Réponse du Conseil d'Etat à un instrument parlementaire
—
Question Demierre Philippe 2021-CE-334
Cyberdéfense dans nos communes fribourgeoises et à l'Etat de Fribourg

I. Question

Dans la nuit du samedi 29 au dimanche 30 mai 2021, la municipalité de Rolle a été victime d'une cyberattaque. L'intégralité de ses données a alors été chiffrée, paralysant ainsi complètement l'informatique de la municipalité. Le 24 juin, selon le média Watson.ch, la municipalité est mise au courant que des données sont disponibles au grand public sur le Dark Web, sur le site des cybercriminels Vice Society (auteurs de l'attaque).

A Rolle, 5393 habitants sont directement impactés par cette exfiltration : numéros de téléphones, fixe et mobile, email, numéros AVS, bulletins scolaires d'enfants, religion, etc.

Selon le journal letemps.ch, des accords fiscaux avec une multinationale et des arrangements avec un riche étranger ont été dévoilés.

La cybersécurité est un mot qui revient sur toutes les lèvres aujourd'hui, et les communes de Suisse ne sont pas exemptées du phénomène.

J'ai pris personnellement cette problématique en main dans ma commune d'Ursy en tant que vice-syndic afin de ne pas nous retrouver dans la situation de la municipalité de Rolle.

Notre Confédération possède un cadre légal et politique très précis en la matière et qui se veut toujours à jour.

Cependant, il est à relever que si les organes politiques tentent de montrer l'exemple, il reste un nombre impressionnant de lacunes à combler.

Les ressources ayant les compétences requises manquent et nous ne trouvons aucune stratégie globale dans les organisations.

Questions :

1. Qu'envisage le Conseil d'Etat fribourgeois pour éviter une telle catastrophe sur le plan cantonal et communal ?
2. Le Conseil d'Etat fribourgeois a-t-il une liste précise des technologies matérielles et logicielles utilisées (canton et communes) ?

10 septembre 2021

II. Réponse du Conseil d'Etat

A titre liminaire, le Conseil d'Etat rappelle que le terme de cyberdéfense renvoie aux mesures des services de renseignement et aux mesures militaires de défense contre les cyberattaques et qu'il concerne principalement la Confédération, et plus particulièrement l'Armée. En revanche, les mesures de prévention, de maîtrise des incidents, de gestion de la résilience, de formation et de recherche que les cantons peuvent mettre en œuvre dans le cadre de la lutte contre les cyber-attaques relèvent du domaine de la cybersécurité.

1. *Qu'envisage le Conseil d'Etat fribourgeois pour éviter une telle catastrophe sur le plan cantonal et communal ?*

Au niveau cantonal

Le Conseil d'Etat constate depuis plusieurs années la multiplication des cyberattaques, qui dans le même temps se professionnalisent. Conscient de la valeur de son patrimoine numérique et de l'importance de ses systèmes d'information, l'Etat de Fribourg est soucieux de mettre en œuvre un ensemble d'actions adaptées, destinées à prévenir la survenance d'incidents tels que celui décrit par l'auteur de la question.

En premier lieu, des tests de vulnérabilité sont effectués régulièrement sous l'égide du Service de l'informatique et des télécommunications (SITel), au sein duquel a été constituée une équipe chargée spécifiquement d'assurer la sécurité des moyens informatiques et qui s'appuie sur de l'expertise externe. Il s'agit d'un Security Operation Center (SOC), mis en place en 2019 et qui constitue une plus-value pour la gestion des risques.

Le champ de compétences et les missions du SITel en la matière ont récemment fait l'objet d'une clarification, à l'occasion de l'adoption de l'ordonnance sur la gouvernance de la digitalisation et des systèmes d'information de l'Etat en juillet 2021. Le SITel est responsable de la sécurité des moyens informatiques de l'Etat. De plus, certaines unités à statut spécifique interviennent dans des domaines particuliers. C'est le cas de l'unité informatique spécialisée de la Police cantonale ou du Centre de compétences pour l'éducation (Fritic) pour le domaine de l'enseignement.

Plus précisément concernant les écoles du canton, les établissements du post-obligatoire sont sous la gestion technique du SITel et se trouvent par conséquent sous la protection des mesures de cybersécurité mentionnées ci-dessus. Il en est de même pour les outils de gestion administrative des écoles ou les outils de communication et de collaboration des établissements du degré de l'enseignement obligatoire. Le centre de compétences Fritic est responsable de la sécurité des données personnelles dans son champ de compétences supplémentaires. En revanche, le matériel et les infrastructures techniques des écoles des degrés primaires et secondaire I sont sous la responsabilité des communes et dépendent donc des mesures de sécurité mises en place par ces dernières.

Enfin, certaines unités administratives telles que l'Université ou l'Hôpital fribourgeois (HFR) bénéficient d'une autonomie légale les habilitant à déterminer de manière autonome leur stratégie informatique.

Un groupe de travail a par ailleurs été institué cet automne, dans le but d'élaborer une nouvelle ordonnance réglant les questions d'organisation et de responsabilité dans le domaine de la sécurité de l'information au sein de l'administration cantonale.

En 2019, le SITel a mandaté une entreprise helvétique externe – spécialisée dans la sécurité informatique – afin de déterminer la maturité actuelle en termes de sécurité informatique et de mettre en place des améliorations continues. Cette analyse a été effectuée selon une méthodologie basée sur une échelle standardisée dite CMMI (Capability Maturity Model Integration). L'analyse de 22 processus de cybersécurité a permis d'initialiser plus d'une vingtaine de projets et de missions. Pour des raisons évidentes de confidentialité et de sécurité, ces informations ne sont pas divulguées.

Par ailleurs, l'Etat de Fribourg collabore avec la Confédération afin de renforcer son action et de maintenir un niveau de connaissance des bonnes pratiques en matière de cybersécurité qui soit constamment satisfaisant. Ainsi, il participe activement à la mise en œuvre de la « Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) pour les années 2018 à 2022 ». Cette stratégie, élaborée au niveau fédéral en collaboration avec les cantons, les milieux économiques et les Hautes écoles, définit les objectifs qui devront être atteints dans différents champs d'action et constitue la base permettant les efforts communs requis afin de réduire les cyberrisques.

Un autre champ d'action destiné à renforcer la stratégie de cybersécurité de l'Etat de Fribourg est la diffusion des bonnes pratiques en matière d'hygiène informatique. Pour ce faire, il s'appuie notamment sur les documents de référence en la matière, tels que la « norme minimale pour améliorer la résilience informatique » rédigée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) en 2018. Le Conseil d'Etat rappelle ainsi l'importance de la sensibilisation de tous les utilisateurs au sein de l'administration cantonale et la nécessité d'adopter des comportements adaptés dans l'usage des outils informatiques.

En outre, sous l'égide de la Confédération et dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyberrisques, l'Etat de Fribourg participe à un groupe de travail dont l'objectif est la mise à disposition d'une solution de sensibilisation à la cybersécurité pour l'ensemble des administrations publiques suisses.

La Police cantonale intervient quant à elle dans le domaine de la cybercriminalité, c'est-à-dire lorsqu'une infraction pénale a été commise sur ou au moyen d'un système informatique. Elle s'est dotée à cet effet depuis 2016 d'une entité en charge de la cybercriminalité.

Elle s'engage dans le domaine de la prévention, sensibilise et conseille aux nouveaux phénomènes cybercriminels. Elle axe ses campagnes sur les phénomènes actuels rencontrés. A ce titre, cette année, elle a notamment participé à la semaine nationale d'action sur la sécurité du cyberespace et diffusé sur ses réseaux des préventions concernant les arnaques en ligne, les fraudes aux investissements en ligne, etc. La page de la Prévention suisse de la criminalité (www.skppsc.ch) permet également de retrouver de nombreuses informations et conseils concernant ces phénomènes.

Force est de constater que les infractions liées au numérique sont en constante augmentation. Les moyens d'action pour lutter contre ces criminels sont limités puisqu'ils agissent le plus souvent depuis l'étranger et que la coopération internationale reste compliquée. Toutefois, il est important que les victimes d'une attaque avisent sans tarder la Police afin qu'elle puisse les conseiller et recueillir le maximum d'éléments d'enquête. Ces informations, réunies et traitées par la plateforme d'analyse et de coordination suisse permettront d'améliorer la lutte contre ces phénomènes.

Le Conseil d'Etat fait observer que les mesures de protection mises en place ont permis à ce jour à l'Etat de Fribourg de contenir les cyberattaques dont il a été la cible, comme le sont par ailleurs toutes les administrations publiques. Cette protection a non seulement été assurée grâce à l'organisation et aux outils spécifiques déployés par l'administration cantonale, mais elle résulte également de l'implication de l'ensemble des collaborateurs de l'Etat.

Il convient néanmoins de rester humbles face à ces résultats, une attaque pouvant toujours survenir. Les risques en la matière ne doivent pas être sous-estimés. Evoquer ouvertement son état de préparation peut s'avérer contre-productif, en suggérant aux personnes et organisations malveillantes une sorte de « défi ».

L'Etat de Fribourg ne souhaite pas dévoiler, pour des raisons évidentes de confidentialité et de sécurité, le détail des outils et technologies utilisés mis en place pour répondre à éventuelle attaque qui pourrait survenir. D'autre part, si tout ou partie d'une attaque devait aboutir, une organisation de crise est prévue. Elle a notamment déjà pu être éprouvée à l'occasion du COVID-19. Finalement, la stratégie de sauvegarde et les processus de restauration offrent une certaine protection afin d'assurer une perte mitigée de données en cas d'attaque de type « Ransomware ».

Au niveau des communes

Concernant la protection des communes, le Conseil d'Etat rappelle qu'il n'est pas compétent pour intervenir en lieu et place de celles-ci. Il recommande vivement à l'ensemble des communes fribourgeoises de prendre la pleine mesure de la menace cyber et des conséquences éventuellement importantes d'une attaque.A cette fin, il rappelle que des solutions telles que le label « Cyber-safe » permettent de réaliser une analyse de l'état de préparation d'une structure face aux cyberattaques. Ce diagnostic doit permettre ensuite la mise en place de mesures d'amélioration de la capacité d'anticipation et de résilience du système d'information.

Le Conseil d'Etat et le Comité de l'Association des Communes Fribourgeoises ont également décidé de renforcer leur collaboration et de coordonner les démarches de digitalisation des prestations publiques fournies aux communes, à la population, aux milieux économiques et aux institutions dans le canton de Fribourg. Ils ont à cette fin signé une convention déterminant les conditions-cadres du développement et du financement de la digitalisation des prestations publiques dans le cadre de la démarche DIGI-FR. Cet élan commun pourrait servir de plateforme également à la mise en place d'une cybersécurité conjointe.

2. *Le Conseil d'Etat fribourgeois a-t-il une liste précise des technologies matérielles et logicielles utilisées (canton et communes) ?*

Comme indiqué ci-dessus, la publication des technologies précises utilisées par l'administration cantonale pour faire face aux cyber-attaques n'est pas souhaitable, pour des raisons de sécurité d'une part, mais également pour ne pas créer un effet « d'appel » aux personnes et organisations malveillantes d'autre part.

Le Conseil d'Etat a entière connaissance des solutions utilisées. Il se prononce sur les investissements et les choix liés aux projets informatiques en matière de sécurité, dans les conditions définies par l'ordonnance sur la gouvernance de la digitalisation et des systèmes d'information de l'Etat précitée. Il s'appuie en particulier pour ce faire sur le rôle joué par la

Commission informatique de l'Etat (CIE) et par la Délégation du Conseil d'Etat en matière de digitalisation et des systèmes d'information (DSI).

En revanche, l'Etat de Fribourg ne gérant pas la cybersécurité des communes, il n'a donc pas connaissance des technologies qu'elles utilisent.

9 novembre 2021