acteurspublics

Cyberattaque du Quai d'Orsay : dans les coulisses d'une crise

7 FÉVR. 2019, PAR EMILE MARZOLF

Tout juste deux mois après la cyberattaque de la base Ariane du ministère des Affaires étrangères, deux sénateurs dénoncent le manque de moyens pour s'en prémunir autant que la gestion désordonnée de la crise.

Mieux vaut prévenir que guérir. Deux sénateurs de la commission des affaires étrangères et de la défense de la Haute Assemble, Rachel Mazuir (groupe socialiste et républicain) et Olivier Cadic (UDI-UC), ont décidé de mener leur "enquête" sur la cyberattaque qu'a subie le Quai d'Orsay le 5 décembre dernier, non pas dans l'intention de *"chercher les coupables et les responsables, mais de susciter un retour d'expérience",* a affirmé, mercredi 6 février, devant ses collègues, le sénateur Rachel Mazuir.

Cette cyberattaque, intervenue le 5 décembre 2018, mais révélée au grand public le 13 décembre, s'est abattue sur la base de données de la plate-forme Ariane. C'est elle qui permet aux Français, lorsqu'ils sont à l'étranger et s'ils s'y sont inscrits, de recevoir un certain nombre de consignes de sécurité par SMS ou courriel de la part du centre de soutien et de sécurité du ministère des Affaires étrangères. Au total, près de 550 000 personnes sont concernées par la cyberattaque, mais seules les données relatives aux personnes à contacter en cas d'urgence ont été dérobées, selon le Quai d'Orsay (nom, prénom, numéro de téléphone et adresse e-mail). *"Ni les mots de passe, ni les dates de destination des voyages n'ont été compromises et les données dérobées ne permettent pas de faire le lien entre les personnes à contacter et les titulaires des comptes Ariane",* tempère Rachel Mazuir.

Autre soulagement, mais qui n'est pas sans poser des questions : lors de l'envoi du courrier d'information des victimes du piratage, le ministère s'est rendu compte que plus de 200 000 adresses concernées étaient tout simplement inactives car elles remontaient aux origines de la création de la plate-forme, en 2010. Une anomalie lorsque l'on sait que les règles de protection des données de la base Ariane imposent que ces données soient effacées *"un mois après la date retour"* du Français en voyage.

Servir d'exemple

Sur le site de la plate-forme, il est pourtant indiqué qu'*"Ariane a fait l'objet d'un travail préparatoire approfondi avec la Commission nationale de l'informatique et des libertés (Cnil) en vue d'offrir aux usagers toutes les garanties en matière de sécurité et de confidentialité des données personnelles."*

La cyberattaque de la plate-forme Ariane n'a peut-être pas eu de onséquences *"dramatiques",* mais elle peut *"servir d'exemple",* a jugé Rachel Mazuir, pour qui *"le ministère et les autres services de l'État pourraient en tirer des enseignements".*C'est dans cette perspective que lui et Olivier Cadic ont démarré leurs travaux d'enquête, à partir du 19 décembre. Ils ont auditionné dans la foulée les principaux concernés, parmi lesquels le directeur général de l'Agence nationale de sécurité des systèmes d'information (Anssi),

Guillaume Poupard, le directeur des systèmes d'information du ministère, Philippe Lefort, ou encore la Cnil.

De ces auditions, les sénateurs tirent plusieurs conclusions sur l'attaque. D'abord, elle aurait largement pu être évitée. Ses auteurs ont profité d'une faille dans une des briques logicielles utilisées pour construire la plate-forme Ariane, faille que l'éditeur avait lui-même identifiée et pour laquelle il avait apporté un correctif. Problème : le ministère n'a pas pris le temps de faire la mise à jour nécessaire.

L'exploitation de cette faille et cette inadaptation révèlent donc, selon Rachel Mazuir, non seulement que les attaquants sont très au fait de l'existence de failles, mais aussi que le Quai d'Orsay, comme la plupart des ministères, n'investit pas assez dans sa sécurité informatique au regard de la transformation numérique dans laquelle il s'est lancé. Le ministère *"dispose d'un budget dédié au système d'information et d'effectifs en stagnation, alors qu'il s'est lancé dans une politique de numérisation et de mise à disposition de services en ligne, ce qui crée une interface de vulnérabilité"*, note le sénateur.

Pour lui, les outils réglementaires tels que la politique de sécurité des systèmes d'information de l'État (PSSIE) ne suffisent pas à faire de la sécurité une priorité pour l'ensemble des systèmes d'information (et pas seulement les plus critiques) tant que les moyens financiers et humains ne suivent pas. Celle-ci serait par conséquent insuffisamment mise en œuvre, comme nous l'indiquions dans notre dossier consacré à la cybersécurité.

Failles dans la communication

Autre dysfonctionnement révélé par cette affaire, la communication autour de la crise n'a pas été parfaite. Ceci est en partie dû aux nouveautés apportées par l'entrée en application du Règlement général sur la protection des données (RGPD) en mai dernier, lequel oblige, lorsqu'il y a compromission de données personnelles, d'en avertir la Cnil dans les 72 heures. Ce qu'a fait le ministère dès le 7 décembre.

Le sénateur Olivier Cadic déplore néanmoins que les discussions qui ont suivi entre la Cnil et la DSI du ministère, sur l'intérêt ou non d'avertir le grand public de ce piratage, son restées confinées *"sans autre appréciation externe ou évaluation de l'éventualité d'un autre motif de l'attaque qui pouvait être simplement l'atteinte à la réputation du ministère en affichant la vulnérabilité de ses applications, ni prise en compte du fait que les personnes concernées pouvaient découvrir leur présence dans cette base à cette occasion"*.

Décision a finalement été prise par le Quai d'Orsay d'adresser un courriel aux victimes du piratage, le 13 décembre. Sauf que ni l'Anssi ni la Cnil ne s'étaient préparées à la déferlante de sollicitations qui s'en est suivie. Pire encore, l'Anssi n'aurait pris connaissance de cette communication aux victimes que lorsqu'elle s'est retrouvée à devoir répondre à leurs questions et inquiétudes.

Le même jour, un communiqué de presse a également été diffusé, précisant que le ministère avait *"saisi la Commission nationale de l'informatique et les libertés (Cnil), ainsi que la justice des faits constatés"* et que *"des messages d'information aux personnes concernées sont également en cours d'envoi"*. Un communiqué qui a également fait l'objet d'un cafouillage, selon les sénateurs. *"On notera, en premier lieu, qu'il y a eu deux communiqués successifs, le premier impliquant l'Anssi sans son consentement et sans qu'elle ait été associée ni à la mise en place des correctifs, ni dans la préparation de cette communication",* a indiqué Oliver

Cadic. En revanche, le centre de crise et de soutien qui, lui, était en première ligne, n'a semble-t-il pas été impliqué.

Gestion de crise désordonnée

De leurs auditions, les deux sénateurs disent constater l'impréparation des administrations publiques, *"à l'exception de l'Anssi"*, face à ce type d'événements dont la multiplication est pourtant à craindre. *"À chaque étape, elles hésitent sur la conduite à tenir parce qu'elles n'ont pas expérimenté les difficultés, parce que les précédents sont peu nombreux, et qu'elles n'ont pas anticipé des scénarios de crise"*, note ainsi Oliver Cadic. Selon lui, une réflexion doit être impérativement menée au niveau interministériel, notamment pour davantage inclure l'Anssi dans la gestion de crises ministérielles.

Bien que mineure, cette cyberattaque et sa gestion mettent en évidence, pour les sénateurs, le sous-investissement des administrations publiques en matière de sécurité informatique. Une mission interministérielle est d'ailleurs en cours pour inspecter les moyens budgétaires et les effectifs des différents ministères consacrés au numérique, et notamment à sa sécurité.

En attendant, les deux sénateurs ont affirmé vouloir poursuivre leur mission de contrôle *"à la fois pour compléter la documentation du dossier Ariane mais aussi pour vérifier les efforts entrepris pour la sécurité de l'ensemble des systèmes d'information du ministère des Affaires étrangères",* et ce afin d'inciter *"les services de l'État à progresser pour mieux se prémunir des attaques et de leurs conséquences*."

Leurs collègues de la commission des finances ont de leur côté décidé, le 31 janvier, de lancer plusieurs missions de contrôle relatives au numérique, dont l'une porte justement sur la sécurité informatique de 4 institutions publiques.