canton de vaud

LIBERTÉ ET PATRIE

JUIN 2017 **17_INT_671**

RÉPONSE DU CONSEIL D'ETAT
à l'interpellation Céline Ehrwein Nihan – Les établissements médicaux vaudois sont-ils immunisés contre les virus informatiques ?

Rappel de l'interpellation

Plusieurs articles parus récemment, notamment en Suisse alémanique, font état d'une augmentation de l'utilisation de logiciels malveillants verrouillant les données — rançonlogiciels — et d'autres modes de piratage dans le domaine de la santé.

En décembre dernier, le chef de la centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération (MELANI), Pascal Lamia, mettait en garde le monde médical contre ces logiciels de chantage dans les colonnes du Bulletin des médecins suisses. Il y a une semaine, la NZZ am Sonntag, puis le Tages Anzeigerrevenaient sur cette problématique et relataient les déboires d'un hôpital suisse piraté par l'envoi d'un simple mail de candidature qui semblait répondre à la mise au concours d'un nouveau poste dans l'établissement : un piratage aussitôt suivi d'une demande de rançon en échange de la clé nécessaire au décryptage des données médicales bloquées.

Il ne s'agit pas là d'un cas isolé. Selon Urs Achermann, chef expert en sécurité auprès de la société Hint à Lenzburg — une société qui gère la sécurité informatique de 15 établissements médicaux — les cliniques suisses sont régulièrement la cible des hackers : chaque établissement subirait entre deux et trois attaques par mois.

Or, une seule attaque, même rapidement maîtrisée, peut coûter très cher. Plusieurs cas sont cités en exemple. Tout d'abord, celui de cet établissement de Los Angeles qui, l'année dernière, a fini par débourser quelques 17'000.- dollars pour obtenir la clé lui permettant de récupérer les données de ses patients. Plus coûteux, et plus grave aussi, le cas d'une clinique de quelques 500 lits à Neuss en Allemagne, dont les 800 ordinateurs et 100 serveurs ont été entièrement paralysés pendant plusieurs jours. Suite à cette attaque, la clinique a été contrainte de réduire les examens effectués dans ses laboratoires, de refuser de prendre en charge les blessés graves et de limiter ses interventions cardiaques, ainsi que les radiothérapies destinées à traiter les patients cancéreux. Dans ce cas, une somme d'un montant évalué à 6 ou 7 chiffres a été nécessaire pour réparer les dégâts — et c'est sans compter sur l'atteinte à l'image de l'établissement et la mise en danger des patients.

Pour ces derniers, le risque ne réside d'ailleurs pas seulement dans le vol ou le blocage de leurs données, mais aussi dans la prise de contrôle des appareils médicaux. Ainsi, on apprend dans la NZZque, depuis 2015, l'autorité américaine de contrôle Food and Drug Administration(FDA) a déjà mis en garde le corps médical contre l'usage d'une pompe à insuline, d'un défibrillateur et d'un pacemaker pouvant facilement être piratés, puis contrôlés à distance par des tiers malveillants.

Au vu de ses différents éléments, des coûts et des risques susceptibles d'être engendrés par les rançonlogiciels et autres modes de piratage, nous nous permettons de demander au Conseil d'Etat de

bien vouloir répondre aux questions suivantes :

1. *Comment le Conseil d'Etat évalue-t-il la qualité de la sécurité informatique qui prévaut aujourd'hui au sein des établissements médicaux vaudois — tout type d'établissement confondu ?*
2. *Existe-t-il à l'heure actuelle un inventaire des outils ou instruments médicaux connectés sensibles et susceptibles d'être piratés par des hackers ?*
3. *Quels outils — sensibilisation des utilisateurs, systèmes de protection, etc. — et moyens financiers le Conseil d'Etat met-il à disposition pour :*

   - prévenir le piratage des systèmes informatiques des établissements hospitaliers publics vaudois ?

   - soutenir les cliniques, hôpitaux ou cabinets privés dans leur lutte contre le piratage ?
4. *Quelles sont les procédures d'urgence existantes au sein des établissements médicaux vaudois pour répondre aux situations d'urgence médicales susceptibles d'être engendrées par une attaque informatique ?*
5. *Ces mesures, outils, moyens et procédures sont-ils jugés suffisants ? Le Conseil d'Etat entend-il en développer d'autres ? Et si oui, lesquels ?*

Souhaite développer.

(Signé) Céline Ehrwein Nihan

Réponses du Conseil d'Etat

La gestion de la sécurité informatique est encadrée au niveau international par des standards (famille ISO 27000, COBIT) définissant les normes et les bonnes pratiques et ce pour tous les secteurs confondus. Les Etats-Unis disposent d'une loi HIPAA, votée par le Congrès en 1996 qui concerne spécifiquement tous les aspects de la sécurité de la santé et de l'assurance maladie, incluant la sécurité informatique. La Suisse quant à elle ne dispose pas de loi traitant spécifiquement de la sécurité informatique dans le domaine de la santé mais de plusieurs lois et ordonnances réglant la sécurité et la confidentialité des données.

Ainsi, en Suisse, chaque établissement médical est responsable de sa sécurité informatique. Les investissements correspondant doivent s'inscrire dans la stratégie financière et de gestion de chaque établissement. Pour maintenir ou augmenter le niveau de sécurité informatique, tout en étant confronté à un nombre grandissants de menaces qui sont par nature de type imprévisible, il est nécessaire d'investir de manière continue et suffisante dans la sécurité informatique.

La mission de l'organisation de sécurité informatique est de mettre en place et de maintenir les bonnes pratiques et les bons outils qui protègent l'institution contre tout impact d'attaques, internes ou externes, tels que l'altération ou le vol de données. Toute stratégie de sécurité informatique nécessite en premier lieu de la prévention qui doit être complétée par la détection et l'intervention rapide afin d'isoler le ou les équipement(s) impacté(s).

Nous devons partir du principe que les attaques ciblées continueront de prendre de l'importance et les établissements médicaux sont - et seront - donc autant visés que toute autre industrie, tel que la plus grande cyberattaque jamais subie du 12 mai 2017 l'a démontré.

1 RÉPONSES AUX QUESTIONS

1.1 Comment le CE (Conseil d'État) évalue-t-il la qualité de la sécurité informatique qui prévaut aujourd'hui au sein des établissements médicaux vaudois (tout type d'établissement confondu) ?

Le Conseil d'Etat n'ayant pas de responsabilité propre quant à la sécurité informatique gérée dans les établissements médicaux du canton, il ne peut se prononcer que pour les hôpitaux subventionnés. Il est utile de rappeler que le contrôle cantonal des finances (CCF), qui mène différents type d'audits tels que comptabilité, finances, informatique, sécurité informatique et juridique, a audité les différents systèmes d'information des hôpitaux subventionnés (CHUV, FHV) ces dernières années.

Les directions des systèmes d'information (DSI) du CHUV et de la FHV bénéficient d'une taille suffisante pour disposer de ressources dédiées à la prise en charge de la sécurité des systèmes d'information ; cela n'est pas le cas pour de plus petites structures. Les stratégies de sécurité informatique mise en œuvre au CHUV et à la FHVi (Fédération des hôpitaux vaudois informatique) sont inspirées par les meilleures pratiques de HIPAA et des standards européens tels que la famille ISO 27000.

Le personnel des grands hôpitaux est sensibilisé par rapport aux risques de cyberattaques et un focus particulier est mis sur la détection et l'isolation rapide des équipements impactés ou infectés en cas d'intrusion.

Ce qui précède permet au Conseil d'État de confirmer que la qualité de la sécurité informatique dans les hôpitaux subventionnés du canton est actuellement plutôt bonne.

1.2 Existe-t-il à l'heure actuelle un inventaire des outils ou instruments médicaux connectés sensible et susceptible d'être piratés par des hackers ?

Au CHUV et à la FHVi toute nouvelle acquisition d'équipement technique biomédical ou de gestion de bâtiment connectable au réseau informatique est préalablement sujet à une validation d'exigences minimales définies dans le document de référence " Sécurité informatique des équipements techniques – Exigences ". Ce référentiel exprime le consensus d'exigences minimales du groupe d'experts " HIL " (Hospital Infosec Liaison), qui représente les hôpitaux de la santé subventionnés des cantons Fribourg, Genève, Tessin, Valais et Vaud.

Tous les équipements biomédicaux connectés au réseau sont identifiés dans les inventaires des équipements techniques des institutions concernées. Cette inscription est obligatoire pour l'accès au réseau informatique de l'établissement. L'inventaire des équipements biomédicaux qui ont été validés par cette procédure peut être établi sur demande par le CHUV et la FHVi.

1.3 Quels outils (sensibilisation des utilisateurs, système de protection, etc.) et moyens financier le CE met-il à disposition pour :

- *Prévenir le piratage des systèmes informatiques des établissements hospitaliers publics vaudois*
- *Soutenir les cliniques, hôpitaux ou cabinets privés dans leur lutte contre le piratage*

La formation du bon usage des outils informatiques et bureautiques des utilisateurs ainsi que l'infrastructure de protection contre les cyberattaques est sous la responsabilité de chaque institution.

Les forfaits hospitaliers DRG incluent une part relative aux investissements, dont les investissements informatiques. L'Etat ne subventionne donc pas spécifiquement des moyens informatiques ou leur sécurité, ceux-ci faisant partie intégrante des prestations fournies par les hôpitaux.

1.4 Quelles sont les procédures d'urgence existantes au sein des établissements médicaux vaudois pour répondre aux situations d'urgence médicales susceptibles d'être engendrées par une attaque informatique ?

Par nature, la prévention contre toute cyberattaque a toujours un peu de retard par rapport au rythme d'apparition de nouveaux virus (4 par seconde sur Internet). De ce fait toute organisation de sécurité consciencieuse et professionnelle doit partir de l'hypothèse que le virus peut entrer tôt ou tard dans le système informatique. Ainsi la détection rapide de l'équipement incriminé et son isolation rapide font partie des procédures d'urgence de base de la sécurité informatique. Des sauvegardes des données fréquentes permettent de rétablir le bon fonctionnement de l'équipement en question dans la majorité des cas.

En cas d'attaques et d'infections importantes, la direction des systèmes d'information peut être amenée à déclencher la procédure de crise conduisant, dans un cas extrême, à un basculement de toutes les applications critiques vers le centre de calcul de secours afin d'assurer la disponibilité de ces applications.

1.5 Ces mesures, outils, moyens et procédures sont-ils jugés suffisants ? Le CE entend-il en développer d'autres ? Et si oui, lesquels ?

Les mesures, outils, moyens et procédures implémentés actuellement dans les hôpitaux subventionnés du canton de Vaud sont considérés comme suffisants par le Conseil d'État. Il est indispensable que les directions de ces établissements continuent à porter une attention particulière et continue à la question de la sécurité informatique. Comme nous l'a rappelé dernièrement l'actualité, une attaque de grande ampleur, impliquant l'ensemble du réseau, pourrait se produire malgré les précautions prises, il est donc important que le domaine sanitaire cantonal continue à s'investir dans la gestion de catastrophe majeures, en collaboration avec les autres services de secours du canton.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 7 juin 2017.

Le président :	Le chancelier :
P.-Y. Maillard	*V. Grandjean*