canton de vaud

GRAND CONSEIL

DÉCEMBRE 2019 RC-147

RAPPORT DE LA COMMISSION
chargée d'examiner l'objet suivant :

Exposé des motifs et projet de décret accordant au Conseil d'Etat un crédit d'investissement de CHF 9'506'000 pour financer l'étape 2 de la mise en place de mesures de diminution des risques relatifs à la sécurité de l'information et à la cyber-sécurité

1. PREAMBULE

La Commission thématique des systèmes d'information (CTSI) s'est réunie le mardi 27 août 2019 à la Salle du Bicentenaire, Place du Château 6 à Lausanne, pour traiter de cet objet.

Elle était composée de M. Maurice Neyroud (président et rapporteur), de Mmes les députées Taraneh Aminian, Céline Baux, Joséphine Byrne Garelli, Carine Carvalho, Carole Schelker, et de MM. les députés Jean-François Chapuisat, Fabien Deillon, Maurice Gay, Philippe Jobin, Daniel Meienberger, Etienne Räss, Alexandre Rydlo.

Excusés : MM. Stéphane Balet et Didier Lohri.

Mme la conseillère d'Etat Nuria Gorrite, cheffe du Département des infrastructures et des ressources humaines (DIRH), a également assisté à la séance, accompagnée de M. Patrick Amaru, directeur de la direction générale du numérique et des systèmes d'information (DGNSI), et de M. Marc Barbezat, responsable de la sécurité informatique et de la cyber-sécurité 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 CONSEIL D'ETAT

Le présent EMPD poursuit les actions entreprises avec l'EMPD 61 de 2013 si bien qu'en additionnant ces deux décrets, l'Etat aura investi environ CHF 18'000'000.- en dix ans dans le domaine de la sécurité numérique. La cheffe du DIRH souligne tout d'abord les succès accomplis dans l'étape d'initiation de la sécurisation des systèmes d'information. Elle rappelle notamment les actions entreprises :

- dans la formation du personnel aux nouveaux systèmes numériques, dans le but de garantir une confiance numérique ;
- dans la mise en place d'un meilleur cloisonnement des systèmes d'information avec la restriction des droits d'administrateur ;
- dans la création du SOC (Security Operation Center) qui permet en permanence de détecter, analyser et traiter les événements affectant les systèmes d'information et, le cas échéant, de rétablir la situation ;
- et enfin, dans la mise en œuvre d'une solution back-up avec un second centre de données au sein duquel les données sont quotidiennement sauvegardées et peuvent être récupérées en cas d'attaques informatiques.

Le présent EMPD (147) vise à renforcer davantage ces quatre axes. La première vague d'internalisation de 53 ETP a permis une meilleure maîtrise de la sécurité informatique et de réaliser des économies. Par conséquent, une seconde vague d'internalisation des ressources externes est également proposée dans le présent EMPD pour assurer un financement pérenne des mesures de sécurité. Le directeur de la DGNSI souligne que cette seconde vague d'internalisation de 45 ETP devrait permettre de réaliser près de 1.7 million d'économie sur le budget de fonctionnement.

3. DISCUSSION GENERALE

Formation des collaborateurs

Les modules de formation sont destinés au personnel de l'ACV, les collaborateurs de l'UNIL et du CHUV disposent de leur propre système d'information et ne sont donc pas concernés. Cela représente au final environ 13'000 collaborateurs. Ces modules sont obligatoires et se présentent sous la forme d'e-modules. La cheffe du DIRH souligne également le niveau toujours plus pointu des attaques informatiques et l'importance de ces modules de formation pour les prévenir.

Le directeur de la DGNSI précise que les formations se focaliseront principalement sur le personnel de l'ACV mais que deux autres actions à plus grande échelle sont envisagées. Une application destinée aux PME pour les aider à mieux gérer les risques informatiques et une collaboration avec la DGEO (Direction générale de l'enseignement obligatoire) pour mener des actions de sensibilisation ciblées.

Internalisation des ressources externes

A plusieurs reprises sera posée la question de l'impact de l'internalisation de personnel sur le budget de fonctionnement, et de plus amples explications seront demandées sur sa fonction compensatoire.

Il est précisé que le tableau en page 19 du présent EMPD récapitule les coûts de fonctionnement et que les compensations des charges par les économies nettes de l'internalisation sont indiquées pour la période allant de 2019 à 2023. Une fois l'opération complétée, le montant de la compensation annuelle se monte à CHF 1'682'000.-.

Un député s'interroge sur la manière dont les compensations ont été calculées et sur la pertinence de recourir à une internalisation. A cet égard, la précédente campagne d'internalisation est une source précieuse d'informations qui permet de connaître de manière précise le montant des économies réalisées et qui fournit également une expérience en matière de négociations des contrats.

Il est demandé s'il serait pertinent d'allouer des ressources dans des collaborateurs ayant des compétences spécifiques sans qu'il ne soit nécessaire d'internaliser ces postes.

La cheffe du DIRH explique que la politique du personnel de l'Etat se construit sur deux temporalités : les fonctions pérennes pour lesquelles des contrats de travail sont mis en place et les interventions ponctuelles requérant des compétences pointues et qui sont confiées à des mandataires externes spécialisés permettant une meilleure souplesse pour l'exécution du projet.

Au président qui se demande s'il sera possible de continuer à internaliser les postes, la cheffe du DIRH estime que cela dépend des capacités d'absorption de l'Etat, mais une troisième vague lui semble envisageable.

4. EXAMEN POINT PAR POINT DE L'EXPOSE DES MOTIFS

(Seuls les points débattus en complément de la discussion générale sont mentionnés ci-dessous)

4.1. POINT 1.4 DE L'EMPD : ANALYSE DE LA SITUATION ACTUELLE

Le responsable de la sécurité informatique et de la cyber-sécurité de la DGNSI estime que les attaques informatiques puis les destructions logiques et physiques sont les postes qui comportent le plus de risques et qui nécessitent des investissements en priorité. Il se veut rassurant sur le fait que les risques sont présents mais que les mesures qui seront mises en place sont des protections de plus en plus performantes qui permettent de les limiter.

Le directeur de la DGNSI ajoute que les pirates sont capables de crypter les données mais également de remonter sur les back-up réalisés. A ce titre, il met l'accent sur la nécessité de mettre à jour régulièrement les mesures de sécurité de l'information pour prévenir et restreindre le périmètre de ces attaques.

Le président mentionne l'application qui offre des recommandations aux entreprises en matière de cyber-sécurité et invite le Conseil d'Etat à faire la promotion de ce type de prestations.

La cheffe du DIRH précise que l'Etat collabore d'ores et déjà avec des associations économiques vaudoises pour la diffusion et la promotion de cette application. Elle ajoute qu'il ne suffit pas que l'ACV ait un système de sécurité de l'information performant puisque des organisations en contact avec elle peuvent involontairement servir de relais aux pirates informatiques comme ce fut le cas dans la seule attaque ayant brièvement paralysé le site de l'ACV. Par conséquent, il est essentiel de construire une chaîne de confiance numérique avec les individus, les communes et les entreprises.

Une députée se demande quels moyens seront déployés en matière de procédures judiciaires.

Le responsable de la sécurité informatique et de la cyber-sécurité de la DGNSI explique que le projet comprend une augmentation des capacités de détection qui permettent à la fois d'améliorer la prévention et de fournir des traces numériques à la police pour ses investigations.

Un député se demande si la Suisse et le canton disposent de moyens de défense suffisants pour lutter contre la cybercriminalité internationale.

Le directeur de la DGNSI estime que la police dispose de nombreux moyens d'action contre les attaques informatiques mais que ces moyens sont limités lorsque les attaques proviennent de l'étranger, ce qui est très majoritairement le cas.

Le responsable de la sécurité informatique et de la cyber-sécurité de la DGNSI, qui appartient au groupe de travail au sein du réseau national de sécurité (RNS), explique que le présent EMPD vise à améliorer la cyber-sécurité du canton mais également à renforcer la collaboration avec d'autres cantons et la Confédération. Il estime que la réflexion sur la lutte contre la cybercriminalité doit en revanche se faire à l'échelle internationale ou du moins à l'échelle fédérale avec une mutualisation des compétences. Le canton de Vaud étant bien positionné en matière de sécurité informatique, une réflexion sur ce type de collaboration lui semble pertinente.

4.2. POINT 1.5 DE L'EMPD : CONTENU ET LIMITES DU PROJET

Un député remarque que le budget alloué au poste des contrôles d'accès est assez faible.

Le contrôle d'accès physique est déjà en place et le budget sera alloué non pas à de l'installation mais à des remplacements de matériel. Le responsable de la sécurité informatique et de la cyber-sécurité de la DGNSI souhaiterait pouvoir combiner accès physique et accès informatique pour une plus grande sécurité des accès.

4.3. POINT 1.8 DE L'EMPD : COUT DE LA SOLUTION

Une députée remarque que les renforts sont désignés sous l'appellation « homme », en particulier comme unité de mesure pour déterminer la charge de travail jour / homme (j*h). Elle demande que les prochains EMPD utilisent une formulation non-genrée telle que l'appellation « personne » pour désigner les collaborateurs et collaboratrices.

Une députée demande des explications sur les raisons pour lesquelles est mise en place une deuxième salle de secours dont le coût de fonctionnement s'élève à CHF 400'000 par an. Le directeur de la DGNSI précise qu'il s'agit d'une extension de la salle de secours existante qui permettrait d'accueillir des machines de production ou de développement si cela s'avère nécessaire.

4.4. POINT 3.7 DE L'EMPD : CONSÉQUENCES SUR L'ENVIRONNEMENT, LE DÉVELOPPEMENT DURABLE ET LA CONSOMMATION D'ÉNERGIE

Un député demande si des mesures de compensation sont envisagées pour équilibrer les frais en énergie supplémentaires provoqués par les nouvelles applications.

La cheffe du DIRH prend note de la remarque qu'elle juge pertinente mais ajoute que cette compensation est difficile et coûteuse à évaluer puis à mettre en place au cas par cas et suggère d'y revenir dans un autre cadre.

Les prochains EMPD devraient contenir de plus amples informations quant aux conséquences sur l'environnement des projets mis en œuvre.

5. VOTES SUR LE PROJET DE DECRET (EMPD 147)

VOTE SUR LE PROJET DE DÉCRET

L'art. 1 du projet de décret est adopté à l'unanimité.

L'art. 2 du projet de décret est adopté à l'unanimité.

L'art. 3 du projet de décret (formule d'exécution) est adopté à l'unanimité.

ENTRÉE EN MATIÈRE SUR LE PROJET DE DÉCRET

La commission thématique des systèmes d'information (CTSI) recommande au Grand Conseil l'entrée en matière sur ce projet de décret à l'unanimité.

Chardonne, le 27 décembre 2019.

Le rapporteur :
(Signé) Maurice Neyroud