canton de vaud
LIBERTÉ ET PATRIE

RAPPORT DU CONSEIL D'ETAT AU GRAND CONSEIL
sur 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 (21_POS_44)

Rappel du postulat

Chaque jour apporte malheureusement son lot de nouveaux piratages, ransomwares et failles de sécurité qui mènent à la divulgation ou la perte de nombreuses données personnelles et autres informations sensibles pour les personnes concernées. Loin de se limiter à quelques rares cas, ces incidents touchent l'entier de la société. Multinationales, PME, individus et services étatiques : tous sont des cibles potentielles de telles attaques[1]. Avec à la clé un risque très marqué pour les personnes concernées, qui s'étend non seulement à la violation de leur sphère privée, mais aussi aux risques économiques qui peuvent découler d'une utilisation des informations volées ou des conséquences de leur perte.

Avec une numérisation toujours plus utilisée, et une valeur des informations toujours plus importante, ces incidents vont en croissant. Chaque semaine, le Centre national pour la cybersécurité (NCSC) reçoit plusieurs centaines d'annonces portant sur des incidents touchant au domaine informatique (fraudes, fuites de données, hameçonnage, piratage informatique, etc.)[2]. Dans l'ensemble du panorama économique, près de 40 % des entreprises sont visées par des cyberattaques – un chiffre qui, en France, a augmenté de 543 % en 2020 par rapport à 2019[3]. C'est dire s'il y a urgence.

Dans ce contexte très inquiétant, les entités et administrations publiques ne sont de loin pas épargnées. Par la sensibilité des informations qu'elles traitent, et le détail de celles qu'elles reçoivent, les administrations publiques sont des cibles privilégiées. Ceci a fortiori en raison du nombre de personnes qu'elles emploient et qui, malheureusement, constituent autant de portes d'entrées d'une cyberattaque. Le cas très récent de la Commune de Rolle n'est qu'un exemple parmi de nombreux autres de l'importance que les administrations publiques revêtent aux yeux des pirates[4]. Et des conséquences très graves qui peuvent en découler pour les personnes dont les données personnelles sont volées.

Le Canton de Vaud déploie des efforts pour protéger au mieux ses moyens et services informatiques à l'aide de la Direction générale du numérique et des systèmes d'information (DGNSI)[5]. Dans le même sens, la Confédération a développé ces dernières années son arsenal de lutte contre les cyberattaques, notamment par le biais du NCSC, ainsi que par une collaboration de principe entre l'administration fédérale d'une part et, notamment, les cantons et communes d'autres part (art. 4 al. 2 de l'Ordonnance sur les cyberrisques [OPCy]). Cela étant, les Communes demeurent souvent laissées à leur propre responsabilité. Quelque chose qui s'avère surtout problématique pour les communes de petite ou moyenne taille, et représente un réel problème compte tenu de l'importance des dangers auxquels elles font face.

Dans l'ensemble, les risques liés à une cyberattaque dépassent largement le seul champ de compétence des communes, en tant qu'elles portent préjudice directement aux habitant.e.s du Canton et peuvent également mener à dévoiler des documents sensibles pour la politique publique. La complexité des attaques exige elle-même des connaissances très poussées dépassant ce cadre, tout comme l'importance de la sensibilité à assurer auprès de toutes les personnes employées au sein des administrations communales.

Pour ces motifs, et compte tenu de l'augmentation exponentielle des cyberattaques qui a été constatée spécialement cette dernière année, il est impératif que le Canton s'aligne sur la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) avalisée par la Confédération dans les 7 domaines recensés tendant à assurer par anticipation une protection contre les failles de sécurité de la télématique.

Dans ce cadre, le rôle de l'Etat doit notamment être :

- *de former le personnel dans toutes les couches opérationnelles informatiques de l'apprenti à l'ingénieur reconnus par le système de certification suisse ;*
- *d'offrir aux administrations communales, ainsi qu'aux associations de Communes, un réseau sécurisé pour ses applications de gestion des registres cantonaux et communaux (bâtiments, personnes, etc.) ; et*
- *assurer un standard minimum devant être respecté par les Communes et associations de Communes, possiblement en validant les compétences des responsables informatiques des communes.*

En conséquence, et par le présent postulat, les signataires demandent au Conseil d'Etat d'élaborer les voies d'action cantonales permettant de faire face aux risques concrets et actuels liés aux cyberattaques, en particulier de façon à :

- *favoriser une stratégie identique à celle de la Confédération (SNPC) ;*
- *assurer un standard minimum devant 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 ;*
- *assurer la continuité et l'essor de la formation des apprentis aux métiers de l'informatique et de la cybersécurité ;*
- *établir un plan directeur cantonal de cybersécurité pour maintenir les infrastructures et les logiciels jusqu'à l'échelon des communes et assurer un accès des citoyens aux cyberprestations sécurisées.*

Rapport du Conseil d'Etat

Le Conseil d'Etat est parfaitement conscient et partage les constats concernant l'évolution des cybermenaces et la diversité des profils des victimes. Comme relevé par le postulant, la nature des attaquants a changé ; il ne s'agit habituellement plus de hackers isolés, mais d'organisations mafieuses disposant d'importants moyens pour industrialiser leurs cyberattaques. Ces acteurs malveillants ne cessent d'affûter leurs techniques afin de pouvoir en tirer une « rentabilité financière » la plus importante pour eux. Il est aussi à relever que certains de ces acteurs malveillants sont proches ou même malheureusement soutenus par des Etats, disposant ainsi de moyens et compétences quasi illimités.

Comme il l'a déjà démontré, le Conseil d'Etat n'entend pas être passif face à l'évolution des cybermenaces. Il continue d'investir et d'accompagner les différents acteurs étatiques et économiques vaudois pour améliorer globalement la cyberrésilience du Canton. Dans ce contexte, il est à relever notamment la création de la force cantonale d'intervention cybersécurité (CSIRT) née d'une volonté politique du Canton et des communes. Celle-ci est opérationnelle depuis le 1er janvier 2024 et développe aujourd'hui des services sur 3 axes principaux :

1) La cyberréaction apportant une méthodologie et des ressources pour la gestion de crise et la réponse technique à un cyberincident ;
2) La cyberrésilience pour renforcer la cybersécurité et qui s'appuie sur la définition de standards minimaux de sécurité et de protection des données. Cet axe s'appuie également sur un travail important de veille sur les cybermenaces qui fait déjà l'objet d'un rapport mensuel de cybermenaces préparé par les experts du SOC (Security Operation Center), le centre opérationnel de sécurité de la DGNSI ;
3) La cyberprévention capitalisant sur les formations, mais aussi sur la création de communautés et, en particulier, celle regroupant les répondants cybersécurité des 300 communes et 137 associations intercommunales.

Au niveau de l'Administration cantonale vaudoise (ACV), le Plan directeur cantonal IT 2023-2028 est en parfaite ligne avec les attentes et propositions du postulant. Il a en effet pour objectif clé de poursuivre le renforcement de la protection des données de la population et des entreprises vaudoises. Il entend notamment consolider la sécurité des SI et améliorer ses performances pour faire face à l'évolution des risques et répondre à l'attente des services de l'Etat et des usagères et usagers. Pour rappel, ce plan directeur vise en particulier à :

- Renforcer le niveau de sécurité des SI (systèmes d'information) critiques pour le fonctionnement de l'Etat ;
- Améliorer la résilience et les temps de réponse des SI ;
- Répondre à la croissance et au perfectionnement des cyberattaques ;
- Mettre en œuvre les nouvelles exigences en matière de protection des données personnelles ;
- Intégrer les principes liés à la politique générale de la donnée.

Il est à relever que ces principes œuvrent également à poursuivre le développement de la souveraineté numérique de l'Etat.

Le Conseil d'Etat souhaite encore rappeler à cette occasion son engagement pour la cybersécurité et la confiance numérique. Celles-ci bénéficient d'initiatives uniques reconnues en Suisse et portées par la promotion économique et de l'innovation réalisées en collaboration étroite avec les acteurs académiques du Canton. Il convient en particulier de mentionner :

1) L'écosystème hyperdynamique provoqué par la Trust Valley pilotant le programme d'accompagnement cybersécurité « Trust4SMEs » développé pour les entreprises et qui est maintenant une référence au niveau de la Suisse ;
2) L'initiative « SEAL Innovation » qui souhaite promouvoir une démarche d'innovation structurée pour la génération d'idées dans le domaine de la lutte contre la cybercriminalité avec les 3 acteurs académiques majeurs locaux, à savoir l'EPFL (Ecole polytechnique fédérale de Lausanne), l'UNIL (Université de Lausanne) et l'HEIG-VD (Haute école d'ingénierie et de gestion du Canton de Vaud).

Le Conseil d'Etat a l'honneur de répondre aux questions du postulat :

1) Favoriser une stratégie identique à celle de la Confédération (SNPC).

En préambule, il convient de rappeler que le Conseil d'Etat vaudois confirme son engagement à publier une Stratégie cantonale de cybersécurité, conformément à son programme législatif. Cette stratégie s'inscrit dans le cadre de la Cyberstratégie nationale (CSN) et répond aux besoins fondamentaux de sécurité et de confiance découlant de la stratégie numérique du Canton de Vaud. Le Conseil d'Etat prévoit de publier sa stratégie de cybersécurité d'ici fin 2024.

La future stratégie cantonale de cybersécurité prévoit de s'articuler autour de trois axes d'action principaux, également alignés sur les priorités de la CSN de la Confédération :

1. La cyberprévention :

- Développement des compétences en matière de cybersécurité : cet axe vise à sensibiliser et accompagner les individus, les collectivités et les entreprises à la protection des données personnelles et aux bonnes pratiques de sécurité, afin de davantage les responsabiliser face aux cybermenaces.

2. La cyberrésilience :

- Amélioration et mesure de la maturité en matière de cybersécurité : cet axe vise à aider les acteurs à renforcer leur capacité à gérer et à se défendre contre les cyberattaques, assurant ainsi la fiabilité et la disponibilité de l'infrastructure et des services numériques. Il s'agit également d'établir des règles fondamentales et des standards minimaux attendus des entreprises et des collectivités par le Canton, à l'instar du code routier.

3. La cyberréaction :

- Préparation à la gestion des cybercrises et des cyberincidents : cet axe vise à fournir des procédures et des outils aux individus, aux collectivités et aux entreprises pour réduire l'impact et la durée d'une cyberattaque sur eux. Il s'agit en priorité de faire connaître les bons réflexes d'urgence et d'améliorer la gestion des cybercrises et des cyberincidents.

Par ces actions coordonnées, la stratégie cantonale de cybersécurité s'inscrit pleinement dans la stratégie nationale, contribuant ainsi à la sécurité globale du cyberespace suisse. Elle renforce par ailleurs le volet cantonal des actions en considérant que :

- La stratégie cantonale prend en compte les besoins et les défis spécifiques du Canton de Vaud en matière de cybersécurité.
- Elle définit des actions concrètes et des mesures opérationnelles adaptées au contexte cantonal.
- Elle met l'accent sur la collaboration et le partage d'informations avec la Confédération et également entre les acteurs intercantonaux.

En complément de ces trois axes, le Conseil d'Etat souligne l'importance de la collaboration et du partage d'informations entre les différents acteurs cantonaux. Il encourage la collaboration par le biais du Réseau national de sécurité (RNS). La Confédération est en effet un partenaire clé en matière de cybersécurité, et des rencontres fréquentes sont organisées pour échanger sur les travaux respectifs et s'assurer de l'alignement des stratégies. Une collaboration étroite est entretenue sur divers sujets, tels que la sensibilisation auprès des communes ou l'établissement de standards minimaux, en veillant à éviter les redondances.

2) Assurer un standard minimum devant 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 apportées, de même qu'en intégrant des exigences en termes de sensibilisation du personnel communal.

Le Conseil d'Etat adhère pleinement à l'idée d'établir un standard minimum de cybersécurité, qui est par ailleurs un axe central de sa future stratégie cantonale de cybersécurité.

Dans l'objectif de renforcer la résilience du Canton, un standard minimum de cybersécurité est, par exemple, en cours d'élaboration par la Force d'intervention cybersécurité cantonale (CSIRT), en étroite

collaboration avec les communes. Ce standard est également développé en coordination avec la Confédération et s'appuie sur la norme minimale pour les technologies de l'information et de la communication (TIC) établie par l'Office fédéral pour l'approvisionnement économique du pays (OFAE).

Le standard minimum définira des directives claires sur les mesures à mettre en place, que les communes pourront implémenter elles-mêmes ou transmettre à leur prestataire informatique. Les premiers volets du standard porteront sur la protection périphérique et la gestion des fournisseurs, en particulier la gestion de la sécurité dans le contexte d'externalisation des services informatiques. Ces thématiques ont été identifiées comme prioritaires à la suite des cybercrises survenues dans les communes.

En outre, les outils, les formations et bonnes pratiques développés pour le Canton sont mis à disposition des communes, afin d'assurer une cohérence et une efficacité maximales dans la gestion de la cybersécurité.

Des formations et sensibilisations ponctuelles sont également organisées pour compléter les compétences des responsables communaux en charge de la cybersécurité et sensibiliser l'ensemble du personnel communal aux risques de cyberattaques et aux bonnes pratiques en matière de cybersécurité.

L'établissement d'un standard minimum de cybersécurité constitue aussi pour le Conseil d'Etat une étape clé pour renforcer la posture de sécurité du Canton et protéger ses communes contre les cybermenaces.

3) Assurer la continuité et l'essor de la formation des apprentis aux métiers de l'informatique et de la cybersécurité.

Le Conseil d'Etat tient en premier lieu à rappeler qu'en matière de formation professionnelle initiale, les cantons ne sont souverains ni dans le développement de nouveaux métiers ni dans l'adaptation des contenus de ceux déjà existants. Ces prérogatives sont légalement l'apanage des associations professionnelles qui adaptent les besoins en matière de formation aux besoins du marché et assurent la promotion de leurs propres métiers afin de veiller à la présence d'une main-d'œuvre qualifiée. Quant aux cantons, ils sont responsables de la mise en œuvre et en assurant l'organisation et le financement majoritaire de la formation dans les écoles professionnelles (pour 75 %), l'orientation professionnelle, la surveillance des entreprises formatrices et des cours interentreprises, le cofinancement de ces cours, ainsi que l'organisation des procédures de qualification (examens théoriques et pratiques).

Ce rappel du partage des responsabilités effectué, le Conseil d'Etat relève cependant être tout à fait conscient des enjeux propres aux pénuries de main-d'œuvre qualifiée relevées dans toute une série de secteurs professionnels, dont l'informatique fait partie, et entend déployer différentes actions pour y pallier.

Ainsi, les demandes d'admission dans les filières d'informatique à plein-temps excédant ces dernières années l'offre de places de formation, une antenne complémentaire de l'Ecole technique des métiers de Lausanne (ETML) a été ouverte en 2022 sur le site de Vennes. Cette extension n'ayant toutefois pas permis de répondre pleinement à la demande, il est prévu d'ouvrir quelque 240 places supplémentaires au sein de la nouvelle Ecole de Payerne, dont la mise en service est prévue pour 2027.

Parallèlement à cet effort étatique sur les places de formation à plein-temps, la DGEP (Direction générale de l'enseignement postobligatoire) est régulièrement en contact avec le Groupement Romand de l'Informatique (GRI), association professionnelle régionale qui représente les intérêts de cette branche professionnelle, afin de trouver des solutions innovantes à même d'augmenter le nombre de titulaires de CFC (certificat fédéral de capacité) sur le marché de l'emploi. Ces deux dernières années, les projets suivants ont ainsi été concrétisés en collaboration avec cette entité :

- Une Junior Team, à savoir une équipe de 6 à 8 apprentis se formant au même métier sous la responsabilité d'un formateur à plein temps et fonctionnant comme une petite entreprise, a été créée en 2023 par le GRI avec un soutien financier de la DGEP. Ce modèle pédagogique innovant permet non seulement d'augmenter le nombre de places d'apprentissage, mais aussi de garantir un haut niveau de réussite des apprentis. Il s'adresse aux jeunes visant un CFC d'informaticien ;
- Le GRI a déployé en ses murs, dès 2023, un modèle de formation mixte qui permet aux entreprises d'envoyer leur apprenti-e de 1re année dans cette structure similaire à une formation en école avant de l'accueillir dans leurs locaux dès la 2e année de formation. D'une capacité maximale d'une douzaine de places pour des jeunes visant l'obtention du CFC d'informaticien, cette mesure permet

d'encourager les jeunes qui auraient des appréhensions à rejoindre le monde de l'entreprise tout de suite après leur scolarité obligatoire, d'effectuer une transition plus souple tout en allouant aux entreprises, qui parfois estiment le travail de formation à réaliser en 1re année trop chronophage, la possibilité de déléguer cette première partie à une entité externe professionnalisée pour ce faire. A noter que dans le cas où le modèle viendrait à rencontrer un succès important et dépasserait les capacités offertes par le GRI, l'ETML est disposée à lui offrir son soutien en ouvrant à son tour une classe de formation mixte supplémentaire ;

- Compte tenu du nombre de personnes travaillant dans l'informatique sans certification et pour faciliter les reconversions professionnelles dans ce domaine, des dispositifs de formation à l'attention des adultes visant une qualification par l'article 32 OFPr (Ordonnance sur la formation professionnelle) ont également été déployés ces dernières années. Il est ainsi possible de faire reconnaître ses compétences grâce à une validation des acquis de l'expérience (VAE), ce tant pour obtenir le CFC d'informaticien que celui d'opérateur en informatique CFC[1]. En outre, une classe de préparation aux examens d'opérateur en informatique a également été développée, grâce à une collaboration entre le GRI et l'EPSIC, à Lausanne[2] ;
- Enfin, un nouveau projet de Junior Team, cette fois-ci à destination des jeunes visant un CFC d'opérateur en informatique, est actuellement à l'étude au Centre d'Orientation et de Formation professionnelle (COFOP) à Lausanne. Son ouverture est prévue pour la rentrée d'août 2025.

Le Conseil d'Etat relève en outre que dans le cadre de son plan d'action en faveur de la formation professionnelle initiale[3], une campagne cantonale de promotion en faveur de l'apprentissage est prévue dès l'année 2025. Dans ce contexte, les métiers de l'informatique, tout comme ceux faisant face à une importante pénurie de main-d'œuvre qualifiée, seront particulièrement mis en avant.

4) Etablir un plan directeur cantonal de cybersécurité pour maintenir les infrastructures et les logiciels jusqu'à l'échelon des communes et assurer un accès des citoyens aux cyberprestations sécurisées.

Le Conseil d'Etat a pris la décision d'intégrer l'aspect cybersécurité directement dans le Plan directeur cantonal des systèmes d'information pour la législature 2023-2028. Influencé par la mise en œuvre de la stratégie numérique, ce plan directeur vise à atteindre des systèmes d'information cibles sécurisés.

Pour concrétiser cet objectif ambitieux, la direction Sécurité de la Direction générale du numérique et des systèmes d'information (DGNSI) s'est fixé six objectifs stratégiques :

1. **Améliorer la culture sécurité** en sensibilisant les utilisatrices et utilisateurs aux bonnes pratiques au travers de formations.
2. **Renforcer la protection des données** en améliorant la gestion de la sécurité de l'information, en promouvant les solutions de confiance numérique et en réduisant le risque de fuite de données en évoluant vers une architecture basée sur l'accès aux données.
3. **Optimiser la gestion des identités et des accès** en étendant la vue globale sur les droits d'accès intégrant les services en ligne et en intégrant de nouvelles solutions d'authentification.
4. **Améliorer la résilience des systèmes d'information** et s'assurer que la continuité des métiers critique est alignée avec la continuité informatique et en réduisant l'exposition aux cybermenaces.
5. **Répondre aux incidents de sécurité** en renforçant la position du SOC comme acteur clé local en matière de cybersécurité et en mettant en place la convention cyberréaction pour les communes.
6. **Renforcer le cadre réglementaire et législatif** en publiant un Règlement IAM (Identity and Access Management) et en déployant une stratégie de cybersécurité.

La mise en œuvre de ces six objectifs stratégiques nécessitera des investissements additionnels pour la sécurité des informations et la cybersécurité qui seront proposés au Conseil d'Etat, puis soumis au Grand Conseil prochainement.

[1] https://www.vd.ch/formation/formations-pour-les-adultes/certification-professionnelle-pour-adultes-cfc-afp/validation-des-acquis-de-lexperience-vae
[2] https://www.gri.ch/2021/09/21/ict-32/
[3] Le plan d'action de la valorisation de la formation professionnelle est consultable à l'adresse suivante : https://www.vd.ch/fileadmin/user_upload/accueil/fichiers_pdf/2022_novembre/Formation_professionnelle_plan_d-action_2022.pdf

CONCLUSION

Face à l'augmentation croissante des cyberattaques, le Conseil d'Etat prend la situation très au sérieux et met en œuvre des mesures concrètes pour protéger les citoyens vaudois. La publication d'une stratégie cantonale de cybersécurité d'ici fin 2024 est un élément clé de cette approche.

La mise en œuvre d'un standard minimum de sécurité, l'essor de la formation professionnelle dans le domaine de la cybersécurité, ainsi que le développement d'une culture de sécurité au sein des administrations et des entreprises sont des mesures cruciales pour protéger les données et garantir la confiance numérique. En travaillant de concert avec les communes, les associations et les partenaires académiques, le Canton de Vaud se dote des outils nécessaires pour faire face à ces défis et assurer la sécurité numérique de tous ses citoyens.

Le Conseil d'Etat s'engage à poursuivre ces efforts, convaincu que seule une approche coordonnée et proactive permettra de renforcer durablement la cyberrésilience du Canton.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 18 septembre 2024.

La présidente :	Le chancelier :
C. Luisier Brodard	*Michel Staffoni*