canton de vaud

LIBERTÉ ET PATRIE

AOÛT 2013 RC-61

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

Exposé des motifs et projet de décret accordant un crédit d'investissement de CHF 8'631'500.- destiné à financer la mise en place de mesures de diminution du risque et du pilotage de la sécurité des SI au sein de la DSI

1. TRAVAUX DE LA COMMISSION

La Commission des systèmes d'information (CTSI) s'est réunie en date du mardi 18 juin 2013 à la Salle des Armoiries à Lausanne pour traiter de cet objet. Elle était composée de Mmes les députées Fabienne Despot (présidente – rapportrice) et Pierrette Roulet-Grin ainsi que de MM. les députés Laurent Ballif, François Brélaz, Jean-François Cachin, Philippe Grobéty, Olivier Kernen, Olivier Mayor, Daniel Meienberger, Michel Miéville, Maurice Neyroud, Cédric Pillonel, Alexandre Rydlo, Filip Uffer et Eric Züger.

Mme la Conseillère d'Etat Nuria Gorrite (cheffe du DIRH) était présente ainsi que MM. Patrick Amaru (chef de la DSI) qui représentait l'administration.

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

2. PREAMBULE

Les systèmes d'information de l'Etat de Vaud doivent être sécurisés pour assurer la disponibilité des outils informatiques, leur confidentialité, leur intégrité et leur traçabilité. C'est là une des missions de la DSI, une mission cadrée au sein d'un document nommé Politique générale de sécurité des systèmes d'information, adopté en juin 2011. L'esprit de ce document est de développer, de manière évolutive, efficace et proportionnée, un système de management de la sécurité conforme aux meilleures pratiques, afin de coordonner et d'amplifier les actions disparates mises en place depuis la création d'une unité de sécurité des systèmes d'information (USSI) .

3. PRÉSENTATION DE L'EMPD

La Conseillère d'Etat Nuria Gorrite a relevé l'importance stratégique de cette sécurisation afin d'assurer le bon fonctionnement de l'administration au quotidien.

Cette importance grandit avec le développement de la cyberadministration.

De nombreux services de l'administration cantonale vaudoise traitent des informations sensibles qui sont soumises à la loi sur la protection des données, comme par exemple l'ACI, le CHUV, les services liés à l'enseignement et à la formation, l'OJV, le SPOP ou encore le SAN.

La Cheffe du DIRH a mentionné certaines situations à haut risque auxquelles l'Etat doit pouvoir faire face :

- le vol de données sensibles (lecture et/ou copie),
- la modification ou la destruction de données,
- la paralysie totale des systèmes informatiques et/ou des serveurs (panne ou destruction complète).

De telles situations mettraient en péril le fonctionnement mais aussi la crédibilité et l'image de l'ACV. En l'absence d'un site secondaire, la destruction totale des serveurs de la DSI, suite à une catastrophe naturelle (inondation, incendie, etc.), provoquerait l'indisponibilité des systèmes informatiques pendant trois mois environ.

En conséquence, la Conseillère d'Etat a présenté les trois axes de la sécurité des systèmes d'information :

1) la maîtrise des risques :
   - cloisonnement physique des serveurs (parois coupe-feu, locaux étanches, etc.),
   - sauvegardes des données et des systèmes,
   - mise en place d'un site secondaire externe,
   - pilotage de la sécurité : veille opérationnelle, émission d'alarmes, détection et prévention d'attaques,
   - sécurisation d'éléments sensibles.
2) la formation et la sensibilisation des utilisateurs (collaborateurs de l'ACV) :
   - sensibilisation des utilisateurs au système d'accès (p.ex. complexité des mots de passe, niveaux d'accréditations),
   - gestion des accès liés à une personne dûment identifiée,
   - comportements prudents et préventifs.
3) la sécurisation des fonctions stratégiques :
   - internalisation de consultants externes qui occupent des fonctions stratégiques et pérennes, et traitent des données sensibles (liées à la fiscalité, la sécurité, la justice, etc.).

Le présent EMPD vise à la mise en œuvre de la première phase de sécurité, avec pour but de diminuer les risques et d'améliorer le pilotage de la sécurité, en mettant en place des processus aux normes ISO de management de la sécurité de l'information.

4. DISCUSSION GÉNÉRALE

Du bienfondé de la démarche

Un député a rappelé que les questions de sécurité informatique sont soulevées depuis les années 2000 ; il y a eu un rapport de la COGES, un audit externe alarmiste, un rapport exhaustif du CCF puis l'établissement d'une Politique générale de sécurité des systèmes d'information. Il estime urgent d'agir et de mettre en place des mesures concrètes et efficaces de sécurisation des systèmes d'information, en particulier avec la cyberadministration qui ouvre l'accès aux citoyens représentant des centaines de milliers d'utilisateurs externes.

Si la nécessité d'assurer des fonctionnalités indispensables paraît évidente aux yeux des commissaires, certains doutent que l'administration cantonale soit régulièrement victime d'attaques ciblées. M. Amaru, chef de la DSI, a confirmé que ces menaces sont réelles. Les hackers deviennent de plus en plus efficaces, ce qui nécessite une modernisation continue des systèmes de sécurité informatique. Il y a lieu de prévenir et d'anticiper les attaques en analysant et traitant automatiquement les événements affectant les systèmes d'information de l'ACV.

90% des incidents découlent d'attaques génériques que subissent aussi des particuliers, des PME, des multinationales ou des gouvernements, mais il existe des actions qui visent spécifiquement les serveurs de l'ACV, dans le but de lire, voler, modifier ou détruire des données.

Le chef de la DSI s'est félicité que le canton de Vaud, à l'image de la Confédération, soit plutôt en avance dans le domaine de la sécurité informatique.

De la nécessité d'un second site de stockage des données

Toutes les données sont sauvegardées auprès de Bedag à Berne. Si le bâtiment de la DSI à Renens devait subir un événement classé catastrophe, cela ne conduirait pas à une perte des données mais leur exploitation et leur mise à disposition des utilisateurs pourraient être bloquées pendant plusieurs semaines.

Un commissaire a estimé qu'une seule sauvegarde chez Bedag est insuffisante pour assurer la continuité du fonctionnement informatique.

Le chef de la DSI a confirmé qu'un site secondaire permettra d'assurer le fonctionnement continu des activités en cas de catastrophe majeure sur le site principal. Lors de la création du « *data center* » actuel de la DSI, il était déjà fait mention de la nécessité d'un site de secours dans le cadre de ce qui était nommé à l'époque « *Disaster recovery plan* » (DRP). Ce second site ne se réalisera pas dans une société privée, et il ne remplacera pas le stockage des données chez Bedag qui répond aux standards d'un 2e site de stockage éloigné d'au moins 60 kilomètres du premier.

La construction d'une telle infrastructure, actuellement à l'étude, n'est pas incluse dans le présent EMPD.

Risques liés aux communications et au télétravail

La Conseillère d'Etat a confirmé que les dangers liés aux systèmes de communication (par exemple le blocage d'une centrale téléphonique) sont inclus dans la pré-analyse des risques sur les applications/plates-formes critiques. Elle a listé quelques risques identifiés avec les mesures proposées dans cet EMPD :

- Mauvaise gestion des droits d'accès administrateur.
- Absence de mécanisme de détection d'intrusions externes (hackers).
- Difficultés d'identification et de prévention des virus.
- Manque de formation et de procédures.
- Insuffisance de sécurité physique (cloisonnement de systèmes).
- Failles dans la confidentialité des données (codage, mesures cryptographiques).

La cheffe du DIRH a également relevé les risques liés aux communications sans fil (WIFI), aux connexions à distances, aux ordinateurs et téléphones portables (« smartphones »). Les procédures liées au télétravail sont également prises en compte, comme par exemple les droits d'accès et la protection des données confidentielles.

Choix d'une variante : priorisation des risques

La solution proposée dans l'EMPD (variante C) permettra la mise en place des mesures de diminution des risques proportionnée à l'importance des risques encourus. Une autre variante, au coût nettement plus élevé, aurait été de prendre des mesures sur tout risque connu, qu'il soit critique, important ou mineur. Le statu quo, quant à lui, ne permettrait pas à la DSI d'assurer en toutes circonstances le fonctionnement de l'ACV, notamment face à l'ouverture des systèmes au grand public (cyberadministration).

Selon la Conseillère d'Etat, la stratégie proposée garantit un niveau de sécurité élevé en engageant des ressources raisonnables. La valeur ajoutée de mesures de sécurité supplémentaires serait marginale par rapport aux moyens financiers et humains qu'elles nécessiteraient. Cette pesée des intérêts entre risques et coûts a été particulièrement prise en compte dans la création d'un site de secours.

La priorisation des risques tient compte de la sécurité physique, de la formation des utilisateurs, du contrôle des collaborateurs, des vulnérabilités personnelles. L'internalisation de fonctions pérennes permet de diminuer les risques liés aux consultants externes. Cet aspect répond aux risques liés au piratage et au vol de données de la part d'employés.

Le chef de la DSI a souligné que le Canton de Vaud est précurseur dans la mise en place d'un Système de Management de Sécurité de l'Information (SMSI) et d'un Centre de sécurité opérationnel (SOC – Security Operation Center). A l'avenir, ces prestations pourraient être proposées à d'autres cantons. Il ajoute que des discussions ont eu lieu avec la Confédération, entre autres sur les risques de blocage du réseau Internet, par exemple par les Etats-Unis, et la possibilité qu'un réseau Internet parallèle, entre les collectivités, devienne une solution de remplacement.

La cheffe du DIRH souligne l'importance de la « souveraineté numérique » d'un Etat, au même titre que l'on parle de souveraineté alimentaire ou énergétique.

Sécurité des données communales

A la question de savoir s'il était prévu d'intégrer les données des communes dans le concept de sécurité des systèmes d'information de l'Etat de Vaud, le chef de la DSI a confirmé des discussions concrètes dans ce sens avec l'AVRiC (Association Vaudoise des Responsables informatiques Communaux) et constaté que le déploiement de la cyberadministration entraînera de facto le traitement de certaines données des communes par la DSI.

A ce jour, il n'est pas prévu d'intégrer les données des communes dans le centre de calcul de l'Etat, mais des sauvegardes pourraient être effectuées et gérées à la DSI.

Un député a relevé que certains employés communaux ont déjà des accès privilégiés et saisissent des données dans le système informatique du Canton (par exemple, accès au SPOP).

5. EXAMEN POINT PAR POINT DE L'EXPOSÉ DES MOTIFS

2.2 But du document

Concernant l'évolution du nombre d'utilisateurs liés à la cyberadministration, il est précisé qu'environ 10'000 collaborateurs de l'Etat utilisent les systèmes d'information de l'ACV, et qu'avec le développement du portail des prestations en ligne (e-vd), entre 600'000 et 700'000 personnes pourraient se connecter au système, ce qui engendre une multiplication importante des facteurs de risques. A ce jour, le chef de la DSI estime que l'on est déjà au tiers du potentiel ; à titre d'exemple, 160'000 déclarations d'impôt sont déjà remplies en ligne.

Un député a estimé que le projet a tendance à mêler les notions d'atteintes extérieures à la confidentialité, à l'intégrité et à la disponibilité des systèmes aux aspects de fiabilité interne des systèmes, de disponibilité critique de plates-formes, d'efficience des processus et de qualité d'applications. Il s'agirait de mieux distinguer les risques découlant de lacunes des logiciels et ceux liés à des attaques externes. Il est répondu que la distinction n'est pas évidente entre risques découlant d'attaques externes et risques liés à des déficiences internes.

2.3 Situation actuelle

Le chef de la DSI a expliqué que l'USSI est une équipe d'environ huit personnes à plein temps. A sa création, l'Unité était composée de deux collaborateurs, puis elle a grandi lors de l'intégration de l'Office de la sécurité informatique cantonale (OSIC) au sein de l'USSI. Il ajoute qu'avec cet EMPD, il y a aura clairement des renforts supplémentaires par l'internalisation de consultants sous contrats externes de type LSE.

Les employés de l'USSI peuvent règlementairement intervenir en cas d'infractions liées à la sécurité des systèmes d'information, sur la base du règlement relatif à l'informatique cantonale (RIC), arrêté par la Conseil d'Etat en 2009, qui s'applique à l'ensemble de l'ACV. Un député constate que ce règlement interne ne s'applique pas aux personnes extérieures qui, en cas d'actes de cybercriminalité, seraient alors dénoncées pour infraction pénale.

5.1 Projet de diminution des risques

Dans la dizaine de mesures de diminution de risques proposées en lien avec les risques identifiés, un député a demandé si la procédure d'accès existante IAM pose problème et s'inquiète du coût apparemment élevé de la mesure M4.

Le chef de la DSI a confirmé que le processus de sécurisation des accès est en cours via l'application IAM. En ouvrant le portail des communes, puis celui des entreprises, il s'agira de renforcer la sécurité avec des accès spécifiques délivrés à des utilisateurs identifiés. La DSI doit connaître les accès de chaque identifiant, il est trop risqué de délivrer des identifiants génériques pour l'ensemble d'un service d'une commune. En parallèle, la prévention d'intrusion doit être utilisée avec circonspection de manière à ne pas rendre les services compliqués d'accès voire inaccessibles aux utilisateurs.

La problématique des hackers internes est prise en compte dans le chapitre de la formation et des mises en place de mesures cryptographiques (M7). Des utilisateurs mal informés pourraient mettre fortuitement des données sensibles sur des sites hébergés aux Etats-Unis, du type « dropbox.com ».

5.1.1.3 Plans de secours

La DSI a réalisé une première analyse et a établi une liste de trente applications et systèmes jugés critiques, qui seront transférés en priorité dans le site de secours. Dans le cadre du plan de continuité, en coopération avec les services, cette liste est amenée à évoluer en fonction des processus métier critiques qui seront identifiés.

5.2 Projet SMSI

Un travail important de mise en place du SMSI est prévu. Son pilotage sera ensuite assuré par une seule personne.

Un député a relevé que la DSI s'alignera sur les normes ISO 27001, 27002 et 27005 et demandé si le système de gestion de la sécurité informatique sera certifié. La priorité de la DSI est de se référer aux normes et d'appliquer les bonnes pratiques dans la mise en place et la gestion du système, cependant il n'est pas prévu de certification ISO.

6. Coûts des solutions

En plus des investissements se montant à CHF 6'619'000 pour la diminution des risque, CHF 150'000 pour l'analyse de risques, CHF 277'500 pour la formation et CHF 1'585'000 pour le SMSI, soit un total de CHF 8'631'500, la somme de CHF 1'120'000 sera prise sur le crédit d'inventaire.

Un député a relevé que cet EMPD aura une incidence limitée sur le budget de fonctionnement, car les frais d'exploitation supplémentaires de CHF 1'556'000 seront compensés par des diminutions de charges liées à :

- l'arrêt d'anciens composants de la Gestion des identités et accès (GDIA) : CHF 469'000
- l'internalisation de ressources externes (consultants sous contrat LSE) : CHF 1'087'000

Concernant ce dernier point, le chef de la DSI a confirmé une économie moyenne de CHF 60'000 à CHF 70'000 réalisée pour chaque consultant engagé à l'Etat de Vaud. Le processus d'engagement est planifié sur trois ans.

La Conseillère d'Etat précise que l'internalisation concerne une cinquantaine de collaborateurs, ce qui dégagera une marge de financement importante, utilisée pour le fonctionnement de ce projet de sécurité des systèmes d'information, mais aussi pour la mise en place de la cyberadministration.

7. Mode de conduite du projet

Un député a relevé que les travaux sont pilotés par la DSI et a demandé s'il est envisagé d'avoir un contrôle extérieur dans la conduite et la mise en place du projet. Le chef de service a confirmé que la DSI dirige seule le projet et admis qu'un regard extérieur au sein du comité de pilotage est envisagé.

6. DISCUSSION SUR LE PROJET DE DÉCRET ET VOTES

6.1 COMMENTAIRES ET AMENDEMENTS

L'EMPD n'a pas fait l'objet de propositions d'amendements de la part des commissaires. Il est à relever qu'il s'inscrit dans une démarche évolutive et qu'il ne s'agit ici que d'une première phase de la consolidation de la sécurité des systèmes d'information.

6.2 VOTE

L'article premier du projet de décret est adopté à l'unanimité (15).

L'article second du projet de décret est adopté à l'unanimité (15).

7. ENTRÉE EN MATIÈRE SUR LE PROJET DE DÉCRET

La commission recommande au Grand Conseil l'entrée en matière sur ce projet de décret à l'unanimité (15).

Vevey, le 21 août 2013

La rapportrice :
(Signé) Fabienne Despot