REPONSE DU CONSEIL D'ETAT
à l'interpellation J. Byrne Garelli et consorts - Quels sont les enseignements à tirer de la cyberattaque de Rolle pour l'ensemble des communes vaudoises (21_INT_106)

Rappel de l'intervention parlementaire

Relayé dans la presse avec fracas ces dernières semaines, la Commune de Rolle a subi une cyberattaque d'une ampleur sans précédent. Plus de 5'000 rolloises et rollois ont vu leurs données personnelles être publiées en ligne. Numéros AVS, dates de naissance, état civil, numéros de téléphones se retrouvent accessibles et disponibles sur le Darknet. Loisible à toute personne malveillante d'utiliser ces dernières à des fins nuisibles aux habitants de la Commune de Rolle.

À la suite de cet événement, si nuisible à la sphère privée, en tant qu'organe législative nous devons nous saisir urgemment de cette thématique afin de permettre aux Communes de disposer des moyens suffisants pour contrer de telles attaques et que ses dernières ne se reproduisent plus

Par ces quelques lignes, j'ai donc le plaisir d'adresser au Gouvernement les questions suivantes :

1. *De quoi les citoyennes et citoyens de Rolle doivent-ils se préoccuper en termes de sécurité internet au vu de la fuite de leurs données ?*
2. *Existe-t-il un risque d'action judiciaire à l'encontre de la commune de Rolle en lien avec la loi sur la protection des données ?*
3. *De quels conseils la commune de Rolle a-t-elle bénéficié de la part de la police cantonale ?*
4. *De nombreuses communes ont reçu depuis cette attaque plusieurs propositions d'assurances ou de services dédiés afin de remédier à des risques de cyberattaque : quel soutient est apporté par le Canton en faveur de nos collectivités locales dans ce domaine ?*
5. *Quelles ont été les communications du Canton auprès des Communes depuis ces événements afin d'éviter la paralysation d'autres administrations communales ?*
6. *Est-ce que le Canton prévoit-il de proposer des formations en faveur des élus et du personnels des administrations communales à ce sujet ?*

Réponse du Conseil d'Etat

Considérations générales :

En préambule, le Conseil d'Etat souligne que nul n'est à l'abri d'une cyberattaque comme l'actualité récente l'illustre – les cybermenaces constituent un des risques principaux auxquels sont confrontés population, entreprises et collectivités publiques, aux trois niveaux institutionnels.

Dans sa stratégie numérique de novembre 2018, le Conseil d'Etat a réaffirmé sa détermination à renforcer son action en matière de cybersécurité, qu'il s'agisse de poursuivre la sécurisation des infrastructures numériques cantonales, de promouvoir les principes de souveraineté et de sécurité dans les instances gouvernant le déploiement des infrastructures numériques ou d'accompagner les personnes, les entreprises et autres collectivités en matière de cybersécurité, notamment par la promotion des bonnes pratiques. Le Conseil d'Etat pour ce faire s'appuie notamment sur les professionnels actifs au sein de la Direction générale du numérique et des systèmes d'information (DGNSI), en particulier sur les spécialistes de son centre opérationnel de sécurité SOC, ainsi que sur les spécialistes cyber de la Police cantonale.

1. ***De quoi les citoyennes et citoyens de Rolle doivent-ils se préoccuper en termes de sécurité internet au vu de la fuite de leurs données ?***

Les données dérobées et publiées dans le *Darkweb* lors de la cyberattaque lancée en 2021 contre la commune de Rolle contiennent le contenu des *e-mails* de l'administration communale, ainsi que des fichiers présents sur ses serveurs internes. Si de tels vols de données n'induisent en principe pas de risques directs, ces données sont en revanche du « pain béni » pour les personnes malveillantes, car elles facilitent les tentatives de fraudes et d'usurpations d'identité.

2. ***Existe-t-il un risque d'action judiciaire à l'encontre de la commune de Rolle en lien avec la loi sur la protection des données ?***

Chacun étant libre de saisir la justice pour faire valoir sa cause, on ne peut par définition exclure qu'une personne entreprenne une action contre la commune de Rolle, si elle juge cette démarche fondée. Le Conseil d'Etat tient toutefois à rappeler que la diffusion de données personnelles dont il est question est la conséquence d'une cyberattaque contre cette commune et que ce n'est pas cette dernière, mais des tiers, qui l'ont opérée.

3. ***De quels conseils la commune de Rolle a-t-elle bénéficié de la part de la police cantonale ?***

Lors de l'annonce de la commune à la Police cantonale le 31 mai 2021, un enquêteur de la Division enquêtes cyber de la Police cantonale a fait un point de situation avec son interlocuteur sur les mesures urgentes à entreprendre (sécurisation du périmètre, préservation des traces, recours à une société spécialisée dans la réponse aux incidents, etc.). La Police cantonale s'est chargée de la diffusion immédiate des renseignements utiles aux organismes concernés, tels que le GovCERT. Un suivi a ensuite été assuré avec la commune et ses mandataires, en cas de besoin. La Police cantonale a entrepris dans l'intervalle après la plainte formellement déposée le 14 juin 2021, les démarches nécessaires en investigation policière.

Il est à relever que la DGNSI, par l'entremise de spécialistes de son centre opérationnel de sécurité SOC, a également apporté à la commune de Rolle un soutien et des conseils dès le 26 août 2021 pour toutes les communications internes et externes, y compris la préparation des communiqués de presse et la coordination de la cellule de crise. Le Directeur de la sécurité numérique de l'Etat était également présent lors des soirées d'information publiques avec les Municipaux présents pour répondre aux questions de la population.

4. ***De nombreuses communes ont reçu depuis cette attaque plusieurs propositions d'assurances ou de services dédiés afin de remédier à des risques de cyberattaque : quel soutien est apporté par le Canton en faveur de nos collectivités locales dans ce domaine ?***

Rappelons que dans l'ordre institutionnel existant, le Canton n'a pas la responsabilité de l'informatique communale, a fortiori de la sécurité informatique des communes. Toutefois au vu de l'urgence et de l'importance de l'affaire, et sur demande des autorités communales, dans le cas de Rolle, 'Etat a proposé l'intervention d'une équipe de spécialistes en cybersécurité du SOC dépêchée en renfort pour contribuer à répondre à ce cyberincident et à coordonner la gestion de crise, qui comporte un volet important de communication de crise. Ce soutien est venu compléter les activités de l'équipe cybercrime de la Police Cantonale Vaudoise qui se charge du volet judiciaire lors d'une cyberattaque. Néanmoins les modalités de ce soutien cantonal aux autorités communales vont évoluer.

En effet, au vu de la multiplication des cyberattaques, les Conseillères d'Etat en charge du numérique, respectivement des communes, ont rencontré en novembre 2021 les représentants de l'Union des communes vaudoises (UCV) et de l'Association de communes vaudoises (AdCV) pour déterminer comment la collaboration entre le Canton et les communes en cas de cyberattaque, ainsi que dans le domaine de cyberprévention, pourrait être organisée et financée dans le long terme. Un groupe de travail technique composé de représentants de l'Etat et des communes, placé sous la responsabilité du Directeur de la sécurité numérique de l'Etat de Vaud, a été chargé de faire des premières propositions dans le courant du printemps 2022 relatives aux modes de collaboration et à leur financement.

5. ***Quelles ont été les communications du Canton auprès des Communes depuis ces événements afin d'éviter la paralysation d'autres administrations communales ?***

Le 15 octobre 2021, le Directeur général des affaires institutionnelles et des communes (DGAIC) et le Directeur de la sécurité numérique ont écrit à l'ensemble des communes vaudoises pour leur rappeler les 5 mesures de prévention principales préconisées par le Centre national pour la cybersécurité, le NCSC, soit :

1. La sécurisation des accès à distance ;
2. Les sauvegardes hors ligne ;
3. La gestion des correctifs et des cycles de vie des actifs informatiques ;
4. Le blocage des pièces jointes et des liens à risque dans les courriels ;
5. La surveillance des fichiers journaux (logs).

Ce courrier était, de plus, accompagné d'une annexe présentant les actions immédiates à entreprendre en cas de cyberattaque ainsi que le moyen de faire appel au support du Canton par l'intermédiaire de la centrale d'alarme du 117 de la Police Cantonale Vaudoise.

Il est également à relever que le Centre opérationnel de sécurité a émis, en 2021, deux notices d'alertes à l'intention de l'ensemble des communes concernant des vulnérabilités critiques pouvant mettre à risques les systèmes d'informations des communes. Ce type de communication urgente ponctuelle sera reconduite lorsque jugée nécessaire.

6. ***Est-ce que le Canton prévoit de proposer des formations en faveur des élus et du personnel des administrations communales à ce sujet ?***

Le Conseil d'Etat est convaincu de la nécessité de renforcer les compétences numériques de l'ensemble de la population, et partant des élus ou du personnel des administrations ou entreprises : la formation et la sensibilisation sont des axes essentiels pour améliorer ce qu'on appelle les « *firewalls humains* », les pare-feux humains. L'Etat propose ainsi depuis plusieurs années déjà, en libre accès sur Internet, des modules de formation et de sensibilisation (formation eSUSI.vd.ch), qui seront complétés en 2022 avec une formation en ligne préparée par

le Réseau National de Cybersécurité (RNS) pour les collaboratrices et collaborateurs des administrations cantonales et communales. Le Centre d'éducation permanente (CEP) propose également une sensibilisation aux cyberattaques. Ce thème est également abordé lors des séances d'information organisées par la DGAIC à l'intention des communes dans le cadre du programme "Au top pour ma commune". Il a également fait l'objet d'un article dans le périodique "Canton-Communes".

L'application mobile d'alertes et d'information cybersécurité du Canton disponible à l'adresse vd.ch/cybersecurité fournit également un set d'informations complémentaires utiles pour les personnels des administrations communales.

En janvier 2022, l'Etat lance une nouvelle campagne, avec des vidéos, pour sensibiliser encore la population aux bonnes pratiques en matière de cybersécurité.

Les résultats des discussions menées avec les représentant-e-s des associations faitières de communes (cf. réponse à la question 4) pourraient conduire au développement de prestations spécifiques en direction du personnel communal et des élus communaux.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 19 janvier 2022.

La présidente :	Le chancelier :
N. Gorrite	*A. Buffat*