canton de vaud

Grand Conseil
Secrétariat général
Pl. du Château 6
1014 Lausanne

Interpellation

(formulaire de dépôt)

A remplir par le Secrétariat du Grand Conseil

N° de tiré à part : 17_INT_671

Déposé le : 14.02.17

Scanné le : _____

Art. 115 et 116 LGC L'interpellation est une demande d'explications ou de précisions adressée au CE sur un fait du gouvernement ou de son administration. Elle porte sur une compétence propre ou déléguée du CE et peut être développée oralement devant le GC. Les questions qu'elle contient sont exprimées de telle manière que le CE puisse y répondre et sont suffisamment précises pour qu'une réponse courte y soit apportée dans le délai légal (attention : ne pas demander un rapport, auquel cas il s'agit d'un postulat).
*Délai de réponse dès le renvoi au CE : **trois mois**.*

Titre de l'interpellation
Les établissements médicaux vaudois sont-ils immunisés contre les virus informatiques ?

Texte déposé

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 Anzeiger revenaient 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 2 et 3 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 NZZ que, depuis 2015, l'autorité américaine de contrôle FDA (Food and Drug Administration) 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 (CE) de bien vouloir répondre aux questions suivantes :

1. Comment le CE 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-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 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 ?
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 CE entend-il en développer d'autres ? Et si oui, lesquels ?

Commentaire(s)

Conclusions

Souhaite développer [X] Ne souhaite pas développer [ ]

Nom et prénom de l'auteur : Ehrwein Nihan Céline

Signature :

Nom(s) et prénom(s) du (des) consort(s) :

Signature(s) :

Merci d'envoyer une copie à la boîte mail du Bulletin : bulletin.grandconseil@vd.ch