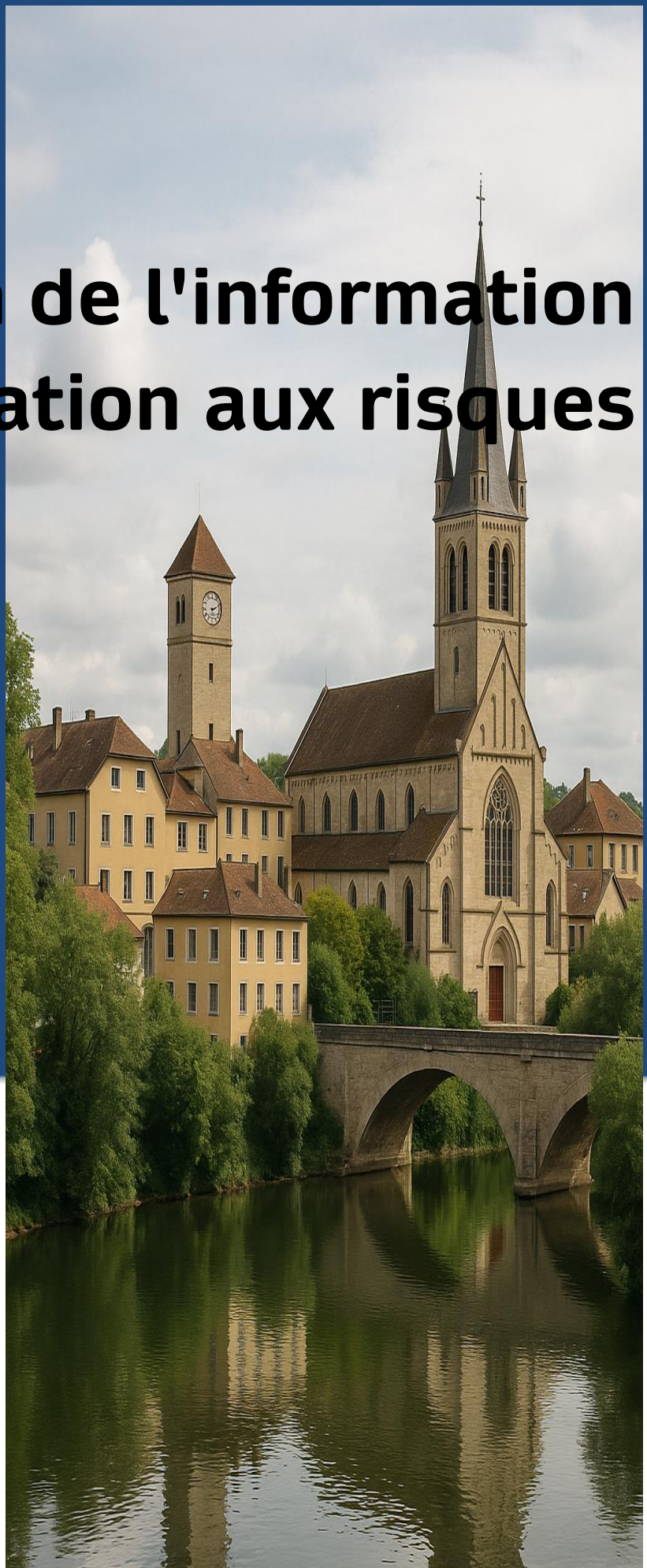
Sécurisation de l'information et sensibilisation aux risques numériques

Cas de la commune de Belleville – Réponse à un incident de fuite de données fiscales



Rapport réalisé par

Pupal Mazamel
Annamammedov Ruslan
Duval Jean-Louis

Haute école de gestion
Genève

Module
63-22

Table des matières

1 CONTEXTE ET ANALYSE DE L'INCIDENT 3

1.1 RÉSUMÉ DE L'INCIDENT 3
1.2 ACTIONS IMMÉDIATES À ENTREPRENDRE 4
1.3 ANALYSE DES RISQUES – MÉTHODE EBIOS RISK MANAGER 5
Atelier 1 — Cadrage et socle de sécurité 5
Atelier 2 — Sources de risque 5
Atelier 3 — Scénarios stratégiques 5
Atelier 4 — Scénarios opérationnels 5
Atelier 5 — Traitement du risque 6
1.4 MATRICE DE FARMER (IMPACT / PROBABILITÉ) : 6

2 GOUVERNANCE ET SÉCURISATION DU SI 7

2.1 ÉLABORATION DE LA PSSI 7
2.1.1 Objectifs 7
2.1.2 Cycle PDCA 8
2.1.3 Gouvernance interne 8
2.1.4 Accès et RBAC 9
2.1.5 Sauvegardes 9
2.1.6 Conformité ISO/LPrD 10
2.2 SÉCURISATION DE L'INFRASTRUCTURE 10
2.2.1 Authentification forte & MFA 11
2.2.2 Chiffrement (AES, TLS) 11
2.2.3 Pare-feux, logs, SIEM 11
2.2.4 Journaux (logs) 12
2.2.5 Segmentation du réseau & gestion des accès 12
2.2.6 Complément : MFA, FIDO2 et AGOV 13
2.2.7 Conclusion 14

3 SENSIBILISATION, COMMUNICATION ET RÉPONSE HUMAINE 15

3.1 SITUATION ACTUELLE 15
3.2 CAMPAGNE DE SENSIBILISATION 16
3.2.1 Objectif principal 17
3.3 MISE EN ŒUVRE DE LA CAMPAGNE DE SENSIBILISATION 17
3.4 COMMUNICATION ET GESTION DE RISQUE 21
3.4.1 Communication externe - citoyens et partenaires 21
3.4.2 Communication interne – collaborateurs 22
3.4.3 Conclusion 23

1 Contexte et analyse de l'incident

1.1 Résumé de l'incident

La commune de Belleville a subi une grave violation de données, entraînant la divulgation publique des déclarations fiscales de ses contribuables. Cette fuite d'informations sensibles constitue une atteinte majeure à la confidentialité des données personnelles et fiscales des habitants.

L'origine de cette brèche pourrait être liée à plusieurs facteurs. D'une part, les applications métier (finances, fiscalité, etc.) utilisées par la commune sont hébergées en mode SaaS par l'Association des Communes Vaudoises. Il est donc possible qu'une faille de sécurité soit survenue du côté du prestataire. D'autre part, la commune ne dispose d'aucun responsable dédié à la sécurité des systèmes d'information (**CISO ou RSSI**), ce qui affaiblit considérablement sa posture de cybersécurité.

La sécurité est actuellement reléguée à l'équipe informatique, déjà engagée sur d'autres tâches opérationnelles, ce qui ne permet ni une surveillance proactive des risques, ni la mise en place de bonnes pratiques ou de plans de prévention efficaces. Ce manque de gouvernance en sécurité informatique favorise les erreurs humaines (telles que le phishing) et augmente la probabilité d'attaques ciblées (par exemple, sur site ou par exploitation d'accès distants).

Conséquences :

- Compromission de données fiscales confidentielles
- Atteinte à la vie privée des habitants
- Risques accrus d'usurpation d'identité ou de fraude
- Dégradation de la confiance des citoyens envers l'administration
- Impact négatif sur la réputation de la commune au niveau cantonal

Cet incident met en évidence l'urgence de structurer et professionnaliser la gestion de la sécurité de l'information au sein de la commune, en instaurant notamment une politique de sécurité, une analyse des risques et des actions de sensibilisation à destination de l'ensemble du personnel.

1.2 Actions immédiates à entreprendre

Face à la gravité de la fuite de données fiscales, plusieurs actions urgentes doivent être menées afin de contenir l'incident et d'en limiter les conséquences :

1. **Isolation du système compromis** : Il est impératif d'isoler immédiatement tout système ou service potentiellement compromis, même si cela implique de suspendre temporairement l'accès aux applications concernées (notamment les services SaaS liés à la fiscalité). Cette mesure vise à éviter toute propagation de l'attaque et à préserver les preuves nécessaires à l'enquête.

2. **Notification du fournisseur** : SaaS Le prestataire (l'Association des Communes Vaudoises) doit être informé sans délai de l'incident. Il pourra ainsi analyser ses propres systèmes, appliquer les correctifs nécessaires et déterminer si l'origine de la brèche se situe de son côté ou s'il existe un impact plus large touchant d'autres communes.

3. **Investigation technique interne** : Une analyse des journaux d'activité (logs) des systèmes locaux doit être lancée pour identifier la source de l'attaque, le vecteur d'intrusion utilisé, et évaluer si d'autres postes ou serveurs internes ont été touchés (ex : installation de malwares, rebond d'attaque, exfiltration supplémentaire de données).

4. **Notification à l'autorité cantonale** : Conformément à la Loi sur la Protection des Données (LPrD), l'incident doit être notifié rapidement au préposé cantonal à la protection des données. Cette démarche est indispensable pour assurer la conformité légale et permettre une gestion transparente de la crise.

5. **Communication contrôlée :** Préparer une communication officielle destinée aux citoyens et aux parties prenantes, reconnaissant l'incident, présentant les premières mesures prises, et rassurant quant à la volonté de renforcer la sécurité à l'avenir. Cette étape est cruciale pour limiter l'impact réputationnel.

6. **Réévaluation des accès sensibles** : Il est important de réévaluer les portes de sorties des informations qui ont été compromises afin de s'assurer qu'une autre attaque de ce type ne puisse pas se représenter.

7. **Conservation des preuves numériques** : Ne pas éteindre ou redémarrer les machines affectées afin de conserver le plus de trace possible de l'incident, ne pas les formater ou les modifié même si elles cessent de fonctionner pour les mêmes raisons.

1.3 Analyse des risques – Méthode EBIOS Risk Manager

Atelier 1 — Cadrage et socle de sécurité

Dans le cadre de la sécurisation du système d'information de la commune de Belleville, nous avons réalisé une analyse des risques en suivant la méthode EBIOS RM, en déroulant les cinq ateliers proposés dans sa démarche.

- Nous avons commencé par définir les éléments essentiels du contexte : Les services critiques (fiscalité, finances, contrôle des habitants, RH) sont opérés en mode SaaS, mais le matériel, les accès et les sauvegardes sont gérés localement. Il n'existe aucun rôle formel en cybersécurité. La protection des données repose donc sur un effort diffus, sans pilotage, ni doctrine claire.
- Les objectifs de sécurité prioritaires sont clairs : empêcher l'accès non autorisé aux données fiscales, maintenir la continuité des services, préserver l'intégrité des informations sensibles, et être capable de tracer les actions et anomalies.

Atelier 2 — Sources de risque

- Les sources de risques principales sont humaines (employés mal informés, erreurs d'usage, comptes mal gérés) et externes (cybercriminels profitant de failles dus au manque de formations du personnel ou du manque de direction distincte, voir d'un manque de surveillance interne).
- Le manque de sensibilisation, l'absence de gestion structurée des identités, et la dépendance à un prestataire externe sans clauses contractuelles de sécurité sont des facteurs aggravants. Ces éléments créent un terrain propice aux incidents, même sans attaque sophistiquée.

Atelier 3 — Scénarios stratégiques

- Plusieurs scénarios stratégiques ont été étudiés à l'échelle de l'écosystème de la commune, notamment :
  - Un acteur externe exploite une faille dans le SaaS pour extraire les données fiscales de l'ensemble des habitants.
  - Un attaquant réussit à compromettre les accès d'un utilisateur légitime grâce à une campagne de phishing bien ciblée.
  - Des informations confidentielles sont publiées en ligne par erreur, sans qu'aucune alerte n'en signale la fuite.
- Ces scénarios démontrent que la commune est exposée à des actions ciblées, amplifiées par la centralisation des services SaaS et l'absence de supervision technique.

Atelier 4 — Scénarios opérationnels

- Sur le plan local, deux scénarios opérationnels ont été choisis car probables :
  - Un ancien compte utilisateur non désactivé est réutilisé pour accéder au système fiscal. Ce cas illustre un manque de gestion des comptes et des droits.

- Un employé clique sur un lien piégé et installe malgré lui un malware, qui permet un accès distant aux données sensibles. Ce scénario reflète l'absence de sensibilisation des collaborateurs et de protection des systèmes d'informations.

- Ces cas révèlent des failles dans l'organisation quotidienne : pas de gestion des habilitations, pas d'authentification renforcée, ni de système d'alerte en cas d'activité anormale.

Atelier 5 — Traitement du risque

- Les traitements recommandés sont orientés vers une sécurisation poussée :
  - **Créer un rôle clair de référent sécurité**, même à temps partiel, pour piloter les priorités, suivre les incidents et s'assurer du respect des différentes solutions mis en place.
  - **Mettre en place une politique de sécurité simple et adaptée**, intégrant les besoins réels et les capacités de la commune.
  - **Renforcer les accès** : suppression systématique des comptes inactifs, MFA pour les services SaaS, gestion des rôles.
  - **Surveiller l'activité** : journalisation centralisée, alertes en cas de comportements inhabituels.
  - **Former les agents** à repérer les attaques courantes (phishing, comportements suspects).
  - **Imposer des clauses de sécurité** dans les contrats SaaS, incluant des audits et des engagements LPrD.

1.4 Matrice de Farmer (impact / probabilité) :

Menaces potentielles :

1. Attaque complémentaire sur notre système
2. Dénis de service
3. Vol d'autres données sensibles
4. Destruction de matériel
5. verrouillage de fichier important

Probabilité ↑	minime	moyen	Fort	Extreme	Impact →
Certain			3		
Probable			1	5	
Improbable		2		4	
Presque null					

Mitigations :

1. Couper le système du réseau global le temps de mettre en place une stratégie de sécurité.
2. Renforcé / mettre en place des sécurités sur l'utilisation de bots /zombies
3. Mettre en place des normes plus stricte de droits d'accès
4. Vérifié que les appareils potentiellement infectés ne le soient plus et si c'est le cas, les nettoyer en urgence.
5. Faire des backups des données par ordre d'importance.

↑ Probabilité	minime	moyen	Fort	Extreme	→ Impact
Certain					
Probable					
Improbable		5	3		
Presque null		2	1	4	

2 Gouvernance et sécurisation du SI

2.1 Élaboration de la PSSI

2.1.1 Objectifs

La politique de sécurité du système d'information a pour objectif de garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations traitées au sein de l'administration, tout en respectant les exigences de la Loi sur la Protection des Données et les normes internationales, notamment **ISO 27001** versions de 2022.

2.1.2 Cycle PDCA

Dans ce contexte, il est pertinent de proposer que Belleville adopte une approche fondée sur l'amélioration continue, en suivant les principes du cycle Plan-Do-Check-Act recommandés par **ISO 27001**.

Cette démarche permet d'identifier les risques de manière proactive et d'adapter les contrôles existants aux nouvelles menaces. La politique devient ainsi un outil stratégique au service de la bonne gouvernance des systèmes d'information, renforçant la confiance des citoyens dans la gestion numérique de la commune.

2.1.3 Gouvernance interne

Parmi les défis à prendre en compte figure l'absence actuelle de personnel spécialisé en cybersécurité. Il serait judicieux de répartir provisoirement les responsabilités entre deux fonctions internes en attendant un renforcement des ressources humaines.

Un délégué à la sécurité, désigné au sein du personnel existant, peut assurer la mise en œuvre technique des mesures de sécurité ainsi que la coordination des actions en cas d'incident. Quant à la supervision globale de la politique, elle peut être confiée au secrétaire communal, chargé de veiller à l'alignement des mesures avec les orientations stratégiques de la commune et les exigences légales.

2.1.4 Accès et RBAC

Un axe prioritaire à développer dans cette politique concerne la gestion des accès aux systèmes d'information. Pour limiter les risques liés à l'erreur humaine ou à l'abus de privilèges, un modèle de contrôle basé sur les rôles RBAC peut être mis en place.

Chaque collaborateur accède uniquement aux données nécessaires à l'exercice de ses fonctions. Par exemple, un employé des ressources humaines n'accède pas aux dossiers fiscaux, et inversement.

Les droits d'accès doivent faire l'objet d'une revue périodique, et tout compte resté inactif pendant plus de trente jours peut être automatiquement verrouillé. Ce contrôle est complété par des mesures d'authentification forte, comme des mots de passe complexes et une vérification en deux étapes pour les applications sensibles.

2.1.5 Sauvegardes

En parallèle, il est pertinent de mettre en œuvre une stratégie rigoureuse de sauvegarde et de restauration des données. Toutes les informations critiques sont sauvegardées quotidiennement avec une double redondance : les copies sont stockées localement sur les serveurs de la commune et externalisées vers une infrastructure cloud sécurisée.

Un test de restauration mensuel garantit l'efficacité du dispositif. Ces pratiques s'inscrivent dans les principes d'accountability (responsabilisation et traçabilité) promus par la norme **ISO 27001** et permettent d'assurer la continuité des activités en cas de sinistre.

2.1.6 Conformité ISO/LPrD

La conformité représente un pilier fondamental de la politique de sécurité. Il est essentiel de respecter la législation cantonale et fédérale, tout en documentant les procédures liées à la sécurité et en conservant les preuves d'exécution (journaux d'accès, rapports d'incidents, audits internes).

En cas d'incident ou de changement organisationnel, la PSSI doit être révisée pour intégrer les enseignements tirés. Un mécanisme de revue annuelle formelle permet de maintenir la pertinence du document dans le temps.

Enfin, la sensibilisation des utilisateurs joue un rôle clé dans cette démarche. Même bien conçue, une politique reste inefficace sans une appropriation collective. Des actions régulières de formation et de sensibilisation peuvent être planifiées afin de renforcer la culture de la sécurité dans tous les services communaux.

2.2 Sécurisation de l'infrastructure

La sécurisation de l'infrastructure informatique de la commune de Belleville peut reposer sur une approche en couches, afin de protéger les systèmes et les données à plusieurs niveaux, de manière cohérente et complémentaire.

Ces mesures peuvent être conçues pour répondre aux besoins d'une petite administration sans département IT spécialisé, tout en intégrant les bonnes pratiques définies par la norme **ISO 27002** dans sa version 2022. Chaque couche joue le rôle d'une barrière de protection supplémentaire, allant de l'authentification des utilisateurs à la gestion des données dans le cloud.

2.2.1 Authentification forte & MFA

Une première étape pertinente de cette sécurisation concerne l'authentification. Dans le contexte actuel, les simples mots de passe ne suffisent plus à garantir un niveau de sécurité satisfaisant.

Il est alors possible de mettre en place une politique d'authentification forte. Les mots de passe doivent respecter des critères stricts de longueur, de complexité et d'unicité, avec un renouvellement obligatoire tous les 90 jours.

En complément, un système d'authentification multi-facteur (MFA) peut être instauré pour l'accès aux applications sensibles, notamment celles contenant des données fiscales et RH. Ce mécanisme vise à bloquer les tentatives d'accès non autorisées, même en cas de compromission du mot de passe.

2.2.2 Chiffrement (AES, TLS)

Le chiffrement représente une autre couche essentielle. Il convient de chiffrer toutes les données sensibles stockées localement (ex. documents fiscaux, fichiers RH) à l'aide de l'algorithme AES avec une clé de 256 bits, en utilisant des outils standardisés tels qu'OpenSSL.

Les communications avec les services SaaS de l'association des communes vaudoises peuvent être protégées via le protocole TLS, assurant la confidentialité et l'intégrité des données échangées. Le recours systématique au chiffrement permet de limiter les risques d'exposition en cas d'intrusion ou de vol de matériel.

2.2.3 Pare-feux, logs, SIEM

Pour le périmètre réseau, l'utilisation d'un pare-feu logiciel installé sur les serveurs peut constituer une mesure simple et efficace. Ce pare-feu, n'ouvre que les ports strictement nécessaires au fonctionnement des services, et bloque toute tentative de connexion non autorisée, en les consignant dans des journaux. Cette configuration offre à Belleville un moyen de contrôle des flux réseau sans investissement important.

2.2.4 Journaux (logs)

La journalisation des événements représente une composante clé de la détection des incidents. Les fichiers de logs tels que auth.log, les rapports de connexion SSH ou d'autres documents similaires permettent de retracer clairement l'activité sur les systèmes. Ces journaux peuvent être centralisés dans une solution de type SIEM (Security Information and Event Management).

En ce qui concerne l'usage du cloud, Belleville peut s'appuyer sur des services SaaS fournis par une association intercommunale. Même si la commune ne contrôle pas directement cette infrastructure, un devoir de vigilance s'impose. Il est donc pertinent d'exiger la transmission régulière des journaux d'activité relatifs aux données communales, afin d'en permettre l'analyse. Cette collaboration contribue à maintenir une visibilité suffisante sur les opérations effectuées à distance.

2.2.5 Segmentation du réseau & gestion des accès

La gestion des droits d'accès au sein du réseau local peut reposer sur une stricte séparation des zones. Par exemple, les données fiscales, particulièrement sensibles, peuvent être hébergées sur une infrastructure logicielle distincte de celle utilisée pour les ressources humaines ou les services techniques. Cette segmentation du réseau limite la propagation potentielle d'un incident et isole les systèmes critiques.

En parallèle, l'accès des employés aux ressources peut être limité à celles strictement nécessaires à leurs tâches, en appliquant le principe du moindre privilège.

2.2.6 Complément : MFA, FIDO2 et AGOV

Dans le cadre de cette sécurisation, il peut être utile de revenir sur l'authentification forte et d'en souligner l'importance croissante. Le MFA repose sur la nécessité de présenter au moins deux types de preuves pour accéder à un système: un élément que l'utilisateur connaît (mot de passe), un qu'il possède (téléphone ou token), ou une caractéristique biométrique (empreinte digitale, reconnaissance faciale).

La combinaison de ces facteurs réduit significativement les risques d'usurpation d'identité ou d'accès non autorisé. Dans sa stratégie de sécurité, Belleville peut ainsi appliquer le MFA en combinant un mot de passe robuste à un second facteur, comme un code à usage unique généré par application ou envoyé par SMS.

Cependant, malgré son efficacité, le MFA classique présente certaines limites face aux attaques de type Man-in-the-middle ou au phishing ciblé. Il semble alors pertinent de prévoir l'introduction progressive de la technologie FIDO2 (Fast IDentity Online).

FIDO2 repose sur la cryptographie asymétrique et permet une authentification sans mot de passe, grâce à une paire de clés (publique/privée). Lors de l'enregistrement, une clé publique est transmise au serveur, tandis que la clé privée reste stockée de manière sécurisée dans un token physique ou dans le terminal.

Lors de la connexion, seul ce token peut répondre au défi émis par le serveur, assurant ainsi une authentification sécurisée.

Les jetons FIDO2 peuvent se présenter sous forme de clés USB, de cartes NFC ou de modules biométriques intégrés. Leur utilisation garantit que seule la personne en possession du token, capable de le déverrouiller avec un code PIN ou une empreinte digitale, peut accéder aux services.

En plus de réduire les risques liés au phishing, FIDO2 améliore l'ergonomie du système en simplifiant la procédure d'authentification.

Dans ce contexte, l'introduction de la solution AGOV prend tout son sens. AGOV, plateforme numérique sécurisée mise en place par les autorités suisses, permet aux employés des administrations publiques d'accéder à leurs services numériques de façon unifiée, traçable et conforme à la LPrD. Elle offre une gestion centralisée des identités et des accès, avec une intégration native de l'authentification forte et du standard FIDO2.

En combinant AGOV à l'utilisation de tokens FIDO2, Belleville peut bénéficier d'un double avantage : une conformité renforcée aux exigences légales suisses, et une forte réduction des risques liés à l'authentification et aux accès non autorisés, en particulier dans les domaines fiscaux et RH.

2.2.7 Conclusion

Dans l'ensemble, cette stratégie technique permet de poser les bases d'un système d'information résilient et fiable, en tenant compte des ressources limitées de la commune, en s'appuyant sur des outils libres, des pratiques éprouvées et des référentiels internationaux. Elle vient compléter la politique organisationnelle définie dans la PSSI et constitue une réponse concrète aux risques identifiés après l'incident de sécurité.

3 Sensibilisation, communication et réponse humaine

3.1 Situation actuelle

A ce jour, les collaborateurs de la commune de Belleville n'ont reçu aucune formation et ni sensibilisation aux risques numériques. Aucun programme de prévention n'est mis en place :

- Pas de sessions d'apprentissage
- Aucun support pédagogique
- Aucune Communication interne

Ce manque crucial d'apprentissage expose fortement la commune à tout type d'attaque de type "ingénierie sociale" et "phishing", constituant un risque réel pour tous les habitants de Belleville. Cet ensemble de manque est en totale contradiction avec les bonnes pratiques mentionnées dans la norme **ISO 27002**, en particulier au **point 6.3** qui impose une mise en place complète d'actions visant à la sensibilisation de collaborateurs.

De plus, au sein de l'administration, il n'existe aucun référent ou responsable cybersécurité, ce qui représente un trou au sein de l'organisation. En effet, aucun employé n'est spécifiquement chargé d'informer, conseiller et d'accompagner les collaborateurs sur toute démarche incluant ce sujet.

Chaque collaborateur agit uniquement selon ses intuitions, sans aucun encadrement. Ce manque de gouvernance constitue divers risque tels que :

- L'utilisation de mot de passe simple et identiques
- De la négligence quant au verrouillage de session
- Clics sur des liens suspects sans vérification
- Téléchargement de fichier sans vérification de provenance

Dans l'ensemble, dans un cas de doute ou de suspicion d'attaque, aucune procédure formelle peut être suivie pour réduire les risques.

Les employés ne savent pas à qui s'adresser et comment réagir, ajoutant à une situation déjà critique davantage d'angoisse et de stress, ce qui peut multiplier la probabilité qu'une autre erreur soit commise, conduisant à de nouvelles failles de sécurité sujette à d'autres attaques.

Enfin, le lien avec l'incident subi : la fuite de données fiscales sensibles aurait pu être évitée ou réduite si des mesures et pratiques élémentaires avaient été mises en place. Le facteur humain constitue ici la plus grosse source de risque.

3.2 Campagne de sensibilisation

A la suite de l'incident de sécurité ayant exposé les données fiscales des habitants de Belleville, la mise en place d'une campagne de sensibilisation à la cybersécurité est devenue une priorité absolue.

Cette démarche vise à réduire les risques à l'avenir ainsi qu'à savoir rebondir face un scénario de menace imminente en transformant le comportement des collaborateurs et en instaurant un cadre organisationnel cohérent.

Il est crucial de comprendre que la mise en place de diverses campagnes de sensibilisation vise à inscrire une logique de pilotage continue et pas uniquement à des actions ponctuelles.

Par conséquent, la désignation d'un référent cybersécurité qui a pour rôle coordonnées les actions, d'être le point de contact en cas d'incidents futurs et de garantir un suivi régulier des formations des collaborateurs sur le sujet est un des prérequis.

3.2.1 Objectif principal

L'objectif global de la campagne est de renforcer la sécurité de la commune en agissant sur deux niveaux :

1. Sur les individus, via la formation, l'entraînement à des scénarios de risque et les responsabilités
2. Sur l'organisation, en désignant un responsable cybersécurité

En mettant en place cette double approche, on permet à la commune de s'aligner sur les bonnes pratiques de la norme **ISO 27002** notamment :

- **Point 5.2** : responsabilité de la direction ;
- **Point 6.3** : sensibilisation des utilisateurs ;
- **Point 5.3** : attribution claire des rôles en cybersécurité.

3.3 Mise en œuvre de la campagne de sensibilisation

A la suite du constat inquiétant sur l'absence de formation et de culture lié à la sécurité de la commune de Belleville.

Une campagne de sensibilisation est prévue en 3 phases, chacune coordonnée par le référent en cybersécurité communal désigné pour superviser la mise en œuvre et évaluer les effets de celle-ci.

Après la désignation du référent cybersécurité, la campagne de sensibilisation est déployée selon les trois phases suivantes, chacune placée sous sa coordination directe :

Phase 1 - Affichage de sensibilisation dans les locaux

Objectif Installer plusieurs affiches pour faire office de présence visuelle et rappeler les bonnes pratiques de cybersécurité dans les espaces de travail. Cette phase est importante car elle permet d'éveiller la vigilance de manière passive, à travers des messages clairs et répétitifs.

Mise en place Des affiches au format A4 seront placé dans des lieux stratégiques :

- Entrée principale
- Couloir d'accès
- Salle de pause / cuisine
- Proximité des imprimantes
- Toilettes
- Salles de réunion
-

Thématiques abordées

- Phishing → Ce mail vous demande d'agir vite ? C'est peut-être une arnaque.
- Mot de passe → Ton mot de passe protège les données de toute la commune.
- Session verrouillée → Pense à verrouiller ton poste en partant. (Ctrl + L).
- USB Piégées → Une clé USB trouvée = un piège numérique.
-

Le référent cybersécurité figurera sur certaines affiches comme point de contact. L'affichage sera renouvelé tous les deux mois pour éviter l'effet d'habituation.

Phase 2 : Simulation de phishing

Objectif

Observer la réaction spontanée des collaborateurs lorsqu'ils sont confrontés à une tentative d'attaque non annoncée, telle qu'un courriel de phishing simulé.

Déroulement

- Utilisation de l'outil GoPhish pour envoyer un faux mail simulant une tentative de phishing (fausse notification team, facture d'un service communal
- Cible : l'ensembles des collaborateurs (27 personnes)
- Analyse des résultats après 48h
-

Résultats attendus :

- 16 clics sur le lien piégé = 59%
- 2 signalements spontanés = 7%
- 9 personnes n'ont pas réagi

Ces chiffres fictifs démontrent une faible capacité de détection des menaces. Ce résultat confirme l'urgence de former les collaborateurs à la détection de ces menaces.

Phase 3 : Formation interactive en ligne

Objectif : Offrir une formation courte engageante et dynamique pour corriger les réflexes à risques, ainsi que pour établir une certaine connaissance de base liée au sujet et renforcer la vigilance.

Déroulement :

- **Plateforme utilisée** : Moodle ou Google Forms + Kahoot
- **Durée estimée** : 30 minutes
- **Contenu** :
    - Une vidéo explicative sur divers types d'attaques
    - Un quiz à choix multiple avec 10 questions
    - Une mise en situation : faux scénarios liés à l'une des type d'attaque vu dans les slides
    - Retour et échanges sur les réponses
    - Remise d'une attestation de participation qui doit être possédé par tous les collaborateurs dans un délai de 2 mois. inscription selon horaire

Suivi : Le référent cybersécurité assurera le suivi :

- Nombre de participation
- Gestion des dates
- Bilan global et suivi de progression
- Ajustement des modules
-

La combinaison de sensibilisation passive (affiches), de test actif (phishing simulé) et de formation interactive (quiz) permet de toucher tous les profils d'employés, y compris ceux moins à l'aise avec le numérique.

3.4 Communication et gestion de risque

Lors d'incident de sécurité impactant une commune entière, la gestion uniquement technique n'est pas suffisante, il est fondamental de gérer la communication avec transparence et cohérence aussi bien en interne qu'en externe et tenir informé les personnes concernées de la situation.

Une mauvaise gestion de la communication peut générer une aggravation de la des conséquences en générant de la méfiance et davantage de panique.

Conformément aux exigences de la **Loi sur la protection des données**, un plan de communication de crise doit être prévu. Celui-ci doit viser à informer rapidement et clairement tout en maintenant la continuité d'activité.

3.4.1 Communication externe - citoyens et partenaires

Objectif : maintenir la confiance de la population et se conformer aux exigences légales

Principes :

- **Information** : informer le plus rapidement possible une fois la nature et l'ampleur de l'incident étant identifié
- **Honnêteté et assurance** : admettre la fuite de données, expliquer les mesures prises tout en évitant un langage trop technique
- **Suggestion** : proposer des gestes concrets à mettre en place pour rester protégé

Contenu du message à diffuser :

- **Description** : donner une description factuelle de la situation
- **Nature des données exposés** : noms, adresses et déclarations d'impôt
- **Mesures prises** : isolément du système, investigation
- **Ce qui doit être fait par les citoyens** : surveiller leur boîtes mail, ne peut répondre à des mails suspects, contacter l'administration en cas de doute
- **Moyen de contact** : donner une adresse mail ou une adresse postale concerné pour reporter des incidents suspects

Moyen de diffusion :

- Email ou lettre postale aux habitants concernés
- Affichage sur le site web officiel de la commune
- Communiqué de presse en cas de diffusion publique de l'incident

3.4.2 Communication interne – collaborateurs

Objectif : éviter les rumeurs ainsi que les réactions désorganisé, mettre en place un cadre de gestion d'incident clair

Étape 1 : information progressive La première personne qui détecte un incident doit le signaler au référent cybersécurité mis en place qui prévient à son tour la direction

Étape 2 : message officiel à tous les employés Dès réception de l'alerte, un message interne structuré doit être rédigé par le référent cybersécurité, soumis à validation par la direction, puis communiqué de manière formelle à l'ensemble des collaborateurs

Étape 3 : Session questions - réponses Prévoir une visioconférence collective pour rassurer l'équipe., cette démarche bien que facultative à pour objectif de désamorcer les tensions et renforcer les communications au sein des départements

3.4.3 Conclusion

Ces stratégies de communication permettent de préserver la confiance et de limiter les impacts psychologiques des habitants et collaborateurs de la commune de Belleville, tout en structurant les informations autour d'un référent cybersécurité identifiée.