Date de dépôt :22 septembre 2021

Réponse du Conseil d'Etat

à la question écrite urgente de M. Alexandre de Senarclens : Piratage et sécurité informatique de l'Etat de Genève : quelles sont les mesures prises ?

Mesdames et
Messieurs les députés,

En date du 3 septembre 2021, le Grand Conseil a renvoyé au Conseil d'Etat une question écrite urgente qui a la teneur suivante :

Le journal Le Temps a très récemment révélé l'ampleur du piratage informatique dont a été victime la ville de Rolle et la masse des informations sur les habitants de cette cité qui sont désormais disponibles sur le darknet.

Il apparaît que les pirates du net utilisent des méthodes de plus en plus performantes pour percer la sécurité informatique d'entités publiques et privées. A ce titre, les administrations publiques représentent des cibles de choix, car elles traitent de nombreuses données sensibles (en particulier : données fiscales, moyens de paiements, données judiciaires et médicales). C'est une lutte sans fin, car les pirates mettent toujours plus de moyens pour arriver à leurs fins et l'Etat doit donc continuellement mettre à niveau ses systèmes de protection.

Mes questions sont donc :

- ***L'Etat de Genève, les communes genevoises ou les entités publiques indépendantes font-ils régulièrement l'objet de tentatives de piratage ? Certaines ont-elles réussi ? Le cas échéant, quelle est la procédure mise en place pour informer et venir en aide aux victimes de ces attaques ?***
- ***Sans entrer dans des informations sensibles, l'Etat pourrait-il décrire les mesures de protection mises en place et leur adaptation régulière ?***
- ***L'Etat bénéficie-t-il de l'aide de mandataires externes pour organiser sa protection ?***

– ***L'Etat collabore-t-il avec la Confédération ou d'autres cantons dans ce domaine ? Quel rôle a dans ce cadre le Centre national pour la cybersécurité (NCSC) ?***

RÉPONSE DU CONSEIL D'ÉTAT

En prenant chaque question individuellement, les réponses sont les suivantes.

L'Etat de Genève, les communes genevoises ou les entités publiques indépendantes font-ils régulièrement l'objet de tentatives de piratage ?

Nos organisations ne sont pas immunes contre les tentatives de piratage. A l'instar des entreprises privées et des citoyens, en particulier à leur domicile, nous faisons quotidiennement l'objet de tentatives de piratage. Celles-ci sont principalement menées par des robots, qui sondent nos défenses.

A titre d'exemple, pour la Ville de Genève, en 2020, 112 640 messages malicieux ont été interceptés en moyenne chaque mois, et 460 virus ont été bloqués sur les stations de travail.

Le service intercommunal d'informatique de l'Association des communes genevoises (SIACG) traite en moyenne 8 cas critiques par année, sur plusieurs centaines de millions d'événements détectés sur les infrastructures des communes.

Enfin, pour l'administration cantonale, en 2020, les services de l'office cantonal des systèmes d'information et du numérique (OCSIN) ont traité 115 incidents de sécurité, détectés à partir de l'analyse de 173 milliards d'événements techniques enregistrés sur les infrastructures de l'Etat de Genève. En outre, 23 027 nouvelles vulnérabilités ont été identifiées sur les systèmes de l'Etat de Genève, dont 1 511 présentaient un risque élevé ou critique. Enfin, plus de 500 000 virus (ou analogues) ont été éradiqués par l'OCSIN.

Certaines ont-elles réussi ?

Aucune, à notre connaissance.

Toutefois, il convient de préciser que la capacité de détecter des tentatives de piratage ne peut être garantie. En effet, les systèmes informatiques sont complexes et reposent sur un grand nombre de composants qui peuvent présenter des failles. Ce phénomène n'est pas propre à l'informatique « traditionnelle » : les éléments informatiques des avions, des voitures ou des

centrales électriques contiennent tous des failles que les pirates peuvent tenter d'exploiter.

En outre, l'erreur ou la maladresse d'un utilisateur peut permettre à un pirate de contourner les dispositifs de sécurité.

Le cas échéant, quelle est la procédure mise en place pour informer et venir en aide aux victimes de ces attaques ?

Chaque collectivité publique dispose de ses propres procédures, qui ont avant tout pour but de décrire l'organisation de gestion de crise. Les canaux de communication et le support aux victimes seront ajustés selon la nature de l'incident, qui peut varier considérablement.

Sans entrer dans des informations sensibles, l'Etat pourrait-il décrire les mesures de protection mises en place et leur adaptation régulière ?

C'est peut-être ce point qui distingue le plus l'organisation genevoise par rapport à celle du canton de Vaud.

Le 17 janvier 2018, le Conseil d'Etat a formalisé l'existence du comité de sécurité des systèmes d'information du canton de Genève, baptisé SécuSIGE.

Mis en œuvre dès 2016, ce comité est composé de représentants de la majorité des institutions étatiques et paraétatiques du canton de Genève. En outre, le chef de la section forensique de la police judiciaire, qui inclut la brigade de criminalité informatique (BCI), est également membre de ce comité, tout comme le responsable de la sécurité des systèmes d'information du pouvoir judiciaire.

SécuSIGE a notamment pour buts d'alerter ses membres en cas de détection d'incidents ou d'annonce de risques majeurs, et de collaborer à la résolution de toute crise relative à la sécurité de l'information, entre pairs et en toute transparence. A ce titre, ses membres mettent en commun l'ensemble des compétences nécessaires pour résoudre un problème avéré, telle une attaque d'envergure contre les infrastructures informatiques d'une ou de plusieurs institutions.

Les membres de SécuSIGE disposent de systèmes de sécurité conformes à l'état de l'art. Constamment mis à jour, ils permettent de protéger au mieux les infrastructures et les données.

En complément, une majorité des membres de SécuSIGE bénéficient de l'appui d'un « centre opérationnel de sécurité » (SOC), fourni par un même prestataire choisi suite à un appel d'offres commun.

Enfin, à l'instar des services de l'OCSIN, certains des membres de SécuSIGE ont des relations privilégiées avec la Confédération et bénéficient de diverses protections et prestations supplémentaires fournies par celle-ci.

Nous nous permettons d'insister sur le fait que le risque zéro n'existe pas. En matière de sécurité, il convient de garder la plus grande humilité. Nous ne sommes en effet plus à une époque où les actes de piratages étaient l'apanage d'individus certes créatifs, mais isolés; dorénavant, ce sont souvent des gangs organisés, voire des Etats, qui procèdent aux attaques, avec des moyens parfois colossaux, sans commune mesure avec les nôtres. Dans toute la mesure du possible, nous devons donc avant tout veiller à les décourager.

L'Etat bénéficie-t-il de l'aide de mandataires externes pour organiser sa protection ?

Oui, indubitablement.

L'Etat de Genève, tout comme la Ville de Genève et le SIACG, entretient des relations étroites avec des partenaires hautement qualifiés, tels que le Centre national pour la cybersécurité (NCSC), la BCI et le Réseau national de sécurité (RNS).

En outre, tous les membres de SécuSIGE ont régulièrement recours à des sociétés privées, expertes du domaine concerné, notamment lorsqu'il s'agit de pratiquer des audits de sécurité ou plus généralement de bénéficier de conseils.

Enfin, la capacité à pouvoir s'appuyer sur un SOC de haut niveau est très bénéfique.

L'Etat collabore-t-il avec la Confédération ou d'autres cantons dans ce domaine ?

Oui.

Comme décrit précédemment, certains membres de SécuSIGE, notamment l'OCSIN, ont des échanges réguliers avec la Confédération à ce sujet et bénéficient donc de diverses prestations fournies par celle-ci, en particulier celles fournies par le Centre national de cybersécurité (NCSC).

Le Réseau national de sécurité (RNS) réunit la Confédération et les cantons pour approfondir en commun les questions de politique de sécurité, incluant notamment la cybersécurité. Des membres de la police et de l'OCSIN y représentent le canton.

La Conférence suisse pour l'informatique (CSI) dispose d'un « groupe latin de sécurité » composé de représentants des cantons de Fribourg, de Genève (OCSIN), du Jura, de Neuchâtel, du Tessin, du Valais et de Vaud. A l'instar de SécuSIGE, ses membres collaborent sur de nombreux points, y compris dans la résolution d'incidents de sécurité ou par des échanges d'informations.

Quel rôle a dans ce cadre le Centre national pour la cybersécurité (NCSC) ?

Le NCSC est le premier point de contact au niveau national pour toute alerte en lien avec la cybersécurité. A ce titre, chaque membre de SécuSIGE le contacte directement dès que cela s'avère nécessaire.

Le NCSC peut mettre à disposition des ressources humaines et techniques afin d'aider les organismes ou sociétés touchés par une attaque. Dans ce contexte, il est notamment intervenu à Rolle.

Il faut noter que dès l'entrée en vigueur de la nouvelle loi fédérale sur la protection des données (nLPD), chaque organisme ou entreprise sera tenu d'annoncer dans les meilleurs délais au Préposé fédéral à la protection des données et à la transparence (PFPDT) les cas de violations de la sécurité des données. Le projet d'ordonnance relative à cette loi prévoit que le PFPDT pourra transmettre les informations nécessaires au NCSC pour déterminer les mesures à prendre, voire mettre en œuvre un portail d'annonces commun. Le rôle du NCSC en sera ainsi renforcé.

Les présentes réponses ont été rédigées après consultation du service intercommunal d'informatique de l'Association des communes genevoises (SIACG) ainsi que de la direction des systèmes d'information et de communication de la Ville de Genève (DSIC). Nous souhaitons les remercier chaleureusement pour leur collaboration active au quotidien.

Au bénéfice de ces explications, le Conseil d'Etat vous invite, Mesdames et Messieurs les Députés, à prendre acte de la présente réponse.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :	Le président :
Michèle RIGHETTI	Serge DAL BUSCO