canton de vaud
LIBERTÉ PATRIE

GRAND CONSEIL

JANVIER 2022 **RC-21_POS_44**

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

Postulat David Raedler et consorts - Les pirates sont informatisés et ne se limitent plus au Léman : agissons à tous les échelons face aux cyberattaques

1. PREAMBULE

La Commission thématique des systèmes d'information (CTSI) s'est réunie le mardi 2 novembre 2021 à la salle du Bicentenaire, pl. du Château 6, à Lausanne, pour traiter de cet objet.

Elle était composée de M. Maurice Neyroud (président de séance et rapporteur), de Mmes et MM. les député·e·s Stéphane Balet, Céline Baux, Jean-François Chapuisat, Jean-Luc Chollet, Salvatore Guarna, Sabine Glauser Krug, Yann Glayre, Vincent Jaques, Didier Lohri, Daniel Meienberger, Alexandre Rydlo, Carole Schelker, Marion Wahlen. Excusés : Nicolas Croci Torti, Maurice Gay (remplacé par M. Wahlen), Philippe Jobin (remplacé par J.-L. Chollet).

Le postulant, M. David Raedler, était également présent avec voix consultative.

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

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

2. POSITION DU POSUTLANT

Le jour même de la séance, la RTS annonçait que le nombre de cyberattaques en Suisse avait doublé au premier semestre de cette année, avec plusieurs constats dont celui que le nombre de rançongiciels (ou *ransomwares)* a complétement explosé en passant de 97 cas à 497 incidents sur la même période entre l'année 2020 et 2021. Le nombre et la gravité des attaques doivent nous préoccuper au premier plan d'un point de vue informatique et de sécurité en général. Certes les cyberrisques ont toujours existé, mais on constate que depuis 2020 le nombre des attaques informatiques a explosé. Cette situation s'explique en particulier par la décentralisation du travail (intensification du télétravail) en lien avec la pandémie et par l'usage accru des réseaux informatiques. L'utilisation de connexions à distance de type VPN ouvre des portes aux cyberattaquants si les mesures sécuritaires nécessaires ne sont pas prises, à la fois chez l'utilisateur et au niveau des serveurs. L'autre explication vient du fait que les cybercriminels, essentiellement localisés à l'étranger, sont de mieux en mieux organisés. Il ne s'agit plus d'arnaques diffuses, mais d'attaques professionnelles et ciblées qui quand elles atteignent leur but ont des conséquences graves pour le fonctionnement entier d'une organisation.

Le postulat, volontairement large, souhaite que le Conseil d'Etat examine la situation actuelle en matière de cybersécurité et de cyberattaques et rende un rapport complet, par rapport notamment au rôle que le Canton est amené à jouer dans ce contexte, en particulier auprès des communes. En effet, on a vu récemment que diverses cyberattaques ont affecté directement des communes, celle de Rolle qui a été la plus discutée, mais ensuite également à Montreux. On constate que les cyberattaquants ne se limitent plus à de grandes entreprises, à des pays ou des cantons, mais s'en prennent véritablement à tous les échelons, ciblant les PME ou les administrations communales de plus en plus victimes de cyberattaques. Ces entités sont plus faciles à attaquer

car elles n'ont souvent pas mis en place les standards nécessaires pour faire face, alors même que les données qu'elles traitent ont une valeur importante.

Le système public vaudois présente un grand nombre de communes de tailles différentes, dont de petites communes qui n'ont ni les connaissances, ni les moyens pour disposer d'une cyberadministration suffisamment sécurisée face à des multinationales de la cybercriminalité qui cherchent à entrer facilement et rapidement dans les systèmes pour soustraire des données informatiques. Même si la question de l'autonomie communale est un point fondamental, le postulant estime que le risque informatique concerne les données des citoyens et citoyennes dans leur ensemble.

Dans ce contexte, le postulant considère une palette relativement large de solutions qui vont d'un côté vers la centralisation totale auprès du Canton, comme c'est le cas à Neuchâtel, et de l'autre côté vers l'application de simples standards minimaux proposés par le Canton et combinés avec une potentielle assistance. Entre ces deux côtés de la palette, il existe diverses variantes pour s'assurer que le Canton mette à disposition des communes les moyens et les compétences dont dispose la DGNSI, que cela soit sous la forme d'une centralisation informatique, de critères minimaux, de standards, d'une surveillance ou de subventions par exemple pour obtenir des labels, tels que Cyber-safe.ch qui s'adresse aux communes et collectivités publiques.

3. POSITION DU CONSEIL D'ÉTAT

En préambule, la conseillère d'Etat indique que le responsable de la sécurité à la DGNSI s'est déplacé en personne tout d'abord au Gymnase cantonal de la Broye (GYB) puis dans les deux communes touchées par des cyberattaques afin d'apporter un soutien sur place à la gestion de la crise. Elle indique qu'il s'agissait de trois événements d'ampleurs diverses avec des niveaux de préparation très différents. L'intervention de la DGNSI, comme support et force d'intervention sur la cyberattaque, n'a pas enlevé l'autorité à la commune (Municipalité), notamment en termes de décision et de communication.

La conseillère d'Etat arrive à un constat similaire à celui du député Raedler et ne serait donc pas opposée à répondre à son postulat. Un rapport sur la sécurité informatique donnerait l'occasion au Conseil d'Etat de partager plus largement ses constats, ses interventions dans l'urgence, son dispositif et ses réflexions stratégiques à plus long terme, avec l'ensemble du parlement et pas uniquement avec la CTSI.

Depuis 2013, la DGNSI a mis en place des mesures importantes pour sécuriser le système d'information de l'Etat de Vaud, en créant notamment une unité dédiée et en intervenant aussi bien sur les infrastructures qu'en termes de formation et d'interventions d'urgence. L'octroi par le Grand Conseil de crédits d'investissements conséquents a notamment permis de créer le fameux Security operation center (SOC) et de doubler le *data center* de l'Etat ce qui augmente significativement la capacité de récupération des données en cas d'attaque. Malgré tous ces efforts, le Canton de Vaud n'est pas à l'abri d'une intervention malveillante qui réussisse à pénétrer ses systèmes, c'est pourquoi la conseillère d'Etat reste humble dans ce domaine, le risque zéro n'existant pas.

Il y a effectivement une intensification des attaques. Par le passé, les états, les banques et les multinationales étaient principalement ciblés alors qu'aujourd'hui un canton et même des communes peuvent être victimes de telles attaques informatiques. Cela incite le Conseil d'Etat à continuer à investir, à être proactif au niveau national et intercantonal, ainsi qu'à collaborer avec les entreprises de pointe dans ce domaine. Aujourd'hui, on se retrouve face à une industrialisation de la cybercriminalité, c'est-à-dire des groupes cybercriminels possédant des ressources financières et des compétences techniques importantes qui leur permettent de cibler des entreprises et institutions particulières dans leurs attaques par rançongiciel. Face à cette évolution, la DGNSI doit pouvoir adapter de manière active ses systèmes de cyberdéfense.

Les plus petites entités, telles que les PME ou les communes doivent se départir d'une confiance naïve et cesser de penser que cela n'arrive qu'aux autres, car elles détiennent aussi des informations sensibles et monnayables. Les données volées à une entreprise, notamment des processus industriels ou des secrets de fabrication, peuvent se retrouver sur le *darkweb* offertes au plus offrant. En collaboration avec la Chambre vaudoise du commerce et de l'industrie (CVCI), le Canton a d'ailleurs développé un guide en ligne des bonnes pratiques à l'attentions des entreprises, plus précisément une application mobile simple et gratuite[1].

[1] https://www.vd.ch/fileadmin/user_upload/organisation/dinf/dsi/ussi/vd_secure/

Comme relevé par le postulant, la nature des attaquants a changé. On ne parle plus de hackers isolés, mais on a à faire à des organisations mafieuses avec d'importants moyens et dont la cybercriminalité est devenue un des business extrêmement rentables. Une partie de ces mafias sont d'ailleurs soutenues par des États.

Le Conseil d'Etat (les deux départements en charge des communes et des systèmes d'information) va rencontrer les faîtières des communes, UCV et ACV, afin d'élaborer ensemble une stratégie et un protocole d'actions. Les interventions sur place, dans les communes, de l'unité sécurité informatique de la DGNSI ont mobilisé du personnel spécialisé de l'Etat qui n'est initialement pas prévu pour ce type de missions. Les récentes attaques montrent à l'évidence qu'il faut renforcer la collaboration avec les communes, au moins la transmission des bonnes pratiques, ce qui correspond au standard minimum. Les discussions avec les représentants des deux faîtières vont viser à mettre en place une politique des trois piliers que sont : a) la cyber-prévention (notamment le e-learning) ; b) la cyber-réaction (groupe d'intervention) et c) la cyberdéfense (veille assurée par le SOC). Il faudra discuter avec les communes de la forme que pourrait prendre la mise en place d'une force de réaction en cas d'attaque, une veille de cyber défense, etc.

Sur la base de la stratégie numérique qui comprend déjà un chapitre sur la sécurité, il est temps de mettre en place une stratégie générale de cybersécurité qui englobe l'ensemble des acteurs institutionnels du Canton de Vaud. Le directeur de la sécurité numérique soutient une volonté de coordination qui regroupe les forces, plutôt que chaque entité travaille de son côté. La force du SOC est d'être composé de spécialistes dont les compétences sont stimulées en collaborant au sein de cette cellule.

Le directeur de la sécurité numérique insiste sur le facteur humain et l'importance de sensibiliser l'ensemble des utilisateurs et utilisatrices de l'ACV à la culture de la sécurité. La DGNSI a repris des bonnes pratiques du Centre national pour la cybersécurité (NCSC). Il y a quelques règles essentielles qui participent à ce que l'on appelle l'hygiène informatique ou cyber-hygiène, on parle notamment de sauvegarde et de comportement vis-à-vis des e-mails.

4. DISCUSSION GÉNÉRALE SUR LE POSUTLAT

Confidentialité des mesures de cybersécurité

Un commissaire trouve intéressant que le Conseil d'Etat établisse un rapport sur la cybersécurité et la stratégie de l'Etat de Vaud à ce sujet, mais il craint que les mesures techniques mises en place soient trop sensibles et confidentielles pour être publiées de manière exhaustive à large échelle.

Le Conseil d'Etat communique régulièrement sur l'objectif d'améliorer la résilience aux attaques informatiques. Il n'y a pas de problème, tant que la communication reste au niveau de la stratégique générale de sécurisation, car il s'agit d'exposer des axes d'actions standards. Par contre, la manière de déployer cette stratégie est effectivement secrète, les documents doivent être classifiés confidentiels sans quoi un citoyen peut y accéder en se prévalant de la loi sur l'information (LInfo).

Le niveau plus général de la méthodologie ne pose aucun problème, par contre des niveaux de détails plus précis peuvent effectivement mettre la DGNSI en difficulté, comme par exemple, donner les résultats des campagnes de sensibilisation en indiquant le comportement précis des utilisateurs et les conséquences sur les machines.

Demandes du postulant

Par rapport à la première demande du postulat « favoriser une stratégie identique à celle de la Confédération (SNPC) », une commissaire relève que le Canton de Vaud est déjà partie prenante, depuis le début, de cette stratégie nationale SNPC. Le directeur de la sécurité numérique siège au réseau national de cybersécurité (RNS) au sein duquel le Canton de Vaud porte, pour l'ensemble des cantons, la thématique de l'identification des cybermenaces. Les démarches au niveau cantonal sont donc en ligne avec la stratégie nationale.

Le directeur de la sécurité numérique précise que la stratégie numérique du Conseil d'Etat présente globalement la manière d'appréhender la thématique de la cybersécurité en conformité avec la stratégie nationale. Dans chacun des chapitres de sa stratégie, le Conseil d'Etat décline déjà des éléments de cyber-sécurité. Pour répondre au postulant, la DGNSI trouve pertinent de formaliser sa stratégie en précisant qu'elle inclut dans sa démarche les acteurs étatiques (Confédération, canton, communes), académiques et économiques.

Le postulant tient à relever que le Canton de Vaud a été proactif et a fait un très bon travail en renforçant la sécurité de ses systèmes d'information dès 2013, en mettant notamment en service le SOC. Face à un nouveau développement de ces attaques, le Conseil d'Etat doit renforcer et adapter ses mesures, il sera intéressant qu'il présente sa stratégie au Grand Conseil et qu'il décrive la manière dont il s'aligne sur la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC).

Risques de la centralisation

Une commissaire relève que le fait de passer à un système unique au niveau cantonal augmenterait possiblement le risque d'attaques ; il y aurait un plus grand nombre de portes d'entrées sur une masse plus large de données. Sans centraliser l'informatique au niveau cantonal, les communes pourraient travailler avec les mêmes logiciels, cela faciliterait notamment la gestion des données lors de fusions de communes.

La conseillère d'Etat confirme que l'impact du *hacking* serait bien plus massif en cas de centralisation des données. A ce titre, le Canton de Vaud a fortement combattu la volonté fédérale de centralisation absolue sur un seul site en matière d'authentification (e-ID). La souveraineté des communes et le respect de l'ordre constitutionnel sont les principales raisons qui conduisent le Conseil d'Etat à ne pas soutenir un système informatique cantonal unique. Le niveau de protection des données et les budgets y relatifs restent un choix des communes.

A la place d'un système informatique centralisé, la conseillère d'Etat prône une convergence de vision sur la cybersécurité, un échange d'informations, un partage des standards et surtout des capacités de réaction mutualisées.

Formation

La conseillère d'Etat propose d'élargir les formations offertes aux communes par le Centre d'éducation permanente (CEP), dans le domaine de la sécurité informatique. Il faudra aussi s'adresser aux entités parapubliques, telles que l'AVASAD (Association Vaudoise d'Aide et de Soins à Domicile), etc. Pour la formation (e-learning), un commissaire propose d'utiliser la plateforme d'apprentissage numérique existante VDACADEMIE. En collaboration avec le RNS, une formation est d'ailleurs prévue pour toutes les administrations cantonales et communales par le biais de VDACADEMIE.

La sécurité informatique est un sujet de préoccupation permanent et au vu du travail déjà réalisé par la DGNSI, un commissaire estime que la réponse au postulat ne devrait pas générer un surplus de travail trop important. Lui-même actif dans le domaine de la formation, il est particulièrement intéressé par le point qui demande « d'assurer la continuité et l'essor de la formation des apprentis aux métiers de l'informatique et de la cybersécurité ». Le point faible reste très souvent l'utilisateur et le meilleur moyen de lutter contre ce risque est évidemment de former les gens.

Il faut parler des risques de cyberattaques. A cet égard, un rapport au plénum permettra de sensibiliser un plus grand nombre de député.es voir au-delà si la presse s'en fait l'écho. Ce postulat doit être utilisé comme un moyen de communication pour rassurer la population que le Canton de Vaud agit très sérieusement et investit depuis de nombreuses années dans le domaine de la cybersécurité, il permettra aussi d'insister sur la formation des utilisatrices et des utilisateurs qui sont le principal maillon faible du système.

Protection active au niveau communal

Un commissaire rappelle que plusieurs crédits ont déjà été votés par le Grand Conseil pour la mise en place de mesures de sécurité. Il confirme aussi qu'il y existe des synergies avec la stratégie nationale de protection contre les cyberrisques. Il partage les inquiétudes déjà exprimées sur la vulnérabilité de certaines petites communes. Il pense que le Canton et les communes doivent se mettre ensemble pour faire face à la menace. Certaines communes ont un intérêt financier à mutualiser les mesures pour lutter contre la cybercriminalité.

Le postulant estime qu'une aide concrète auprès des communes en matière de cybersécurité se justifie pour protéger l'intérêt public. Dans la conclusion de son rapport, le Conseil d'Etat pourra définir les besoins et les moyens nécessaires en termes de formation, d'intervention, etc. au niveau des communes et des associations de communes.

Un commissaire est rassuré d'entendre, de la part de la conseillère d'Etat, que la collaboration avec les communes et les entreprises va se structurer et s'intensifier, car il constate qu'on passe d'une vieille passive à une surveillance beaucoup plus active comprenant des actions préventives. Dès lors, il se déclare plus enclin à soutenir ce postulat et à obtenir des informations sur les développements relatifs aux mesures de protection contre les cyberattaques.

Il trouve qu'en demandant d'élaborer les voies d'action cantonales permettant de faire face aux risques concrets et actuels liés aux cyberattaques, l'intervention parlementaire se rapproche d'une motion. Il demande si le Canton a réellement pour mission d'assurer un standard minimum en validant la formation des responsables informatiques des communes.

La conseillère d'Etat prend le postulat dans son esprit, pas forcément à lettre, c'est-à-dire la préoccupation d'élever le niveau de compétence des responsable informatiques communaux (standard minimum). Le Canton collabore déjà avec l'association vaudoise des responsables informatiques communaux (AVRIC), mais le Conseil d'Etat n'est pas une autorité de validation des compétences informatiques. Pour les plus petites communes, il serait intéressant de connaître le cahier des charges qu'elles donnent à leur prestataire de service externe.

Pour les communes, un commissaire préconise un standard de connexion minimum.

Le postulat permettra au Conseil d'Etat de présenter ce qui est déjà mis en place. Il pourra aussi développer le lien Canton-communes dans le domaine de la sécurité informatique et rejoindre les forces (mutualisation de systèmes d'information et des expertises). La sécurité informatique doit devenir une priorité aussi dans les petites communes.

5. AMENDEMENT ET VOTE SUR LA PRISE EN CONSIDÉRATION DU POSTULAT

5.1. PROPOSITION D'AMENDEMENT / PRISE EN CONSIDÉRATION PARTIELLE

Afin de ne pas contraindre les communes à respecter un standard cantonal et maintenir leur autonomie, un commissaire propose l'amendement suivant à la deuxième demande :

« …assurer un standard minimum devant **ou pouvant** être respecté par les Communes et associations de Communes, possiblement en validant la formation des responsables communaux en charge de la détection des risques de cyberattaques ainsi que des réponses y apportées, de même qu'en intégrant des exigences en termes de sensibilisation du personnel communal. ».

Le postulant souhaite tout de même une réponse sur les avantages qu'il y aurait à implémenter, dans toures les communes, un standard minimum.

5.2. VOTE

A l'unanimité, la CTSI recommande au Grand Conseil de prendre en considération ce postulat tel que modifié ci-dessus et de le renvoyer au Conseil d'Etat.

Chardonne, le 11 janvier 2022

Le rapporteur :
(Signé) Maurice Neyroud