Ville de Renens
Une différence créative

MUNICIPALITÉ

RÉPONSE ÉCRITE

à l'interpellation de Monsieur le Conseiller communal Luis Guedes relative à la protection des données personnelles

Renens, le 20 janvier 2025

Monsieur le Président,
Mesdames les Conseillères communales, Messieurs les Conseillers communaux,

En date du 3 octobre 2024, M. le Conseiller communal Luis Guedes a interpellé la Municipalité au sujet de la protection des données personnelles depuis l'introduction de Microsoft Authenticator pour assurer l'authentification sur les systèmes informatiques de la Ville. M. Guedes souligne une certaine inquiétude générale de la part du législatif vis-à-vis de l'imposition d'une application externe et potentiellement intrusive sur des appareils privés. Sur cette base, il invite la Municipalité à organiser une séance d'information relative à ces questions en marge du Conseil communal.

En préambule, la Municipalité rappelle que l'environnement géopolitique actuel incite à la prudence, et donc à des mesures de protection pour les outils connectés – outils garants du bon fonctionnement du travail de l'exécutif et du législatif, des services communaux et plus largement de la société dans laquelle nous vivons. Les exemples récents des piratages de la Ville de Montreux ou du groupe VidyMed illustrent la recrudescence et l'impact des cyberattaques en Suisse.

Trouver le juste équilibre entre la protection des données personnelles d'une part et de l'infrastructure informatique communale de l'autre reste donc un défi complexe. Dans ce contexte, l'utilisation de Microsoft Authenticator ne représente qu'une facette des multiples contraintes d'authentification qui rythment notre quotidien (prestations en ligne, paiements bancaires, configuration d'un téléphone portable, etc.). La Municipalité est donc consciente que l'utilisation d'un outil supplémentaire peut générer tension et questionnement. S'appuyant sur l'expertise du Service informatique, elle fait cependant le constat qu'en l'état, aucune meilleure solution n'a pu être identifiée pour garantir la sécurité de l'infrastructure numérique communale.

La Municipalité apporte dès lors la réponse suivante à ladite interpellation :

Le Service informatique est chargé de monitorer et renforcer la sécurité des systèmes informatiques de la Ville notamment face à l'intensification des cyberattaques.

Afin d'atteindre les objectifs précités, la mise en place d'une authentification à deux facteurs (2FA) est l'une des mesures de sécurité les plus efficaces en matière de protection des comptes utilisateurs et des données. Il s'agit d'un outil majeur pour garantir l'intégrité des systèmes communaux.

./..

1. Utilisation de Microsoft Authenticator

Microsoft Authenticator est une solution gratuite qui ne nécessite pas d'abonnement payant ni de licence Microsoft 365. De plus, l'application peut être utilisée pour l'authentification 2FA d'autres systèmes que celui de Microsoft. Les solutions open source, bien qu'elles soient également gratuites, posent parfois des problèmes en matière d'intégration dans un écosystème préalablement établi. En effet, l'authentification est un domaine extrêmement sensible qui doit être continuellement surveillé, mis à jour et audité pour répondre aux enjeux des cybermenaces.

L'avantage de Microsoft Authenticator réside dans le fait qu'une équipe de Microsoft est dédiée à la mise à jour du système, à son évolution et son maintien aux normes de sécurité – à contrario d'autres solutions open source qui peuvent nécessiter une expertise technique continue, des configurations spécifiques ou encore un support technique supplémentaire pour en assurer la sécurité.

2. Collecte des données par Microsoft Authenticator

Microsoft Authenticator ne collecte ni n'exploite les données personnelles à des fins commerciales. En effet, l'application est conçue pour accéder uniquement aux informations strictement nécessaires pour confirmer l'identité de l'utilisateur sans interférer avec les données personnelles. Les informations utilisées, à savoir les données d'authentification, sont stockées localement sur l'appareil et ne sont pas transmises à Microsoft. De plus, ce dernier a mis en place des politiques de confidentialité et de sécurité strictes quant aux données de l'utilisateur.

Les informations collectées pour l'authentification sont les suivantes :

- localisation : il est nécessaire de connaitre le pays et les coordonnées GPS depuis lesquels la demande émane afin de déterminer si la requête pour accéder à la source protégée est recevable. Aucune de ces informations n'est transmise à Microsoft. Seul le nom du pays peut être envoyé à l'administrateur (à savoir le Service informatique de la Ville), pour analyse si besoin ;
- clés secrètes et identification de comptes : stockées localement sur l'appareil de l'utilisateur et chiffrées, ces données ne sont en aucun cas transmises à Microsoft ;
- sauvegarde des données (optionnelle) **:** si l'utilisateur active la sauvegarde, les données seront chiffrées et sauvegardées sur le cloud. Par défaut, rien n'est actif ;
- données de diagnostic : collectées de manière anonymisées pour améliorer le service et garantir la sécurité, les données de diagnostic sont conservées pour une courte période et peuvent être désactivées par l'utilisateur ;
- caméra : l'accès à la caméra est utilisé uniquement pour scanner les QR codes. Les droits d'accès à ce périphérique sont contrôlables par l'utilisateur ;
- sécurité des données : les données stockées localement sont cryptées selon la norme AES[1].

3. Conservation des données

Microsoft Authenticator conserve les données tant que l'application est utilisée. Les données d'authentification, qui sont notamment les identifiants de comptes ainsi que les secrets nécessaires pour générer les codes d'authentifications, sont régis selon deux principes fondamentaux :

1. conservation locale : ces données sont stockées uniquement sur l'appareil en question et ne sont pas transmises à Microsoft. Cela signifie que la durée de vie de ces informations est liée à l'utilisation de cette application. Ainsi, si elle est supprimée, les données seront effacées de l'appareil ;
2. non-centralisation : l'application ne stockant pas de mots de passe ou de secrets de manière centralisée, il n'y a aucune période de conservation spécifique pour ces informations sur les serveurs de Microsoft étant donné qu'elles ne sont pas envoyées.

[1] Le cryptage AES, ou Advanced Encryption Standard, est un type de cryptage (méthode de transformation d'un message pour en dissimuler le sens) qui protège le transfert de données sur Internet. Son utilisation fait référence au niveau international.

Les données de diagnostics, qui sont contrôlables manuellement, sont quant à elles anonymisées et conservées pour des courtes périodes à des fins statistiques et de sécurité.

Microsoft garantit la suppression et l'anonymisation des données afin de s'assurer que ces dernières ne soient pas conservées plus longtemps que nécessaire et éviter ainsi de pouvoir identifier un utilisateur après une collecte. De plus, les usagères et usagers ont la possibilité de supprimer les données via l'application ou via leur compte Microsoft.

4. Protections et conformités renforcées

Contrairement à d'autres applications, Microsoft Authenticator ne stocke pas les mots de passe des utilisatrices et des utilisateurs sur des serveurs distants ni sur l'appareil lui-même. Seuls les éléments nécessaires à la génération des codes OTP (clés de configurations) sont stockés et sécurisés avec un cryptage fort.

De plus, des mécanismes complémentaires de sécurité sont mis en place sur les appareils qui le peuvent, pour isoler et protéger les données d'authentifications critiques. Cela empêche même une application malveillante présente sur le même appareil d'accéder à ces informations.

En ce qui concerne Microsoft de manière générale, l'entreprise respecte les lois sur la protection des données pour en déterminer la durée de conservation, notamment les lois Suisse et Européennes respectivement la LPD (Loi fédérale sur la protection des données) et le RGPD (Règlement européen sur la protection des données). De plus, le fait que l'hébergement de nos données soit en Suisse, à Gland, offre une meilleure conformité aux exigences suisses en matière de souveraineté de nos données.

Pour finir, il est également à noter que Microsoft procède régulièrement à des audits de conformité pour ses différents services. De plus, il dispose de nombreuses certifications de sécurité comme SOC 1,2,3 (normes en matière de cybersécurité), ISO 27001 (sécurité des systèmes d'informations) et 27018 (protection des données).

5. Alternative à Microsoft Authenticator

Au sein de la présente interpellation, il est fait mention d'un échange avec le Chef du service informatique de la Ville concernant la sécurité des données. En complément aux éléments mentionnés dans l'interpellation, il est important de préciser le fait que la sécurité des données est présente dans le nouveau système 2FA et qu'il n'y a pas d'informations collectées, tel qu'expliqué plus haut. En revanche, le risque zéro ne peut être garanti.

Sur la base des informations fournies ci-dessus, les membres du Conseil communal qui ne souhaitent pas utiliser Microsoft Authenticator peuvent faire une demande au Service informatique pour pourvoir utiliser un système alternatif, la clé FIDO. Cette solution, qui se présente la plupart du temps sous la forme d'une petite clé USB, permet une authentification forte sans passer par une application sur un smartphone tout en offrant un niveau de sécurité extrêmement élevé et un usage facilité.

La demande peut être faite en prenant contact avec le Service informatique par courriel à l'adresse informatique@renens.ch ou par téléphone au 021 632 78 00.

./.

6. Séance d'information

Une intervention du Chef du service informatique suivie d'un échange sur cette thématique sera planifiée en préambule d'une future séance du Conseil communal. La date ainsi que le mode d'organisation seront communiqués lors de la prochaine séance du plénum.

7. Sources d'informations

- Déclaration de confidentialité de Microsoft | https://www.microsoft.com/fr-fr/privacy/privacystatement
- Microsoft et RGPD | https://www.microsoft.com/fr-ch/trust-center/privacy/gdpr-overview
- FAQ sur Microsoft Authenticator | https://support.microsoft.com/fr-fr/account-billing/faq-sur-microsoft-authenticator-12d283d1-bcef-4875-9ae5-ac360e2945dd

---

La Municipalité considère avoir répondu à l'interpellation de Monsieur le Conseiller communal Luis Guedes relative à la protection des données personnelles.

Au nom de la Municipalité

Le syndic
Jean-François Clément

MUNICIPALITÉ DE RENENS
LIBERTÉ ET PATRIE

Le secrétaire municipal
Michel Veyre