



Réponse de la Municipalité à l'interpellation de M. Nicola Di Giulio déposée le 4 octobre 2022

« Les très sensibles données personnelles des Lausannois, ainsi que son data-center(s) sont-ils réellement ultrasécurisés ? »

Lausanne, le 24 octobre 2024

Rappel de l'interpellation

« Pas moins de 450 applications sont stockées, pour au moins 700'000 gigas de données. Parmi celles-ci, les très sensibles données personnelles des Lausannois. Deux data-center(s) hébergent les services nécessaires au fonctionnement de l'Administration communale lausannoise.

Il a l'aspect d'un container anodin de l'extérieur, posé à même le sol, sur l'herbe et clôturé uniquement d'un grillage. Des caméras de surveillance qui pointent du haut des mâts installés semble indiquer que ce que contient le container revêt une valeur incontestable.

Perché à 700 mètres d'altitude, au nord de Lausanne, proche de l'autoroute ce container hors norme d'un poids total de 18 tonnes, accueille un des deux datacenter(s) de la Ville de Lausanne avec à l'intérieur des racks, ces armoires contenant une centaine de serveurs physiques hébergeant les quelque 450 applications utilisées par les services de la ville de Lausanne. Pas moins de 700'000 gigas de données y sont stockées. Une ventilation refroidit en permanence l'ensemble des dispositifs informatiques. Des extincteurs automatiques à l'azote y sont installés ainsi que des batteries qui permettent de suppléer à de brèves coupures d'électricité.

Précieux, ces serveurs agrègent non seulement les applications qui permettent le bon fonctionnement de l'administration, mais aussi les très sensibles données personnelles des citoyens lausannois du contrôle des habitants. Ces données doivent obligatoirement être maîtrisées par la collectivité publique, ils n'en demeurent pas moins qu'à l'heure de la cybercriminalité il est judicieux de pouvoir s'assurer d'une protection optimale. Il est à relever que jusqu'en 2015, les données étaient stockées dans des serveurs disséminés dans divers bâtiments de l'administration communale et en particulier à Chauderon.

Ces anciens data-center(s) étaient forcément grandement énergivores et situés dans des endroits qui n'étaient pas conçus pour cela, souvent vétustes et dans des conditions de sécurité très insuffisantes. Le premier des enjeux était d'identifier un emplacement adéquat en termes d'espace disponible, d'approvisionnement électrique et bien entendu de disponibilité de la fibre optique. Lausanne dispose aujourd'hui de deux centres d'hébergement informatique neufs et sécurisés et qui ne tournent actuellement qu'à 30% de leur capacité. Un chiffre appelé à enfler très rapidement.

A l'échelle de la planète, Lausanne est une bien petite ville. En ce domaine, la tentation est grande de s'en remettre aux solutions de stockage offertes par les multinationales du « cloud » comme Amazon ou Google, avec bien sûr des risques juridiques liés à leur extraterritorialité, mais aussi à l'exploitation induite et commerciale de nos données personnelles. De fait, le bon sens dicte de privilégier le stockage des données sur sol



lausannois, dans des serveurs lausannois. Mais permettez-moi un petit scoop qui n'étonnera pas grand monde : même s'il y a de la marge, ces deux centres de stockage, au vu de l'augmentation vertigineuse des données produites chaque année, seront assez rapidement au maximum de leur capacité.

Elle impliquerait certainement pour une petite ville comme Lausanne de mutualiser ses infrastructures avec d'autres villes, voire d'autres cantons pour créer des data-center(s) collectifs qui permettraient non seulement des économies d'échelle, mais autoriseraient aussi une importante amélioration en termes de sécurité. Néanmoins tout ceci est de la musique d'avenir. »

Introduction

La protection des données du point de vue légal et du point de vue technique est une préoccupation majeure pour la Municipalité. La Ville de Lausanne met en œuvre des processus alignés sur les normes et bonnes pratiques du domaine pour rénover les solutions informatiques et prendre en compte la sécurité de l'information ainsi que la protection des données le plus en amont possible dans chacun des processus.

Plusieurs actions ont été menées depuis des années, elles se poursuivent et se renforcent grâce au crédit d'investissement du préavis N° 2023/47 « Pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026 ». Parmi ces actions, des tests de pénétration sont effectués : les nouvelles applications sont soumises aux techniques des pirates. Avec sa gestion de crise, la Ville se prépare en cas d'attaque. Les dispositifs et technologies mises en œuvre pour parer aux risques évoluent sans cesse et doivent être adaptées en conséquence.

Les cyberattaques ont beaucoup évolué ces dernières années. Elles ciblent particulièrement les pays occidentaux et, de plus en plus, les institutions publiques, en lien avec la situation géopolitique mondiale actuelle.

Les institutions y sont plus sensibles et les dispositions d'accompagnement des administrations s'adaptent et contribuent à relever le niveau de la sécurité en Suisse.

Réponse aux questions posées

La Municipalité répond comme suit aux questions posées :

Question 1 : La Municipalité peut-elle affirmer qu'à l'heure de la cybercriminalité les très sensibles données personnelles des Lausannois, sont-elles réellement ultrasécurisées ?

Des événements récents en lien avec l'Ukraine ont montré que nul n'est à l'abri, il convient de rester humble. Comme indiqué dans le préambule, la Ville engage des actions dans tous les domaines du Système d'information afin de réduire au maximum la surface d'attaque exploitable par les pirates. Un des maillons faibles de la chaîne reste l'humain et c'est ce moyen qui est le plus utilisé pour piéger les particuliers et les institutions. Une campagne de formation et de sensibilisation est en cours de mise en place à l'échelle de la Ville dans le cadre du préavis N° 2023/47 « Pilotage de la sécurité des systèmes d'information et de la protection des données pour la période 2023-2026 ».

Question 2 : La Municipalité peut-elle affirmer que les infrastructures de l'emplacement du data-center(s) situé dans le nord de la Ville de Lausanne, sont-elles suffisamment sécurisées de manière générale, et de manière plus précise au moyen d'un seul et unique grillage (voir photo dans l'initiative) ?

Le local informatique modulaire situé dans le nord lausannois répondait aux normes et risques de sécurité lors de son installation. Comme précisé dans le préambule, les risques cyber ont beaucoup évolué ces derniers temps et les mesures de protection de la Ville sont revues régulièrement. Cependant les salles informatiques sont des infrastructures qui nécessitent des investissements importants et ne peuvent être renouvelées facilement. La Municipalité a pris la décision de déménager ce Data center dans d'autres locaux, plus appropriés, prévus à cet effet et aménagés récemment. Le déménagement a été effectué au début du mois d'octobre 2024, supprimant dès lors le risque mentionné.

Le second local informatique présente toutes les garanties en termes de sécurité physique et de protection des données. Il répond également à tous les critères de durabilité des Data centers (selon l'indicateur Power Usage Effectiveness).

Question 3 : Quelle(s) mesure(s) souhaite prendre la Municipalité le cas échéant pour y remédier ?

Comme expliqué ci-dessus dans la réponse à la question 2, le Data center mentionné a fait l'objet d'un déménagement en 2024.

Question 4 : Y a-t-il une redondance de ces deux data-center(s) au cas où ils seraient détruits ? Quel serait le délai de remise en fonction de cette informatique grâce à la redondance ?

La Ville de Lausanne dispose d'un système d'information réparti dans deux locaux principaux et un troisième local, plus limité, qui héberge des éléments de secours.

Les deux premiers locaux fonctionnent en redondance l'un de l'autre, par conséquent l'arrêt (forcé ou non) d'un des deux locaux n'altère que faiblement la disponibilité des données. L'ensemble du système d'information peut être à nouveau disponible dans un délai d'une journée au maximum.

En cas de destruction complète de ces deux locaux, la Ville de Lausanne dispose d'une sauvegarde des données et doit dérouler un processus de reprise d'activités (PRA ou DRP en anglais, Disaster Recovery Plan). Ce type de reprise est plus long et complexe, et dépend de la capacité des fournisseurs de services et constructeurs à fournir les matériels et services nécessaires.

Il est à noter que les dispositifs de communication (réseaux, accès internet, composants de sécurité) sont gérés dans des locaux différents prévus à cet effet, en redondance.

Question 5 : Ces containers sont-ils sécurisés par un système d'alarme effraction, agression et ouverture sous la menace ?

Les locaux utilisés pour le Data center sont équipés de tous les dispositifs de sécurité et de contrôle d'accès. En particulier, les locaux sont sous alarme, en lien avec un contrat d'intervention sur site 24 heures sur 24 et 7 jours sur 7 d'une société spécialisée dans ce domaine. Le système d'alarme en place est équipé de dispositifs d'alerte en cas d'ouverture sous la menace. De plus les locaux bénéficient d'une vidéosurveillance extérieure et intérieure.

La Municipalité estime avoir ainsi répondu aux questions de M. Nicola Di Giulio.

Ainsi adopté en séance de Municipalité, à Lausanne, le 24 octobre 2024.

Au nom de la Municipalité

Le syndic
Grégoire Junod





Le secrétaire
Simon Affolter

