Annexes au préavis « Pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026 »

Annexe 1

Cas marquants d'attaques subies en Suisse et dans le monde

Le tableau ci-dessous liste quelques cas marquants de ces cinq dernières années en Suisse et dans monde.

Date	Cible et nature de l'attaque	Commentaires
10 octobre 2021	Administration communale de Montreux (VD, Suisse) : l'évaluation est encore en cours.	Evaluation en cours. *Plus d'information : 24heures.ch*
20 août 2021	Administration communale de Rolle (VD, Suisse) : vol des données personnelles de quelque 5000 habitants, données actuellement publiées sur le Darknet.	L'attaque était sophistiquée. S'y opposer nécessite des moyens techniques et humains appropriés, et une bonne organisation. *Plus d'information : RTS Info*
4 octobre 2020	Trois universités suisses, dont celle de Bâle : détournements de salaires, suite au vol de mots de passe par Phishing (hameçonnage).	Les criminels ont détourné un montant à six chiffres. Une partie des sommes se trouve désormais sur des comptes à l'étranger. *Plus d'information : RTS Info*
9 février 2021	Service des eaux de la Ville de Oldsmar (Floride, USA) : réseau d'eau potable contaminé par piratage informatique	Le piratage, découvert par hasard, utilisait un dispositif de prise de contrôle à distance mal configuré. *Plus d'information : swissinfo.ch*
10 mars 2021	Groupe aérien Swiss, via la société SITA, basée à Genève : vol des données personnelles des clients du programme de fidélité.	Attaque très sophistiquée. Vol important de données des clients de la société SITA, qui concernerait 1,35 million de passagers. *Plus d'information : Le Temps*
17 février 2021	Hôpitaux des villes de Dax et de Villefranche-sur-Saône (France) : sabotage des postes de travail par Ransomware, entraînant la paralysie des établissements.	L'ensemble des équipes ont opéré un retour forcé au papier et au stylo. Les blocs opératoires ont été mis en pause. *Plus d'information : Le Temps*
5 déc. 2020 **15 mai 2021**	Constructeur d'hélicoptères KOPTER (Wetzikon, Suisse) : vol de données suivi d'un sabotage des systèmes IT via un Ransomware, entraînant la paralysie du SI.	Kopter ayant refusé de payer la rançon, les données volées ont été diffusées sur le Darknet (dossiers commerciaux, contrats de défense, etc.) *Plus d'information : ZDnet.com, Le Temps*
14 mai 2021 **10 mai 2021**	Opérateur d'oléoducs Colonial Pipeline (USA) : sabotage des systèmes IT via un Ransomware, entraînant la paralysie de l'activité des principaux pipelines de la côte est des Etats-Unis.	Craignant une pénurie d'essence, Colonial Pipeline aurait accepté, avec l'accord du gouvernement, de verser une rançon de $ 5 millions aux pirates du groupe DarkSide. *Plus d'information : Le Temps, ICTJournal.ch*

Annexe 2

Liste des attaques subies par la Ville de Lausanne

Le tableau ci-dessous liste les attaques subies par la Ville ces cinq dernières années.

Période	Nature de l'attaque	Commentaires
12 septembre 2017	Infection de plus de 1'200 postes de travail par le logiciel malveillant EMOTET (cheval de Troie polymorphique difficile à détecter visant à collecter discrètement des données bancaires).	Une analyse poussée de tous les postes et serveurs de la Ville (environ 6'000) a dû être réalisée. Les coûts globaux de cette attaque sont estimés à plus de CHF 200'000.-.
28 juin 2021	Infection d'un poste de travail par un logiciel malveillant sophistiqué, piloté à distance sur Internet et se propageant sur d'autres postes.	L'intervention rapide des équipes a permis de contenir l'incident et de limiter ses effets.
Permanent	Attaques de phishing (hameçonnage) par vagues successives, visant à installer des logiciels malveillants (cheval de Troie, rançongiciel, etc.) sur les postes de travail.	Les techniques utilisées sont de plus en plus sophistiquées et permettent aux attaquants de franchir les barrières de sécurité de plus en plus fréquemment.

Annexe 3

Définitions des principes stratégiques de protection des données

1. Principe de responsabilité commune mais différenciée

Chaque collaboratrice ou collaborateur de la Ville ou chaque sous-traitant opérant pour le compte de la Ville doit être personnellement impliqué, en fonction de son rôle et de ses responsabilités, dans la mise en œuvre des exigences légales et/ou imposées par la Ville en matière de protection des données personnelles. Elle ou il doit, après avoir pris connaissance de ses droits et devoirs, reconnaître formellement ses responsabilités en la matière.

Au niveau de chaque direction ou service de la Ville, les autorités hiérarchiques sont responsables, sur leur périmètre de responsabilité, de l'application des exigences de la Ville en matière de protection des données personnelles. Ils doivent s'assurer que les consignes sont respectées et que les contrôles internes prévus par la Ville sont effectués.

2. Principe de gestion de la conformité

La gestion de la protection des données personnelles doit être basée sur un registre des activités de traitement régulièrement tenu à jour ainsi que sur l'établissement d'une stratégie pour identifier, analyser et traiter les non-conformités identifiées.

La gestion de la conformité se fait par l'adoption cohérente et concertée de mesures de prévention et de protection visant à éviter la violation des exigences applicables et en limiter l'impact en cas d'incident. Outre le degré d'impact pour les droits et libertés des personnes concernées, lesdites mesures tiennent compte du principe de cohérence, tel qu'exprimé ci-dessous, ainsi que de la nature, de la portée, du contexte et des finalités du traitement. Elles sont réexaminées et actualisées autant que nécessaire.

En outre, la mise en place d'une nouvelle activité de traitement ou la modification d'une activité de traitement existante doit faire l'objet d'une analyse permettant d'appréhender la licéité et les impacts potentiels sur les droits et libertés des personnes concernées.

3. Principe de cohérence

Toutes les exigences et pratiques relatives à la protection des données adoptées au sein de le Ville, sans égards à leur nature ou forme, doivent être, dès leur publication officielle :

- conformes à la législation applicable ;
- alignées avec la stratégie globale de la Ville ;
- cohérentes avec les moyens, humains et financiers, dont dispose la Ville, et applicables, immédiatement ou à court terme, dans le cadre de ces moyens.

Les sous-traitants œuvrant pour le compte de la Ville doivent se voir imposer contractuellement, ou par tout autre moyen contraignant, le respect des exigences en matière de protection des données personnelles applicables au sein de la Ville.

4. Principe de gestion du cycle de vie et d'amélioration continue

Les données personnelles sont protégées depuis leur collecte jusqu'à leur destruction ou anonymisation définitive. Par conséquent, les exigences et mesures adoptées par la Ville doivent couvrir toutes les étapes du cycle de vie des données personnelles.

En outre, toute solution ou service permettant le traitement de données personnelles doit prendre en compte, dès sa conception, les exigences applicables en la matière, qui ne doivent pas être traitées "à part" ou "après".

Le respect des exigences adoptées par la Ville doit être contrôlé de manière appropriée ; les principes et les moyens de contrôle interne adéquats doivent être inclus dès le départ et effectués sur une base régulière. Lors des contrôles, tout constat de non-conformité avec

une ou plusieurs exigences de protection des données, ou avec la législation en vigueur, ne doit pas être ignoré et doit faire l'objet d'un signalement à la hiérarchie, puis résolue par des mesures appropriées.

L'ensemble des processus permettant d'assurer la protection des données personnelles doit être audité régulièrement. Les éventuels dysfonctionnements observés ne doivent pas être ignorés, et seront pris en compte comme des opportunités de contribuer à la démarche globale d'amélioration continue de la protection des données personnelles.

5. Principe de transparence

Toutes les exigences applicables et toutes les décisions importantes prises dans le cadre de la gestion de la protection des données personnelles doivent être formalisées dans des documents. Cette documentation liée à la protection des données personnelles (politiques, directives, décisions, résultats d'audit, etc.) doit être gérée avec rigueur sur la base de processus clairement définis (élaboration, validation, enregistrement, classement, diffusion et mise à jour) et connus de tous les acteurs impliqués.

Les documents relatifs à la stratégie et à la politique de la Ville en matière de protection des données personnelles doivent être connus par tous les acteurs concernés (collaboratrices et collaborateurs de la Ville, sous-traitants, etc.). La dernière version en vigueur de chaque document doit être facilement accessible. Afin de faciliter la compréhension et l'approbation de la politique de la Ville en matière de protection des données, un programme de sensibilisation et de formation couvrant tous les besoins pédagogiques des acteurs concernés doit être défini et mis en œuvre.

La politique de contrôle et de supervision de la Ville en la matière doit être connue par tous les acteurs concernés ; les objectifs et modalités de mise en œuvre doivent être communiqués de façon totalement transparente.

Annexe 4

Enjeux pour la Ville

La sécurité de l'information et la protection des données ne sont ni des produits, ni des états, mais des processus perpétuels, des activités. Leur mise en place exige une prise de conscience forte : le risque numérique doit faire partie intégrante des risques opérationnels gérés par la Ville et ne relève plus des seules équipes informatiques ou juridiques. Les paragraphes suivants explicitent l'importance de la sécurité et de la protection des données pour le déploiement de politiques publiques essentielles.

1.1 Cyberadministration

La cyberadministration a pour objectif de permettre à la population et aux entreprises de traiter leurs affaires importantes avec les autorités par voie électronique, grâce aux technologies de l'information et de la communication. La stratégie suisse de cyberadministration[1] poursuit les trois objectifs suivants :

1. l'économie effectue les transactions administratives avec les autorités par voie électronique ;
2. les autorités modernisent leurs processus et communiquent entre elles par voie électronique ;
3. la population peut régler ses affaires importantes avec les autorités par voie électronique.

Pour que ces objectifs soient atteints, il est impératif que la protection des données et la sécurité de l'information soient prises en compte à un stade précoce et dans une mesure appropriée. Par ailleurs, dans un tel contexte, tout incident de sécurité peut avoir des conséquences importantes. Par conséquent, sans cybersécurité et sans protection des données personnelles, il ne peut y avoir de cyberadministration sûre et efficace.

1.2 Ville intelligente (smart city)

Une *smart city* a pour objectif d'offrir une qualité de vie élevée à ses habitants et à ses entreprises tout en consommant le minimum de ressources, grâce notamment à une connexion entre les systèmes d'information et de communication des bâtiments, des sites et des villes[2]. Pour être considérée comme une *smart city*, une ville doit être en mesure de répondre à différents critères définis par SuisseEnergie, notamment :

- exploiter de façon efficiente des formes d'énergie propres, ce qui implique une gestion numérique en temps réel des ressources ;
- gérer de façon optimale les transports publics et le trafic routier, ce qui implique une intégration poussée de l'informatique dans les moyens de transport et les infrastructures ;
- appliquer le principe de transparence en offrant à la population un accès ouvert aux données (notion d'*open data*), tout en garantissant la confidentialité des données sensibles et personnelles ;
- développer de nouveaux lieux et modes de travail, basés sur la collaboration, tout en réduisant les déplacements, ce qui implique le développement d'outils informatiques appropriés.

Dans tous ces domaines, une *smart city* utilise intensivement les technologies numériques. Cela implique que tous les systèmes informatiques qui supportent ces domaines soient sécurisés. En effet, un incident de sécurité peut affecter significativement le système d'information, allant possiblement jusqu'à la paralysie totale. Sans sécurité de l'information et

[1] Source : E-Governement Suisse (https://www.administration-numerique-suisse.ch/fr).

[2] Source : programme SuisseEnergie (https://www.suisseenergie.ch/)

sans protection des données personnelles, il ne peut y avoir de projet *smart city* réussi. Il s'agit de deux prérequis indispensables.

1.3 Souveraineté numérique

L'expression « souveraineté numérique » englobe une multitude de concepts, mais peut se résumer aux deux définitions suivantes :

- pour un individu, la souveraineté numérique est la maîtrise de son passé, son présent et de son futur tels qu'ils se manifestent et s'orientent par l'usage des nouvelles technologies de l'information ;
- pour une administration publique ou un état, elle désigne sa capacité à agir dans le cyberespace en préservant ses intérêts et ceux de ses usagères et usagers, à le réguler et peser sur l'économie numérique.

En l'espace de quelques années, l'Internet est devenu l'épine dorsale de nos sociétés, engendrant une dépendance aux nouvelles technologies et aux entreprises qui les contrôlent. Cette dépendance ne peut qu'augmenter avec le temps. Les faits survenus dans l'actualité récente (p.ex. cybersurveillance massive de citoyens, manipulation d'élections libres, opérations de déstabilisation à distance, espionnage économique, etc.) mettent en lumière les nouveaux défis auxquels sont confrontés les états, les acteurs économiques et la population elle-même. Bien qu'elles ne constituent pas une réponse unique à cet enjeu majeur, la sécurité de l'information et la protection des données sont des conditions nécessaires à la souveraineté numérique.

1.4 Évolution vers l'informatique en nuage (cloud computing)

Depuis plusieurs années, l'informatique connaît à l'échelle mondiale une évolution fondamentale et inexorable : les solutions historiquement hébergées dans les centres de données des entreprises (solutions sur site, *on-premise* en anglais) sont petit à petit externalisées, le plus souvent sur des infrastructures partagées accessibles via Internet. Ces solutions sont désignées par le terme informatique en nuage (*cloud computing* en anglais), et généralement par le terme Cloud.

Les moteurs de cette évolution sont multiples :

- le Cloud fournit des services qui répondent aux nouveaux modes de travail (nomadisme, télétravail, etc.) : applications en ligne, accessibles partout, à tout moment, etc. ;
- le Cloud fournit des services délivrés à la demande et facturés à l'usage, ce qui permet aux organisations de dégager des économies financières substantielles ;
- les grands éditeurs (p.ex. Microsoft, Oracle, SAP, etc.) investissent de moins en moins dans les solutions traditionnelles au profit des solutions Cloud. Certains ont même annoncé l'arrêt de la commercialisation de plusieurs de leurs produits phares *on-premise* ;
- le Cloud est d'ores et déjà omniprésent dans le quotidien des collaboratrices et collaborateurs, tant dans leur sphère privée que professionnelle, par exemple lors de l'usage de solutions telles que WhatsApp, Google Docs, Gmail, Facebook, Dropbox ou Swiss Transfer.

Le Cloud offre de réelles opportunités. Néanmoins, il présente également des risques, notamment juridiques, que la Ville doit gérer (par exemple le risque de ne pas pouvoir récupérer les données en cas de faillite ou de rachat, le risque de non-conformité du service avec la loi sur la protection des données, etc.). Plusieurs services différents offerts par le Cloud pourraient être envisagés, par exemple la location de certaines applications, l'utilisation de plateformes de développement, l'utilisation d'infrastructures, dont les choix seraient dépendants du niveau de sécurité et de la conformité à la protection des données.

Ainsi, sans sécurité de l'information et sans protection des données personnelles, il ne peut y avoir de mise en place de solutions Cloud. En clair, les données sensibles au sens de la loi resteraient à la Ville, les données non sensibles pourraient être mises sur un Cloud. Et pour finir, l'objectif est de travailler avec des Clouds locaux regroupant différents grands acteurs et/ou en tous cas des Clouds suisses.

1.5 Transformation numérique

Aujourd'hui, l'ensemble du personnel est amené à traiter en continu et le plus efficacement possible une quantité toujours plus grande d'informations, sous des formes variées et évolutives. Or, les usages en matière d'organisation, établis à l'ère du tout papier, n'ont pas été collectivement revus et repensés pour s'adapter à un environnement toujours plus numérique.

Cette nouvelle donne impose de restructurer les processus et les systèmes sous-jacents pour mieux accompagner les services dans la transition vers le tout numérique. Dans ce contexte, la mise en œuvre de la sécurité de l'information et de la protection des données personnelles, dès le début (« by design ») avec une approche zéro confiance (voir chap. 7.8), permettra de mettre en œuvre des pratiques et des solutions moins contraignantes et plus faciles à adopter.