REPONSE DU CONSEIL D'ETAT

à l'interpellation Yann Glayre et consorts –

Cybersécurité - Quelle est la stratégie de l'Etat de Vaud pour traiter la plus grande collection de fuite de données de l'histoire ?

Rappel de l'interpellation

Le 17 janvier, la cybersécurité a à nouveau fait la une des journaux à travers le monde.

Et malheureusement, à nouveau pour de mauvaises nouvelles. Plus de 773 millions d'adresses email et 21 millions de mots de passe uniques ont été mis en danger dans une base de données nommée « Collection #1 ».

Il s'agit à ce jour de la plus grande collection de failles de données compilant plus de 2000 piratages : un record.

Si parmi cette base de données, beaucoup d'informations étaient déjà connues, au moins 140 millions sont inédites et doivent impérativement faire l'objet d'une nouvelle étude approfondie. Suite à l'analyse d'une partie de cette base de données, il relève que l'application d'un simple filtre permet de découvrir près de 500 logins de connexion appartenant ou ayant appartenu à des collaborateurs de l'Etat de Vaud. Et ceci accessible à n'importe qui.

vd.ch, hospvd.ch, heig-vd.ch, chuv.hospvd.ch, edu-vd.ch, tous les domaines sont concernés et personne n'est épargné, y compris des personnalités à hautes responsabilités.

A l'heure où la protection des données et la sécurité des infrastructures sont d'une importance cruciale, j'adresse au Conseil d'Etat les questions suivantes :

1. *Les services de l'Etat avaient-ils connaissance de l'existence de ces bases de données ?*
2. *Si oui, quelles mesures ont été prises afin de protéger les données de l'Etat de Vaud et celles de ses collaborateurs ?*
3. *Les services de l'Etat avaient-ils connaissance que des informations de connexion liées à des collaborateurs de l'Etat de Vaud sont disponibles dans ces collections de données ?*
4. *Est-ce que des analyses périodiques et surveillance des nouvelles fuites de bases de données ont lieu afin de prévenir le vol d'informations ?*
5. *Quelles mesures urgentes le Conseil d'Etat a-t-il prises, ou entend prendre pour protéger ses collaborateurs, sa population et ses services ?*

Souhaite développer.

(Signé) Yann Glayre

Réponse du Conseil d'Etat

1. Les services de l'Etat [1] avaient-ils connaissance de l'existence de ces bases de données ?

L'État de Vaud a pris connaissance de l'existence des données rassemblées sous le nom de Collection#1 dès le 17 janvier 2019 grâce à sa veille continue des cyber-menaces. Il s'est appuyé en particulier sur l'annonce publique de Troy Hunt, un expert en cybersécurité, qui a révélé publiquement l'existence de cette méga-archive de données potentiellement sensibles et l'incorporation de ces données sur son site haveibeenpwned[.]com (ci-dessous, HIBP).

Le CHUV a également pris connaissance de cet évènement le 17 janvier au matin suite à une alerte transmise par la société Hacknowledge qui effectue une surveillance sur internet pour le compte du CHUV. Dès réception de l'information, un incident de sécurité a été créé avec la liste des 270 collaborateurs du CHUV mentionnés dans cette fuite.

2. Si oui, quelles mesures ont été prises afin de protéger les données de l'Etat de Vaud et celles de ses collaborateurs ?

Il est important de noter que ces données ne proviennent pas d'une fuite d'un site appartenant à l'Etat de Vaud, mais qu'elles émanent de multiples vols sur divers forums de discussion ainsi que sur des sites privés, tels que LinkedIn, Adobe ou encore Dropbox. De plus, de par le fonctionnement de ses portails d'authentification, aucune information contenue dans Collection#1 n'aurait pu être directement utilisable sur les infrastructures de l'État de Vaud.

Par mesure de prévention et de sensibilisation, en collaboration avec MELANI et la société Kudelski Security, toutes les adresses e-mail finissant par « vd.ch » qui étaient contenues dans Collection#1 ont été extraites. Le Centre de sécurité opérationnel (ci-après SOC) de l'Etat de Vaud a informé personnellement toutes ces personnes que leurs identifiants avaient été trouvés dans cette fuite de données ; des conseils leur ont été fournis afin qu'ils puissent, le cas échéant, prendre des mesures de précaution nécessaires. Une communication générale a également été faite via l'Intranet de l'État de Vaud (et transmise aux responsables des Intranet police et educanet), en donnant les éléments nécessaires pour que chacun puisse vérifier si ses identifiants étaient connus ou non de Collection#1 et, plus globalement, des autres fuites de données répertoriées par HIBP.

Au CHUV, comme le prévoit la procédure dans un tel cas, un message a également été immédiatement transmis aux collaborateurs concernés afin de les instruire sur les actions à entreprendre et de leur rappeler les bonnes pratiques.

Les données contenues dans Collection#1 datent de brèches anciennes, les plus récentes datant de deux ou trois ans. Là où ils peuvent être déployés, des mécanismes obligent les collaboratrices et collaborateurs de l'État de Vaud à modifier régulièrement leur mot de passe ; ainsi, si l'un des mots de passe utilisés était contenu dans Collection#1, le mot de passe en question a depuis été modifié. Pour les comptes où de tels mécanismes ne sont actuellement pas possibles, l'État de Vaud encourage les utilisatrices et utilisateurs à respecter les bonnes pratiques dans la gestion de leurs mots de passe.

La politique de sécurité du CHUV impose aussi un changement régulier du mot de passe et interdit la réutilisation des 10 derniers.

3. Les services de l'Etat avaient-ils connaissance que des informations de connexion liées à des collaborateurs de l'Etat de Vaud sont disponibles dans ces collections de données ?

Comme mentionné précédemment, les collaboratrices et collaborateurs concernés de l'État de Vaud (y compris le CHUV) dont les données étaient contenues dans Collection#1 ont été informés personnellement de la situation, ceci dès janvier 2019.

[1] A défaut de pouvoir consulter l'ensemble des exploitants de systèmes d'information de l'Etat, les réponses à cette interpellation ont été préparées par la DSI pour l'informatique de l'Administration Cantonale Vaudoise et par le CHUV pour son périmètre respectif, ceci en vue d'obtenir une vision plus représentative des mesures engagées par l'Etat de Vaud.

4. Est-ce que des analyses périodiques et surveillance des nouvelles fuites de bases de données ont lieu afin de prévenir le vol d'informations ?

Le SOC surveille différentes sources d'actualités concernant la sécurité informatique et, entre autres, les fuites de données pouvant potentiellement impacter les collaboratrices et collaborateurs de l'Etat de Vaud. En revanche, le SOC n'a pas les moyens financiers et humains de surveiller les forums clandestins utilisés pour la vente de ce genre de fuites de données, de les acquérir et de les analyser. Par exemple, mi-février 2019, le même hacker a successivement mis en vente sur un marché du Dark Web 3 groupes d'informations issues de fuites de données de plus de 30 sites web au total. Le prix des informations pour chaque site internet peut varier de quelques dizaines de dollars à plusieurs milliers. Quant au site HIBP (qui avait ajouté les informations de Collection#1 à sa banque de données), il ne contient que les informations de 3 sites Internet sur la trentaine mentionnée plus haut à l'heure où cette réponse est rédigée.

La qualité des données joue également un rôle important : d'autres archives (nommées Collection#2 à 5) dans la même veine que Collection#1 ont été largement mises à disposition à bas prix ou gratuitement récemment ; cependant, leur contenu a été jugé trop redondant avec Collection#1 ou de trop mauvaise qualité par de nombreux chercheurs (y compris celui ayant publiquement révélé Collection#1) pour que les informations contenues soient analysées et considérées comme fiables.

Au-delà des opérations de surveillance et d'analyse, différentes actions de sensibilisation sont régulièrement mises en place afin de prévenir les risques liés à ce type d'événements. Entre autres, des formations et des campagnes de sensibilisation sont effectuées afin d'améliorer la prise de conscience de l'importance et de la confidentialité de ces données, ainsi qu'une présentation des bonnes pratiques à respecter pour réduire les risques et les impacts potentiels lorsque ce genre d'événement survient. Un module de formation en ligne sur la sécurité de l'information est également publiquement disponible sur le site de l'État de Vaud.

Le CHUV utilise, quant à lui, les services de la société Hacknowledge qui effectue cette surveillance et informe directement le support informatique en cas de fuite de données. Depuis quelques mois, du fait de la multiplication des fuites de données, cette procédure est régulièrement déclenchée. Ce système de surveillance fait l'objet d'un reporting mensuel et de mesures d'amélioration continue.

5. Quelles mesures urgentes le Conseil d'Etat a-t-il prises, ou entend prendre pour protéger ses collaborateurs, sa population et ses services ?

Les mesures déjà prises concernant les collaboratrices et collaborateurs de l'État de Vaud sont décrites ci-dessus. Au moment de la rédaction de cette réponse (mars 2019), l'application de ces mêmes mesures a été lancée pour couvrir l'ensemble des collections 1 à 5 sorties, pour les adresses « vd.ch » et « vd.educanet2.ch ».

Afin de vérifier la qualité du service de renseignement de la société Hacknowledge, le CHUV a testé, en fin d'année dernière, un autre service de « Threat Intelligence » (identifications des menaces ciblées et des scénarios d'attaque actuels et potentiels). Celui-ci n'ayant pas apporté beaucoup plus d'information que notre solution existante, il n'y a pas eu de suite à ce test.

En l'état et en synthèse des informations fournies ci-dessus, cette situation ne nécessite pas de mesures d'urgence supplémentaires mais confirme qu'une sensibilisation continue des employés de l'Etat de Vaud aux cyber-menaces est absolument nécessaire pour compléter les mesures techniques implémentées. Par ailleurs, elle conforte la vision du Conseil d'Etat en matière de renforcement de la sécurisation du système d'information (SI) de l'Etat, telle que décrite dans le plan directeur cantonal ad hoc 2018-23 : poursuite des efforts visant un SI cible sécurisé, agile et innovant permettant d'accompagner la transition numérique, avec comme 1er axe d'évolution du SI le renforcement de la sécurité et de la protection des données ; cet axe comporte plusieurs initiatives dont une partie fera l'objet d'une demande de crédit d'investissement (EMPD Sécurisation du SI – étape 2) qui sera soumise prochainement au Parlement.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 22 mai 2019.

La présidente :	Le chancelier :
N. Gorrite	*V. Grandjean*