Réponse de la Municipalité à l'interpellation de M. Samuel Vargas et consorts déposée le 5 septembre 2023

« Incidents en matière informatique, quelles réactions de la Ville ? »

Lausanne, le 5 octobre 2023

Rappel de l'interpellation

« Le 14 juin 2023, les services informatiques de la Ville de Lausanne ont fait l'objet d'une attaque informatique. Cela a notamment eu pour conséquence d'empêcher l'accès au site internet www.lausanne.ch. Dans un courrier adressé en juillet à certains administrés, les Services industriels de Lausanne (SIL) leur ont indiqué qu'un certain nombre de données les concernant avaient été dérobées et s'étaient retrouvées sur internet.

Dans un communiqué du 16 juin 2023, la Municipalité indique que l'attaque informatique du 14 juin 2023 a nécessité la fermeture du site internet www.lausanne.ch en application du principe de précaution. Par ailleurs, des analyses de la cellule de crise mise sur pied à cette occasion ont permis d'écarter une intrusion ou un vol de données. Il est aussi indiqué que cette cellule a mis en place un dispositif d'alerte permettant de détecter un éventuel redémarrage de l'attaque.

Le 14 juillet 2023, les SiL ont informé des usagères et des usagers de leurs services que certaines de leurs données sensibles avaient été piratées et avaient été disponibles sur internet durant trois semaines ».

Préambule

Le mercredi 14 juin 2023, le site www.lausanne.ch a subi une attaque de type « déni de service distribué (DDoS) » visant à saturer le site et à le rendre indisponible. Une cellule de crise a immédiatement été activée au sein de l'administration en collaboration avec les services compétents de la Confédération. Le site de la Ville a été mis hors service par précaution avec un retour à la normale à partir du 16 juin 2023 au matin. Une réplique de cette attaque a eu lieu le 18 juin 2023, mieux contenue, mais avec les mêmes conséquences. Le retour à la normale s'est fait le 19 juin 2023 au matin. Dans les deux cas, les activités opérationnelles de la Ville n'ont pas été directement touchées. En outre, il n'y a eu ni tentatives d'intrusion ni vols de données. Les attaques ont été revendiquées par le groupe de pirates russes NoName057 et a eu lieu dans le contexte de la rencontre par vidéoconférence du 15 juin 2023 entre le Parlement suisse et le président ukrainien. Les sites d'autres villes suisses ont subi des attaques comparables.

Le lundi 10 juillet 2023, une faille de sécurité a été identifiée sur le site www.equiwatt.ch/lausanne, qui n'est pas hébergé sur les infrastructures de la Ville. La faille était contenue dans le code source et pouvait mener à des données personnelles de personnes ayant demandé des subventions et participé à un concours.

Cette faille a été ouverte suite à une modification informatique du site réalisée le 22 juin 2023. Au vu de cette découverte, il a été identifié que des données personnelles avaient donc pu être théoriquement exposées à des tiers entre ces deux dates, soit durant 18 jours.

Toutefois, aucune consultation et aucun téléchargement de ces données n'a été établi à ce jour et aucune utilisation de ces dernières n'a été rapportées aux SIL. La faille de sécurité a été comblée immédiatement une fois connue. Conformément aux obligations légales, tous les clients concernés ont été avertis. Comme mentionné précédemment, il semble que la faille soit passée inaperçue auprès de personnes mal intentionnées, et qu'aucune donnée n'ait été volée.

Les procédures de sécurité ont été renforcées suite à cet incident, qui a été dûment signalé à l'Autorité cantonale de protection des données et de droit à l'information.

La Municipalité relève encore que les deux incidents ne sont pas liés : le premier est le fruit d'un acte malveillant, le second d'une erreur humaine identifiée de manière indépendante.

Réponse aux questions posées

La Municipalité répond comme suit aux questions posées :

Question 1 : Combien de personnes sont concernées par le vol de données des SiL?

Comme indiqué en introduction, il n'y a pas eu, à la connaissance de la Municipalité, de vol de données. La faille sur le site équiwatt a potentiellement exposé des données personnelles de 2'658 personnes.

Question 2 : Quelles sont les bases de données des SiL qui ont fait l'objet de l'attaque?

Comme indiqué en introduction, il ne s'agit pas d'une attaque, mais d'une faille de sécurité ouverte suite à une mise à jour informatique du site www.equiwatt.ch. En passant par le code source de la page, il était possible d'atteindre un fichier contenant les données personnelles de 2'400 personnes ayant participés à des concours et de 258 personnes ayant fait une demande de subventions.

Question 3 : Quelles ont été les mesures prises à la suite de l'incident survenu aux SIL ?

La faille de sécurité a été immédiatement comblée par les collaborateurs des SIL en charge du site équiwatt. Une cellule de crise a été constituée sous la supervision du Service d'organisation et d'informatique (SOI), qui a mis à disposition son savoir-faire pour gérer une telle crise, ainsi que ses modèles et procédures. Les personnes concernées ont rapidement été averties par email et par lettre. Une hotline avec un numéro dédié a été mise à disposition des personnes exposées, de même qu'une adresse email dédiée. L'Autorité cantonale de protection des données et de droit à l'information a été avertie et tenue au courant de l'évolution de la situation.

En parallèle, les formulaires de demandes de données personnelles ont été revus, de même que le processus interne de gestion et de stockage, afin d'être plus sécurisés.

La procédure d'évolution du site internet équiwatt a aussi été revue et fera désormais systématiquement l'objet d'un audit de sécurité.

Question 4 : Le vol de données de clients des SIL est-il lié à l'attaque informatique du 14 juin 2023 ?

La faille de sécurité sur le site équiwatt, dont aucun vol de données n'a résulté à la connaissance de la Municipalité, est sans lien avec les attaques informatiques des 14 et 18 juin 2023. Le site n'est en outre pas hébergé sur les infrastructures de la Ville.

Question 5 : En cas de réponse positive à la question 4, pourquoi la Municipalité n'a-t-elle pas communiqué publiquement à ce sujet ?

Question sans objet.

Question 6 : En cas de réponse positive à la question 4, comment se fait-il que le vol de données des SIL n'a pas pu être identifié avant la parution du communiqué du 16 juin 2023 ?

Question sans objet.

Question 7 : En cas de réponse négative à la question 4, pourquoi la Municipalité n'a-t-elle pas communiqué publiquement au sujet de l'attaque étant survenue aux SIL ?

La Municipalité n'a pas souhaité communiquer publiquement sur la faille de sécurité du site équiwatt pour ne pas attirer l'attention d'individus malveillants sur ce site, ni les encourager à tester sa robustesse. Les personnes concernées et l'autorité de surveillance ont été informées.

Question 8 : En cas de réponse négative à la question 4, comment se fait-il que le dispositif d'alerte mis en place à l'issue de l'attaque du 14 juin 2023 n'ait pas empêché le vol de données survenu aux SIL ?

Il n'a y pas eu vol de données, ni attaque ou intrusion du site équiwatt, mais l'identification, avant une conséquence de ce type, d'une faille dans le codage du site. La question semble donc sans objet.

Question 9 : De manière générale, quelles ont été les mesures prises à la suite à ces incidents en matière de sécurité informatique ?

Ces incidents ont permis de tester les processus internes de mise en place d'une cellule de crise. Les enseignements de ces deux crises ont été tirés. Le renforcement de la sensibilisation de l'ensemble des collaborateurs gérant des informations et particulièrement des données personnelles est aussi nécessaire et se met en place : la sécurité de l'information n'est pas qu'un problème informatique. Pour le surplus, il est renvoyé à la réponse de la question 3.

La Municipalité estime avoir ainsi répondu aux questions des interpellateurs.

Ainsi adopté en séance de Municipalité, à Lausanne, le 5 octobre 2023.

Au nom de la Municipalité

Le syndic
Grégoire Junod

Le secrétaire
Simon Affolter

MUNICIPALITÉ DE LAUSANNE