Conseil communal de Lausanne

Rapport de la Commission n°64

chargée de l'examen du préavis n°2023/47

« SOI – Pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026 – Demande de crédit d'investissement »

Rapportrice : Mme Magali Crausaz Mottier (eàg)

Membres : Mmes Onaï Reymond (soc) Gaelle Mieli (soc) Marisa Maurer (plr) Marlyse Audergon (vert, remplaçant Sima Dakkus)
MM. Roland Philippoz (soc, remplaçant Yvan Salzmann) Yusuf Kulmiye (soc,remplaçant Astrid Lavanderos) Matthieu Delacrétaz (plr, remplaçant Nicola Hurni) Jean-Claude Seiler (plr) Eric Bettens (vert) Mathias Paquier (v'lib) Nicola Di Giulio (udc)

Membres excusés : Mme Tatiana Taillefert (vert)

Représentant-e-s de la Municipalité et de l'administration :

Mme Natacha Litzistorf, Conseillère municipale, Directrice LEA
MM. Vincent Naïnemoutou, SOI et Benoit Hérisson, SOI

Note de séance : Mme Caroline Lemery accompagnée par Mme Patricia Pacheco

Lieu : Port-Franc 18, 3ème étage, salle 368

Date : mercredi 29 novembre 2023 de 17h à 18h30

Présentation du projet

Madame la Municipale constate la numérisation des logiques et des pratiques administratives devant faciliter la tâche des administrés, particuliers comme entreprises. Selon elle, cette numérisation engendre cependant certains risques, en termes de sécurité et de protection des données. Ce sont des enjeux forts actuels et pour les années à venir qu'elle se propose de traiter dans ce préavis. En cas de cyberattaques, elle souligne une forte attente de la part du public en termes de communication. Elle évoque la difficulté à garder une transparence envers le public et les personnes concernées tout en ne disant pas tout, afin de pouvoir continuer à se protéger. Selon elle, ce préavis est donc capital de nos jours. Elle dit vouloir porter davantage d'attention sur ces thématiques, malgré le fait que beaucoup a déjà été fait. Ce préavis passe en revue tous les domaines sur lesquels il faut agir, et il spécifie également que les demandes qui y sont formulées permettent de traiter seulement certains aspects, et non pas la globalité des objets évoqués. Le montant demandé est élevé mais il ne permettra pas de traiter l'ensemble des objets abordés dans le préavis. Elle évoque trois enjeux fondamentaux à ses yeux. Premièrement, la sécurité de l'informatique industrielle, qui présente des risques élevés sur lesquels elle souhaite intervenir. Deuxièmement, la protection des données. Le fait que la numérisation change les pratiques et les logiques administratives suppose aussi, en plus des nouvelles bases légales qu'il faut implémenter, qu'un changement de culture à l'interne de l'administration doive s'opérer. Troisièmement, la gestion des identités et des accès. Elle ajoute qu'en arrière-plan, ce préavis exprime également l'intention résolue d'entreprendre des actions de formation et de sensibilisation pour accompagner ce changement de culture qui doit être opéré, cela doit être rendu obligatoire. Elle dit qu'il faut intensifier la vigilance concernant les enjeux et les risques liés à la protection des données. Selon elle, il n'y a pas assez de conscience de ces risques, et la gouvernance est donc essentielle pour savoir comment s'organiser et communiquer en cas d'attaque, afin de mieux gérer les crises.

Discussion générale

L'obsolescence : le sujet n'est pas traité dans ce préavis parce qu'il a déjà été abordé dans d'autres préavis

L'audit de sécurité informatique (Audit interne du CFL[1]) : ce rapport contient onze recommandations, dont certaines ont déjà été adressées, telle que la recommandation sur les anomalies d'accès à la gestion des mots de passe. La Directive sur la gestion des comptes informatiques avait également été publiée. De plus, un processus de contrôle a été instauré pour s'assurer que les recommandations de la directive soient bien mises en place. Actuellement, il y a un projet de refonte de l'Active Directory, qui vise à travailler sur la qualité des comptes, notamment sur leur recertification. Néanmoins, cela ne remplace pas un outil de gestion des identités et des accès (GDIA), qui est nécessaire pour assurer la pérennité et l'automatisation à long terme. Ces mécanismes d'automatisation sont prévus en partie dans ce préavis. Un vrai projet de gestion des identités et des accès à l'échelle d'une administration comme celle de Lausanne se chiffre en millions. Ce préavis vise à établir des premières fondations, notamment vis-à-vis du Provisioning des comptes et de la recertification des comptes.
Pour la recommandation n°8 du rapport, concernant le Programme de formation et sensibilisation à la sécurité informatique, le contenu a déjà été discuté et travaillé avec plusieurs services de la Ville. Une sorte de catalogue de formation et sensibilisation à la sécurité a été créé, pour le personnel mais aussi pour des profils particuliers, tels que ceux des personnes qui travaillent dans les Services industriels, qui ont besoin, en plus de la sensibilisation générale, d'une formation spécifique. Le financement pour mettre en œuvre ce projet est prévu dans ce préavis.

La certification en cours sur le numérique responsable : un préavis va bientôt arriver au Conseil communal qui contiendra les critères utilisés pour octroyer ce label.

Problématiques de sécurité informatique : en termes de protection des données, il sera plus facile et rapide pour des Services qui sont moins en avance de mettre en place un système efficace, que de rectifier des mesures déjà mises en place dans d'autres Services. A propos du risque le plus dangereux et le plus probable, le SOI travaille de manière systématique avec une matrice de risques, où les risques sont classés en termes d'importance. A ce sujet, la Ville tient aujourd'hui un registre où 300 risques ont été documentés et suivis très régulièrement avec des plans d'action. Un risque est un évènement qu'on redoute, qui a un impact et une probabilité d'arriver. D'un côté, des évènements très probables sont, par exemple, le fait qu'un poste de travail soit infecté par un virus, mais si un seul poste est touché, l'impact est minime. D'un autre côté, il y a des évènements très impactants, mais dont la probabilité est très faible. La matrice de risque est tenue à jour en prenant en compte ces deux éléments. De plus, les risques les plus élevés et les plus probables sont essentiellement liés aux comportements des utilisateurs. Il est très difficile de casser les protections techniques que la Ville met en place, mais il est en revanche très simple de tromper un humain. **L'axe de sensibilisation et de formation des collaborateurs de la Ville est donc un axe clé**, car si les gens sont correctement formés, la fenêtre d'ouverture du risque va être réduite.
La prise de conscience récente quant aux enjeux sécuritaires et informatiques montre la nécessité d'investir dans le domaine de la sécurité publique.
En réponse à la question sur le risque quant à la formation Agir des conseillers communaux, il appartient au bureau de faire la demande. Le SOI est à disposition pour une formation.

Collaboration avec le Canton : (DGNSI - Direction Générale du Numérique et des Systèmes d'Information). Il y a bien une collaboration continue avec le Canton. Sur les aspects sécuritaires et informatiques, mais aussi pour tous les autres dossiers qui sont traités au niveau communal et au niveau cantonal, les équipes métier assistées des équipes informatiques en charge de ces solutions-là sont en contact régulier avec le Canton.

[1] Rapport d'audit interne Gestion des accès informatique – Audit de Sécurité informatique
https://www.lausanne.ch/apps/actualites/Next/serve.php?id=13312

Il y aussi des collaborations très concrètes avec le Canton. Par exemple, au travers de son SOC (Security Operation Center), le Canton scanne depuis ses installations ce qui est visible depuis l'Internet de l'extérieur et donne les listes de vulnérabilités qu'il observe à la Ville chaque mois, ce qui permet de se mettre dans la peau d'un hacker et de voir ce qu'il voit afin de corriger les failles constatées avant qu'elles ne soient exploitées. Il y a également eu des échanges avec le Canton afin de déterminer si une mutualisation pour le programme de formation et de sensibilisation était possible, mais que pour l'instant, les fonds nécessaires à ce projet ne sont pas disponibles.

Les deux Data centers à Lausanne vont être déplacés.

Résumé : *« Le montant du présent préavis est revu pour couvrir le périmètre additionnel de protection des données ».* Madame la Municipale explique que les champs sont énormes, et que dans chaque champ, le périmètre qui sera couvert par le préavis a été mis en évidence. Monsieur Hérisson répond également en expliquant que le précédent préavis couvrait seulement le domaine de la sécurité de l'information, tandis que le présent préavis couvre un domaine supplémentaire, celui de la protection des données personnelles.

Etat de lieux – contexte – sécurité de l'informatique industrielle

Beaucoup de choses ont été mises en place lors de ces dernières années. Par exemple il y a 15 ans, les systèmes industriels avec les serveurs se trouvaient sous des bureaux d'opérateurs industriels. De nos jours, tous les serveurs qui pilotent des systèmes industriels se trouvent dans des data centers. Cela illustre les efforts qui ont été fournis. Beaucoup de segmentation a été faite sur les réseaux. A l'époque, il existait un réseau technique sur lequel il y avait le réseau de l'eau, du gaz, de l'électricité. Aujourd'hui, il y a une virtualisation du réseau qui s'est opérée, où les flux sont séparés. De plus, les systèmes d'information qui pilotent tous les réseaux industriels ont reçu beaucoup de pression des gouvernements en Europe, comme aux Etats-Unis et en Suisse, pour amener de la sécurité afin de protéger toutes les organisations que l'on appelle les organisations d'importance vitale. Aujourd'hui, la Ville de Lausanne est considérée comme une telle organisation. Des recommandations claires sont faites et elles sont prises en compte et mises en œuvre avec les Services concernés.
Des coopérations concrètes existent déjà pour un certain nombre d'entités industrielles, telles que pour l'électricité, le chauffage à distance et pour le Service de l'eau. Des analyses de risques poussées sur leurs infrastructures industrielles ont été faites, et un certain nombre de mesures de sécurisation de leurs installations industrielles ont été préconisées. Certaines mesures peuvent être réglées ensemble, tandis que les autres, qui sont liées à la façon des Services de configurer les automates industriels, relèvent plutôt de la responsabilité des Services eux-mêmes. Des formations *ad hoc* des acteurs industriels ont déjà été faites pour les sensibiliser aux bons comportements à adopter. Des contacts sont réguliers avec ces trois services, notamment au sujet du *hardening* (le fait de renforcer les mesures de sécurité en installant les nouveaux systèmes, afin que ceux-ci soient le plus robuste possible dès le départ). Cependant, le but du préavis est de démultiplier les forces, car à partir du 1er janvier 2025, les recommandations de la Confédération vont devenir des obligations, elles ne seront plus optionnelles.
Sur les questions de sécurité et de recommandations qui viennent de la Confédération, ce sont plutôt les Services industriels qui sont contactés. En revanche, pour les questions de sécurité informatique, c'est le SOI qui va être contacté directement pour la mise en œuvre et le suivi. Le SOI et les SIL collaborent sur les deux sujets lorsque des recommandations sont émises.

Bilan du précédent préavis 2015/73 « renforcement de la sécurité des Systèmes d'information pour la période 2016-2019 » : le dernier préavis en date au sujet de la sécurité des Systèmes d'information date de 2016.

Renforcement des systèmes et des solutions informatiques

Concernant l'application Goéland, tant qu'il n'y a pas un outil équivalent fonctionnel, rapide et économique, il s'agit plutôt de faire évoluer Goéland dans sa forme actuelle, afin d'éviter le risque d'obsolescence. Il est nécessaire de se pencher sur ce problème qui n'est pas réglée dans ce préavis.

Sensibilisation et information à la sécurité de l'information

Dans le cursus de formation qui a été prévu, deux dimensions sont présentes. Une première dimension de formation en ligne, qui sera pour tous les collaborateurs sans exception. En complément de cette formation en ligne, des formations en présentiel avec des formateurs ont été prévues pour certains sujets. Ces formations auraient donc un coût en termes de temps et d'argent, et qu'il s'agirait de traiter de thèmes complémentaires à la formation de base à laquelle tout le monde participe. De plus, une insistance est portée sur le fait que chaque année le contenu des formations doit être mis à jour et suivre les évolutions technologiques.
Dans le cadre de ces formations, il est bénéfique de recevoir des rappels de manière régulière.

Sécurité des systèmes d'information industriels

Les montants prévus ne couvrent de loin pas l'ensemble des domaines. Pour chaque domaine, une liste des possibilités est établie en fonction de ce budget.
Pour la partie industrielle, l'apport de l'expertise se fait dans la façon de gérer les problématiques de sécurité. L'essentiel des mesures et des corrections qu'il faut apporter se trouvent au niveau des systèmes industriels eux-mêmes, que ce soient des automates ou des capteurs par exemple. Ce sont donc plutôt les services techniques ou industriels qui doivent reconsidérer leurs manières de faire, où changer leurs équipements.

Protection des données

En termes de protection des données, la démarche est sensiblement similaire à celle pour la sécurité de l'information. Sur le fait que pour la sécurité de l'information, un certain nombre de mesures, avec une analyse de risques, des directives, etc. ont été mises en place. Ces structures documentaires sont quelque peu l'équivalent de cette démarche, mais elles sont orientées sur la protection des données. Au même titre que l'on a une politique de sécurité de l'information, on va avoir une politique de protection des données, ainsi que des directives associées sur la façon de traiter les documents, de les partager.

Impact sur le climat et le développement durable

Etant donné qu'il y a régulièrement des préavis du SOI qui font tous partie d'une même stratégie informatique, peut-être que faire référence aux autres préavis concernant la question de l'obsolescence pourrait aider les conseillères et conseillers à comprendre comment s'intègre un préavis dans la stratégie globale.

Aspects financiers – coûts prévisionnels

Pour déterminer la base des coûts pour ce qui concerne la gestion des identités et des accès, la sensibilisation, et le contrôle de conformité, un appel a été fait auprès d'un certain nombre de sociétés auxquelles ont été demandé des estimations budgétaires. Pour d'autres domaines, tel que le renforcement des socles techniques, le SOI s'est basé sur leurs propres connaissances des prix pour une estimation des coûts par rapport à ce qui était inscrit au plan des investissements.
Il y a peu d'administrations dans le Canton de Vaud qui ont la même taille et les mêmes problématiques. Les moyens humains au Canton affectés à la Sécurité sont 10 fois supérieurs à ceux de la Ville. Cela se traduit aussi au niveau des moyens qui sont affectés.
Pour le préavis sur l'obsolescence par exemple, le Service avait entrepris des *benchmarks* (analyses comparatives) avec le Canton. Il serait intéressant d'entreprendre des *benchmarks* avec les budgets des services informatiques.

Aspects financiers – incidences sur le budget d'investissement

Concernant les dépenses prévues pour 2023, ces dépenses de CHF 320'000.- seront initiées dès 2023 malgré que le préavis ne soit soumis que lors de la 1ère séance du Conseil communal de 2024.

Aspects financiers – incidences sur le budget de fonctionnement

La Ville n'a pas de possibilité d'engager du personnel supplémentaire actuellement. En termes de gouvernance, la Ville tend ces dernières années à mettre l'accent sur la priorisation des objets sur lesquels elle travaille. Il faut travailler à périmètre constant en termes de ressources humaines.

Vœu (adressé aux membres du bureau)

La commission souhaite que le Bureau du Conseil se rapproche du SOI en vue d'une formation des membres du Conseil à la sécurité et protection des données.

Vote : la commission accepte le vœu à l'unanimité.

Conclusions

Une remarque a été exprimée sur la conclusion 2 qui demande de rendre obligatoire des formations. Cette formulation a été validée par le Service du personnel et, sur un sujet de sécurité et de protection, il est utile de rendre cette formation obligatoire, autant pour le personnel de la ville que pour les membres du Conseil.

Les conclusions 1 à 5 ont été votées de manière groupée et ont été acceptées à l'unanimité

Lausanne, le 2 janvier 2024 Magali Crausaz Mottier, rapportrice