestion des infrastructures informatiques au niveau communal et comment la problématique de la cybersécurité est abordée dans les différentes administrations.

Les données récoltées sont traitées avec un haut degré de confidentialité. Elles sont stockées sur un serveur suisse.

En cas de question vis-à-vis de la confidentialité des données, n'hésitez pas à me contacter sur mon adresse Email (Blank) ou par téléphone au (Blank)

Ce questionnaire devrait prendre entre 15 et 20 minutes pour être complété.

Quel est le nom de votre commune (réponse facultative, vous pouvez également choisir de répondre anonymement) : _____

Avez-vous été victime d'une cyberattaque lors des 12 derniers mois.

a. Oui
b. Non

Démographie

1. Dans quel district se situe votre commune ?

a. Aigle
b. Broye-Vully
c. Gros-de-Vaud
d. Jura-Nord Vaudois
e. Lausanne
f. Lavaux-Oron
g. Morges
h. Nyon
i. Ouest Lausannois
j. Riviera-Pays d'Enhaut

2. Quel est le nombre d'habitants de votre commune ?

a. Moins de 1000 habitants
b. 1000 – 1999 habitants
c. 2000 - 4999 habitants
d. 5000 - 9999 habitants
e. 10'000 - 19'999 habitants

f. 20'000 - 49'999 habitants
g. 50'000 - 99'999 habitants
h. plus de 100'000 habitants

3. Quel est le nombre d'équivalents temps pleins (ETP) travaillant dans votre commune ?

Organisation

4.a Est-ce que votre commune a un budget spécifiquement dédié à l'informatique ?

a. Oui
b. Non

4.b Quel pourcentage de ce dernier est dédié à la sécurité informatique ?

4.c Comment le budget a-t-il évolué au cours des 5 dernières années ?

	Grande diminution (-30 % ou plus)	Petite diminution (-1 % à -29%)	Resté pareil	Petite augmentation (+1 % à + 30%)	Grande augmentation (+30% ou plus)
Informatique					
Sécurité informatique					

5.a Les membres de la municipalité utilisent-ils des ordinateurs fournis par la commune dans la réalisation de leurs tâches ?

a. Oui
b. Non

5.b Est-ce que l'authentification à deux facteurs a été mise en place pour accéder aux serveurs de la commune ?

a. Oui
b. Non

6. Quel est le niveau de priorité stratégique que donne la municipalité aux questions suivantes en lien avec l'informatique pour la législature 2021-2026 ? (1 = pas prioritaire, 5 = Priorité n° 1)

	1	2	3	4	5
Digitalisation des services communaux					
Sécurité informatique					

7.a Est-ce que votre commune a un répondant informatique formellement reconnu ? (personne ayant dans son dicastère ou dans sa description de poste la responsabilité des questions liées à l'informatique)

a. Oui
b. Non

7.b Si oui, quel est son rôle dans la commune ?

a. Membre de la municipalité
b. Boursier
c. Secrétaire communal
d. Spécialiste salarié de la commune
e. Autre

7.c Si autre, Merci de préciser

8.a Est-ce que votre commune compte parmi ses employés des personnes ayant des compétences professionnelles en informatique (études supérieures en informatique, CFC d'informaticien) ?

a. Oui
b. Non

8.b Gérez-vous en interne l'aspect administratif des systèmes d'information (création de compte, gestion des accès aux données, etc.) ?

a. Oui
b. Non

9.a Où sont stockées vos données ?

a. Serveur interne
b. Sur un service cloud
c. Sur les serveurs de votre prestataire informatique

9.b Si différentes données sont stockées à différents endroits, merci de préciser :

10.a Votre commune procède-t-elle à des sauvegardes régulières des données (backups) ?

a. Oui
b. Non
c. Je ne sais pas

10.b À quelle fréquence ces sauvegardes sont-elles effectuées ?

10.c Où sont stockées vos sauvegardes (plusieurs réponses possibles) ?

a. Sur un serveur interne
b. Sur un service cloud
c. Sur les serveurs d'un de vos prestataires

Procédures et pratiques liées à la cybersécurité

11. Avez-vous réalisé une analyse des risques liés à la cybersécurité ?

a. Oui
b. Non

12.a Avez-vous établi une liste des prestataires de services informatiques externes de votre commune ?

a. Oui
b. Non

12.b Avec combien de prestataires externes travaille votre commune ?

12.c Lors de vos négociations avec vos prestataires externes, avez-vous établi une liste d'exigences liées à la sécurité informatique ?

a. Oui
b. Non
c. Nous ne faisons pas appel à un prestataire externe

12.d Est-ce que cette liste se base sur une norme nationale (norme minimale pour les TIC) ou internationale (NIST Framework, ISO 27001) ? (Plusieurs réponses possibles)

a. Non
b. Norme nationale
c. NIST Framework
d. ISO 27001
e. Recommandation d'un partenaire externe (P.E. Cyber-safe – merci de préciser)

f. Je ne sais pas
g. Autre (merci de préciser)

12.e Merci de préciser

12.f Avez-vous négocié un SLA (accord de niveau de service) pour la cybersécurité avec vos prestataires externes ?

a. Oui
b. Non
c. je ne sais pas

12.g Selon votre SLA (accord de niveau de service), quels sont les horaires durant lesquels vous pouvez joindre votre prestataire pour des problèmes liés à la cybersécurité ?

13.a Avez-vous souscrit une assurance pour le risque de cybersécurité ?

a. Oui
b. Non

13.b Est-ce que cette assurance couvre les risques liés aux attaques de type rançongiciels (Ransomware) ?

a. Oui
b. Non
c. Je ne sais pas

14.a Votre commune a-t-elle établi des procédures de réaction d'urgence en cas d'évènements en lien avec la sécurité informatique ? (P.E. cellule de crise, plan de communication) Sélectionnez les procédures que vous avez établies :

a. Procédure d'identification de l'attaque
b. Procédure d'isolation des systèmes du réseau
c. Procédure d'alerte auprès de la police
d. Procédure de cellule de crise
e. Plan de communication
f. Procédure de récupération des données
g. Autre (merci de préciser)

14.b Merci de préciser :

14.b Une personne de l'administration communale a-t-elle été désignée pour prendre la décision d'interrompre les systèmes d'information en cas d'attaque ?

a. Oui
b. Non

15.a Votre commune a-t-elle construit un réseau pour partager des connaissances et des procédures pour se préparer au mieux à un évènement de cybersécurité ?

a. Non
b. Oui

15.b Avec qui êtes-vous en contact ?

a. Avec une commune limitrophe disposant de meilleures compétences dans le domaine.
b. Avec les autorités cantonales
c. Avec les autorités fédérales
d. Avec l'Union des Communes Vaudoises (UCV)
e. Avec l'association Cybersafe
f. Autre (Merci de préciser)

15.c Si Autre, Merci de préciser

16. Les employés communaux ont-ils reçu au cours des 2 dernières années une sensibilisation à la sécurité informatique ?

a. Oui
b. Non

17. Faites-vous appel à des prestataires externes afin de tester la sécurité de votre infrastructure informatique (hackeur éthique) ?

a. Oui
b. Non

18. Avez-vous répondu à une offre spontanée d'une entreprise privée pour des prestations liées à la cybersécurité ?

a. Oui
b. Non

Vos attentes

Qu'est-ce qui, selon vous, devrait être mis en place pour faciliter l'augmentation du niveau de la cybersécurité de votre commune ?

19. Votre opinion nous intéresse.

20. Qu’avez-vous prévu d’entreprendre durant les prochains mois ?

Annexe 2 – Outil d'auto-évaluation – Page de garde

Outil d'auto-évaluation de la cybersécurité	Fonctionnement	Ressources
Dans le cadre du travail de Master de Stéphane Müller étudiant la thématique de la cybersécurité des communes vaudoises, un outil d'auto-évaluation a été mis en place. Ce dernier a pour but de permettre aux élus municipaux d'aborder cette problématique et de se poser les bonnes questions dans l'objectif de mettre en place une politique en ce domaine. Dans le présent document, le masculin est utilisé dans le seul but d'alléger le texte.	L'outil d'auto-évaluation présente des affirmations concernant votre commune. Si une affirmation vous semble vraie, sélectionnez VRAI dans le menu déroulant, si elle vous semble fausse, sélectionnez FAUX.	Cet outil souhaite également permettre aux élus municipaux de pouvoir accéder depuis un seul endroit à divers outils d'auto-évaluation existants créés par des organismes reconnus, ainsi qu'à de la documentation sur les mesures à mettre en place pour améliorer la cybersécurité.
Public cible	**Poids**	
Elus municipaux du canton de Vaud	Chaque mesure a un poids différent dans l'évaluation de la maturité de la commune en matière de cybersécurité. En effet, certaines mesures techniques ou organisationnelles ont un impact plus important que d'autres.	
IMPORTANT	**Evaluation**	
La cybersécurité n'est pas une thématique qui s'improvise. Il est recommandé de faire appel à un prestataire spécialisé qui mènera un audit spécifique de l'état de maturité de la commune en matière de cybersécurité et pourra établir avec les responsables communaux une liste personnalisée de mesures à prendre.	L'évaluation s'effectue sur le modèle que l'on trouve habituellement dans le système éducatif vaudois. Les notes vont de 1 à 6 et sont calculées selon la formule : (point obtenus x 5/points totaux) + 1. L'onglet résultat vous donne un aperçu de l'évaluation avec une représentation graphique des résultats.	

Annexe 3 – Outil d'auto-évaluation - questionnaire

Organisation			
Critère	Réponse	Poids	Remarques
Votre commune a désigné une personne responsable de l'informatique.		4	
Le responsable informatique a reçu une formation adéquate.		3	
Le responsable informatique a rejoint un réseau intercommunal sur cette thématique.		2	
Votre commune a un budget dédié à l'informatique.		4	
Votre commune a réalisé un audit avec un prestataire externe indépendant.		4	
Votre commune a mis en place une stratégie pour la cybersécurité.		4	
Identifier			
Votre commune a défini les processus qu'elle souhaite protéger en priorité.		4	
Votre commune a défini les données qu'elle souhaite protéger en priorité.		4	
Votre commune a classifié ses données selon leurs niveaux de confidentialité.		3	
Votre commune a identifié les risques liés à la cybersécurité.		3	
Votre commune a intégré les risques liés à la cybersécurité dans son processus de gestion des risques.		3	
Votre commune dispose d'une cartographie de ses données.		2	
Votre commune a réalisé un inventaire de ses équipements informatiques.		2	
Votre commune a réalisé un inventaire des logiciels et licences qu'elle utilise dans ses activités.		2	
Votre commune a réalisé un inventaire des prestataires informatiques avec lesquels elle collabore.		3	
Votre commune reste informée sur les dernières menaces en lien avec la cybersécurité.		2	

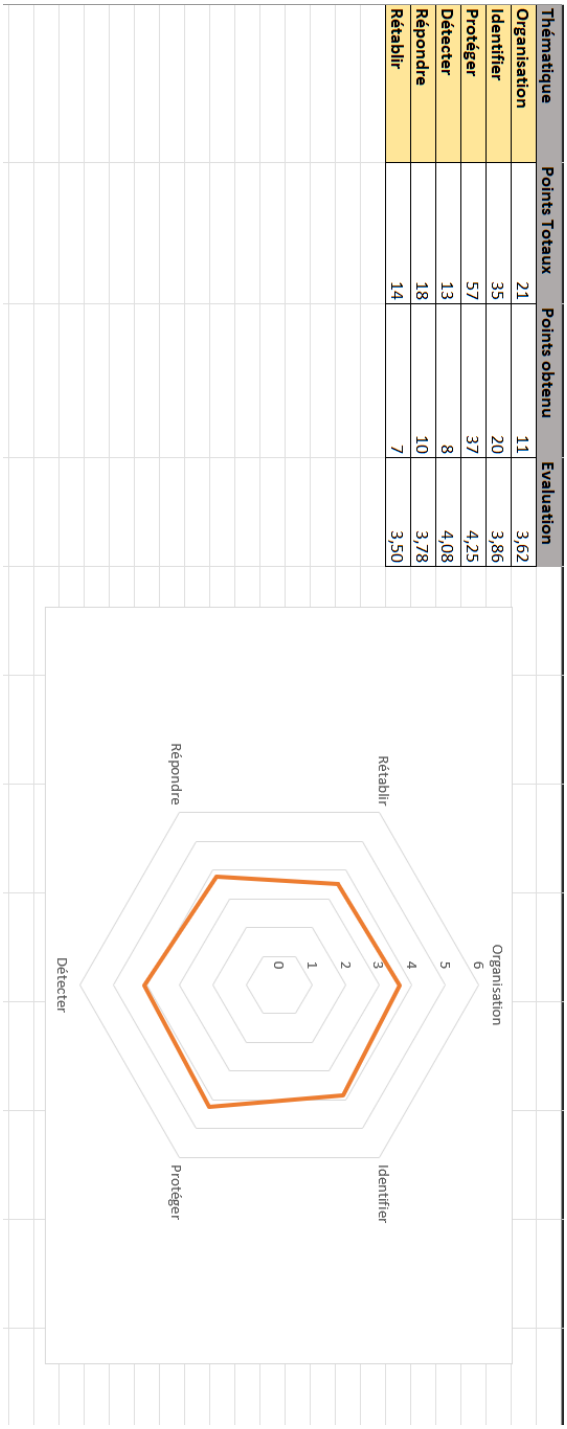
Votre commune enregistre les opérations effectuées sur son réseau au moyen de logs.		3	
Les employés, les élus et les prestataires externes connaissent leur rôle en matière de cybersécurité.		4	
Protéger			
Votre commune forme régulièrement ses collaborateurs et les élus à la problématique de la cybersécurité. (Phishing, fraude, utilisation correcte des outils informatique, etc.).		4	
Votre commune a mis en place une charte informatique à destination des collaborateurs et des élus.		2	
Votre commune a négocié avec ses prestataires informatiques des exigences de cybersécurité sur la base de normes reconnues. (Norme minimale TIC, NIST, ISO 27001,…)		3	
Votre commune fait usage d'un pare-feu pour protéger son réseau de l'extérieur.		2	
Pour se connecter à distance aux réseaux de votre commune, l'utilisation d'un VPN est nécessaire.		2	
Votre architecture réseau fonctionne selon le principe "Zero-Trust".		2	
L'accès aux boites mails de votre personnel et de vos élus est protégé par une authentification forte (2-facteurs).		3	
Votre commune travaille selon le principe du "Need-To-Know" (voir définition).		4	
Votre commune recourt à l'utilisation de gestionnaires de mots de passe pour sécuriser ses accès.		2	
Votre commune procède à des mises à jour régulières sur l'ensemble de son infrastructure informatique et de ses logiciels.		4	
Votre commune a investi dans l'achat d'un logiciel antivirus.		4	
Votre commune procède régulièrement à des sauvegardes de données.		4	

Votre commune procède régulièrement à des tests de restauration de données.		3	
Les droits des utilisateurs sont limités au minimum pour réduire le risque d'erreur.		2	
Votre commune fait appel à un prestataire crédible pour l'hébergement de son site internet.		3	
Votre site internet est régulièrement mis à jour.		3	
Les infrastructures connectées (caméras, panneaux électroniques d'information) sont protégées par des mots de passe forts.		2	
Votre commune a convenu des exigences de sécurité avec ses fournisseurs d'infrastructures connectées.		2	
Votre commune utilise un logiciel anti-spam.		3	
Votre commune utilise un filtre DNS.		3	
Détecter			
Votre commune dispose de moyens techniques pour détecter les incidents de cybersécurité.		4	
Les évènements identifiés sont analysés et répertoriés.		2	
Les incidents sont analysés pour en évaluer l'impact sur les parties prenantes.		3	
Votre commune procède régulièrement à des tests de sécurité pour identifier les vulnérabilités.		3	
Les incidents sont communiqués aux autorités cantonales et fédérales.		2	
Répondre			
Votre commune a mis en place des procédures de réaction d'urgence.		4	
Votre commune a négocié avec ses prestataires informatiques un accord de niveau de service pour la cybersécurité (En cas d'urgence le prestataire est-il joignable ?).		4	
Votre commune dispose d'une liste de personnes à contacter en cas d'urgence.		3	
Votre commune a prévu un plan de continuité des activités.		4	

Votre commune a mis en place un plan de communication de crise.		3	
Récupérer			
Votre commune est en mesure de rétablir son système d'information en cas d'incident.		4	
Votre commune apprend de l'incident.		3	
Votre commune communique sur les mesures prises pour prévenir ce type d'incident dans le futur.		3	
Les parties prenantes impactées sont informées.		4	

Annexe 4 – Outil d'auto-évaluation - Résultats

Thématique	Points Totaux	Points obtenu	Evaluation
Organisation	21	11	3,62
Identifier	35	20	3,86
Protéger	57	37	4,25
Détecter	13	8	4,08
Répondre	18	10	3,78
Rétablir	14	7	3,50



Annexe 5 – Outil d'auto-évaluation – Ressources

Ressources

Cette section regroupe un ensemble de ressources librement disponibles en ligne qui vous aideront à approfondir la thématique et permettront à votre commune d'effectuer diverses analyses pour évaluer votre maturité au niveau de la cybersécurité.

Documentation	**Institution**	**URL**
Norme minimale sur les TIC	Confédération, Suisse	Lien
Prévenir les cybercrimes, guide à destination des communes	NEDIK / UCV	Lien
Conseils en cas de cyberattaques	Canton de Vaud / UCV	Lien
Aide-mémoire des premières mesures à prendre en cas d'attaque informatique	Cybersafe / UCV	Lien
Cadre pour l'amélioration de la cybersécurité des infrastructures critiques	NIST	Lien
Conditions générales pour les prestations TIC	Administration numérique, Suisse	Lien
Cybersécurité Vaud	Canton de Vaud	Lien
Si001 - Protection informatique de base dans l'administration fédérale	Confédération, Suisse	Lien
Ransomware Risk Management: A Cybersecurity Framework Profile (En Anglais)	NIST	Lien
Outils d'auto-évaluation	**Institution**	**URL**
Norme minimale sur les TIC - Outil d'auto-évaluation	Confédération, Suisse	Lien
Si001 - Hi01 - Mise en œuvre des mesures de protection informatique de base dans l'administration fédérale	Confédération, Suisse	Lien