COMMUNIQUÉ

A L'ATTENTION DE NOS CLIENTS COMMUNAUX SUITE À LA CYBER ATTAQUE CONTRE L'ADMINISTRATION ROLLOISE

Renens, le 1er septembre 2021

A la suite de la cyberattaque que la commune de Rolle a subi à fin mai 2021 sur son infrastructure informatique, dont la presse, les radios et les TV ont abondamment parlé ces derniers jours, il nous paraît utile de préciser les informations suivantes à l'attention de nos communes clientes.

Nous souhaitons ainsi partager avec vous quelques constats et continuer le travail d'information, de recommandations et de conseils que nous avons toujours privilégié avec nos communes clientes.

Les infractions liées à la cybercriminalité économique sont en très forte augmentation depuis maintenant 2 ans et les cybercriminels trouvent sans cesse de nouvelles techniques pour les contourner. Cet état de fait nous pousse de plus en plus à recourir à des sociétés spécialisées dans ce domaine.

Constat et sensibilisation

Aujourd'hui, la problématique des cyberattaques/rançonnages n'épargne ni les entreprises, ni les administrations communales et publiques, ni les individus. C'est un vrai fléau qui est d'ailleurs devenu une industrie du crime.

Les possibilités d'entrer dans les infrastructures informatiques sont multiples et de plus en plus professionnalisées. Ces intrusions peuvent se faire de diverses manières :

- Par des données d'accès d'utilisateurs (hameçonnage)
- Par des failles de sécurité des outils et logiciels
- Etc.

Dans un premier temps, il est nécessaire de sensibiliser les administrations communales et leurs utilisateurs sur les risques potentiels et sur la sensibilité des données sur lesquelles ils travaillent tous les jours, les former sur les bonnes pratiques, sur le maniement des données sensibles ou confidentielles, et faire prendre conscience aux exécutifs et aux patrons des vrais enjeux de la gestion de ces données. La future loi sur la protection des données (LPD) qui va arriver en Suisse tout prochainement permettra de renforcer le cadre légal sur la protection de ces données.

Mesures préventives et recommandations

En parallèle aux efforts de sensibilisation et de formation ci-dessus, nous souhaitons aussi insister sur divers éléments pour minimiser les risques de telles pratiques. Tout d'abord, il est certain qu'un hébergement professionnel des infrastructures est de plus en plus recommandé, l'infrastructure individuelle sur site devenant de plus en plus complexe et coûteuse à mettre en place et à maintenir avec un niveau de sécurité important.

L'hébergement OFICLOUD que nous commercialisons, est construit sur la base de la plateforme DCS+ de Swisscom, ce qui permet de disposer de différentes certifications ISO dont la 27001 sur la couche matérielle. Le reste de l'environnement à savoir la partie virtualisée est à la charge d'OFISA Informatique.

Nous assurons ainsi la mise en place de bonnes pratiques à savoir le patching régulier de l'infrastructure, le suivi et le respect des règles concernant les sauvegardes ainsi que la gestion de la sécurité dont les plateformes antivirus, les filtrages réseaux et le blocage d'applicatifs malveillants.

Notre infrastructure OFICLOUD a par ailleurs été auditée par Cybersafe dans le cas d'une labellisation d'une commune cliente en septembre 2020 et celle-ci répond à leurs exigences. Il est donc possible d'obtenir le label pour une commune de manière facilitée grâce à cet aspect.

Comme indiqué il est impossible de réduire à zéro le risque d'exploitation de vulnérabilités, c'est pourquoi nous restons en permanence vigilant sur le sujet en procédant à une veille technologique, au suivi de l'actualité, et des annonces des principaux acteurs de la cybersécurité.

D'autres éléments techniques sont certainement aujourd'hui incontournables comme par exemple la mise en place d'un système de double authentification pour les accès des utilisateurs, le décommissionnement de serveurs pour lesquels les constructeurs ne livrent plus des patchs de sécurité, l'automatisation du patching par exemple pour certains systèmes d'exploitation ou logiciels, l'extension des logs des outils de firewall (outil de filtrage et de protection de réseau), le chiffrement des données sur les postes de travail fixes et/ou portables, etc.

Une autre mesure technique consiste à effectuer régulièrement des copies de sauvegarde des données dans le cadre d'une stratégie de sauvegarde partielle et complète sur des supports physiquement déconnectés.

A ces mesures techniques, il est aussi nécessaire d'y intégrer des mesures organisationnelles et documentées, comme par exemple la mise en place d'une charte informatique interne, la labellisation et/ou certification de l'infrastructure et des pratiques, l'intervention ponctuelle de sociétés de services spécialisées en termes de sécurité pour apporter un niveau de conseil professionnel et adapté aux dernières évolutions liées à la cybercriminalité.

En conclusion, ces mesures et recommandations sont certainement une partie des premières réponses à apporter à cette vague de cybercriminalité, un renforcement au niveau confédéral et cantonal, permettrait encore d'aider les administrations communales à mieux aborder ces problèmes. Il n'en reste pas moins que chaque exécutif communal doit être conscient que sa commune représente une cible potentielle, et doit élaborer une stratégie de cybersécurité adaptée à sa situation.

Nous restons volontiers à votre disposition pour vous permettre d'engager ces réflexions ou une campagne de sensibilisation, et vous aider à définir votre stratégie de cybersécurité.

Pour toutes questions complémentaires, vous pouvez contacter :

- Par mail : st@o-i.ch
- Par téléphone : Mme Rebecca Beiro ou M. Daniel Chevalier au no 021 321 51 11

OFISA Informatique SA