GRAND CONSEIL

RAPPORT DE LA COMMISSION THÉMATIQUE DES SYSTÈME D'INFORMATION chargée d'examiner l'objet suivant :

Motion Yann Glayre et consorts au nom du groupe UDC – Soutien financier urgent aux communes pour la sécurité de leurs infrastructures informatiques

1. PREAMBULE

La Commission thématique des systèmes d'information (CTSI) s'est réunie le mardi 1er mars 2022 à la salle du Bicentenaire, pl. du Château 6, à Lausanne, pour traiter de cet objet.

Elle était composée des Députés et des Députées : Maurice Neyroud (président et rapporteur), Stéphane Balet, Céline Baux, Jean-François Chapuisat, Nicolas Croci Torti, Maurice Gay, Sabine Glauser Krug, Yann Glayre, Salvatore Guarna, Vincent Jaques, Didier Lohri, Daniel Meienberger, Daniel Ruch, Alexandre Rydlo.
Excusé-e-s : Carole Schelker (remplacée par D. Ruch), Philippe Jobin

Mme Nuria Gorrite, cheffe du Département des infrastructures et des ressources humaines (DIRH) a participé à la séance, accompagnée de M. Patrick Amaru, directeur général de la Direction générale du numérique et des systèmes d'information (DGNSI).

M. Yvan Cornu, secrétaire de la commission, a tenu les notes de séance, ce dont nous le remercions.

2. POSITION DU MOTIONNAIRE

Le texte proposé vise à apporter une aide financière aux communes qui souhaitent moderniser et sécuriser leurs infrastructures informatiques. Cette motion part du principe que certaines communes ont freiné leurs investissements sur la partie informatique pour des raisons évidemment financières.

Concernant le calcul de la subvention, que cela soit CHF 10.- par habitant ou une autre méthode de calcul, le motionnaire se déclare ouvert à toute proposition du moment qu'on aide les communes à sécuriser leurs systèmes d'information. Par contre, si toutes les communes se déclarent suffisamment à l'aise financièrement et qu'elles n'ont pas vraiment besoin d'aide pour investir, le motionnaire serait alors prêt à retirer son texte.

On pourrait reprocher à cette motion de proposer une politique dite de l'arrosoir en distribuant largement des subventions sur la seule base du nombre d'habitants par commune, sans tenir compte d'autres caractéristiques du bénéficiaire. Néanmoins, selon le motionnaire, le principe même d'une subvention est d'offrir un financement pour une tâche déterminée.

3. POSITION DU CONSEIL D'ÉTAT

Le Conseil d'Etat comprend le dépôt de cette motion suite aux récentes cyberattaques qui ont touché les communes de Rolle et Montreux. Il est évident que ce nouveau type de criminalité informatique va en s'accentuant et s'étend indéniablement aux communes. De son côté, consciente que le canton peut être une cible potentielle, la DGNSI a mis en place depuis plusieurs années des mesures importantes pour sécuriser le système d'information de l'Etat de Vaud.

Dès le début, le canton de Vaud a activement collaboré avec la centrale fédérale d'enregistrement et d'analyse pour la sûreté de l'information (Melani[1]), centrale qui est maintenant intégrée au sein du Centre national pour la cybersécurité (NCSC).

[1] En allemand : Melde- und Analysestelle Informationssicherung, abrégé Melani

Le Conseil d'Etat a également beaucoup travaillé avec les faîtières des entreprises, à commencer par la Chambre vaudoise du commerce et de l'industrie (CVCI), pour améliorer la protection et la sensibilisation des PME en particulier, car certaines d'entre elles sont mal préparées à affronter de telles cyberattaques. Le canton mise sur une campagne d'information et de sensibilisation.

Soutien aux communes

Lors de l'attaque de la commune de Rolle par exemple, la DGNSI a agi sur plusieurs fronts. Une cellule d'intervention d'urgence est intervenue rapidement pour déterminer le périmètre du dommage, isoler les réseaux et éviter une infiltration au niveau des services informatiques de l'Etat. La DGNSI a aidé la commune à rétablir son système d'information. Des experts en sécurité numérique du canton ont apporté leur aide à la communication de crise ; notamment la manière d'informer la population sur les risques encourus. La DGNSI a également accompagné la commune à trouver un partenaire privé, pour mettre à niveau leur système informatique. A noter que la commune de Montreux, qui dispose d'un service informatique, doté en professionnels, était mieux préparée à faire face à une cyberattaque.

Le Canton de Vaud est forcément limité dans ses interventions auprès des communes puisqu'il ne dispose que de cinq collaborateurs au sein du Security operation center (SOC). Il n'a pas les forces nécessaires pour aller régulièrement aider les communes, au risque d'affaiblir sa mission de base de sécurisation du système d'information de l'Etat.

Réponse à la menace : collaboration canton-communes

Les deux Conseillères d'Etat en charge de l'informatique et des affaires communales ont déjà engagé une discussion auprès des faîtières des communes, l'UCV et l'AdCV. A l'occasion d'une première rencontre, les parties ont convenu de l'importance pour les communes de se doter d'un système d'intervention d'urgence. Le canton a proposé trois alternatives aux communes :

1) Confier au canton la gestion du centre d'intervention d'urgence auprès des communes, en finançant par exemple deux postes supplémentaires au sein du SOC pour assurer cette tâche nouvelle.
   En période normale, ces experts accompagneraient les communes dans l'analyse de leur niveau de cybersécurité et dans l'identification des actions à prendre pour réduire les risques. En cas d'intervention d'urgence, la mutualisation des forces permettrait d'intervenir pour aider directement les communes touchées.
2) Mettre en place et financer un pool d'experts dédié à la sécurisation des données des communes.
3) Lancer un appel d'offre public et mandater un fournisseur privé de services de cybersécurité.

Une décision est attendue d'ici à fin mars 2022 qui permettra de construire ce réseau.

Quand le SOC identifie un risque spécifique, il en informe évidemment la commune concernée. De manière plus générale, les communes pourraient rejoindre un système de newsletters.

Matériel d'information et de prévention

Le canton peut déjà mettre à disposition des communes les outils qu'il a développés tels que les bonnes pratiques en matière de sécurité informatique et de protection des données personnelles, la sensibilisation aux risques, etc. L'application de ces règles de base permet de sensiblement réduire les risques. Des modules de formation du personnel peuvent aussi être mis gratuitement à disposition des communes.

Séparation des pouvoirs canton-communes

Ayant décrit les diverses actions que le canton entreprend déjà avec les communes en termes de cybersécurité, le Conseil d'Etat ne soutient pas le versement de subventions supplémentaires. Attaché au principe de la séparation des pouvoirs, le Conseil d'Etat estime que les communes doivent in fine décider librement de leur niveau de sécurité informatique, même si l'Etat peut éditer des standards et des bonnes pratiques. Par contre, il n'est pas envisagé d'imposer un standard cantonal uniforme. La conseillère d'Etat indique que les faîtières des communes n'ont pas formellement demandé de financement pour la sécurisation de leurs systèmes d'information.

Le Conseil d'Etat préfère mettre à disposition ses compétences, son expérience et son savoir-faire, en laissant la souveraineté aux communes de décider du dispositif de sécurisation informatique qu'elles veulent mettre en place. L'Etat est évidemment prêt à les accompagner.

Les communes ont pris conscience des risques liés aux cyberattaques ; elles prennent leurs responsabilités et sont en train de tester leurs systèmes, d'identifier les failles et de prendre des actions pour améliorer leur cybersécurité.

4. DISCUSSION GÉNÉRALE

Montant de la subvention

Le motionnaire a considéré un budget global de CHF 8 millions pour une aide unique aux communes, sans obligation toutefois d'appliquer un standard unique. Cette démarche doit permettre d'aider rapidement les communes sur le point bien précis de l'obtention d'un label de cybersécurité.

Au sein de la commission, plusieurs interrogations ont porté sur à la méthode de calcul de la subvention proposée de CHF 10.- par habitant ; dans quelle mesure ce montant forfaitaire est en lien avec la tâche de certification ou de sécurisation des systèmes d'information communaux. L'infrastructure informatique n'est pas directement liée au nombre d'habitants. Une commune de 10'000 habitants recevrait CHF 1000'000.-, sans être certain que la totalité soit effectivement nécessaire à la sécurisation des infrastructures informatiques.

En introduction, le motionnaire a indiqué qu'il était prêt à modifier la méthode de calcul de la subvention. De même, il n'est pas prévu de standard obligatoire pour les communes.

La conseillère d'Etat précise que le subventionnement pose une multitude de questions quant à l'octroi, au suivi et au contrôle.

Certification Cyber-safe

Des discussions ont été engagées avec les faîtières qui proposent notamment aux communes de se faire auditer (diagnostic informatique) afin d'obtenir un label de cybersécurité, notamment celui délivré par Cyber-safe qui est une association à but non lucratif. En termes de prévention, certaines communes ont mandaté des entreprises privées pour effectuer une veille informatique. Des mentions sur le darknet sont des indices d'une possible attaque. Il s'agit d'un choix politique, dès lors un investissement de quelques milliers de francs par année reste en principe supportable pour une commune, même petite ou moyenne.

La commission insiste sur l'importance de la formation des utilisatrices et utilisateurs et sur l'application de bonnes pratiques, car l'erreur humaine reste la principale cause des cyberattaques qui réussissent.

Pérenniser la sécurité

La présente motion a l'intérêt de souligner l'importance de pérenniser la sécurité informatique. La sécurité est un élément indispensable de réflexion en permanence. Il faut éduquer le personnel à la protection des données et à la sécurisation des accès. Toute action de sécurité doit s'inscrire dans la durée, il n'est pas efficace de proposer une subvention unique.

Il existe déjà des formations sur la cybersécurité des personnes « Sensibilisation des utilisateurs à la sécurité de l'information » sur la plateforme VD ACADEMIE, mais il craint que ces formations soient peu suivies.

Il apparaît important de sensibiliser les communes, mais ces dernières doivent rester responsable de prendre les mesures appropriées à la sécurité informatique. Un label et une subvention unique ne sont pas suffisants ; il s'agit de mettre en place une politique de cybersécurité sur le long terme.

Dialogue entre spécialistes et politique

Depuis des années, la DGNSI travaille avec l'Association vaudoise des responsables informatiques communaux (AVRiC), mais force est de constater que l'information ne remontait pas suffisant vers le pouvoir politique. Il est important de mettre en place une structure de dialogue entre le canton et les communes au sujet de l'informatique, afin notamment d'augmenter la prise de conscience du risque des cyberattaques et des mesures préventives à prendre.

Dans cette logique de dialogue, les deux départements en charge de l'informatique et des communes vont mettre en place une plateforme de discussion permanente avec les communes. Il est envisagé d'organiser une journée de la cyberadministration et/ou d'envoyer des newsletters régulières sur la thématique de l'augmentation des risques et des attaques.

Postulat David Raedler (21_POS_44) … agissons à tous les échelons face aux cyberattaques

Pour rappel, la CTSI a soutenu le postulat David Raedler et consorts - Les pirates sont informatisés et ne se limitent plus au Léman : agissons à tous les échelons face aux cyberattaques, qui demandait déjà une série de mesures pour améliorer la cyberdéfense au niveau des communes.

Afin de ne pas contraindre les communes à respecter un standard cantonal et de maintenir leur autonomie, la CTSI avait unanimement accepté d'amender le postulat Raedler en indiquant qu'un standard minimum pouvait, mais ne devait pas forcément être respecté, en validant possiblement la formation des responsables informatiques des communes.

Bien que le soutien financier aux communes ne fût pas abordé dans ce postulat, la CTSI se montre défavorable à une subvention arrosoir basée sur un montant par habitant.

Dans un rapport, le Conseil d'Etat pourra ainsi communiquer sur la collaboration canton-communes dans le domaine de la cybersécurité.

Transformation en postulat

La transformation en postulat a été évoquée à plusieurs reprises, mais il faudrait amener des corrections importantes au texte qui va vraiment dans le sens d'adopter un décret accordant une subvention urgente unique aux communes qui se dote d'un label.

Le motionnaire prend acte que la majorité de la commission ne souhaite pas proposer une aide financière directe, peu importe la manière. Il prend aussi note que cette position est partagée par le Conseil d'Etat.

Au final, la commission renonce à une transformation en postulat et l'auteur maintien sa motion.

Conclusion du motionnaire : des aides indispensables face aux risques de cyberattaques

Le motionnaire indique qu'il ne demande ni standard unique, ni expertise, mais requiert l'obtention d'un label de cybersécurité pour bénéficier d'une subvention unique. Les communes restent libres ensuite de la manière de continuer la gestion de leur infrastructure informatique. Personne n'a parlé d'envoyer des fonctionnaires cantonaux faire la police dans les communes vaudoises.

Pour faire face aux risques de cyberattaques, les communes ont dû investir, parfois de grosses dépenses. Après le diagnostic (l'audit), les communes doivent parfois investir massivement pour moderniser leur infrastructure informatique.

Alors qu'on vient d'affirmer que les faîtières n'ont pas besoin d'argent, il est piquant que l'AdCV demande aux candidates et candidats au Grand Conseil s'ils sont favorables à des aides cantonales aux communes pour leur informatique et leur cybersécurité.

Le montant total serait de CHF 8 millions, mais en cas d'attaque le montant des rançons pourrait s'avérer bien supérieures.

5. VOTE SUR LA PRISE EN CONSIDÉRATION DE LA MOTION

La CTSI recommande au Grand Conseil de classer cette motion par 11 voix et 3 abstentions.

Chardonne, le 26 avril 2022

Le rapporteur :
(Signé) Maurice Neyroud