NOTE DE SYNTHÈSE

RÉPUBLIQUE FRANÇAISE

CYBERATTAQUE CONTRE « ARIANE » : UNE EXPÉRIENCE QUI DOIT NOUS SERVIR

Commission des affaires étrangères, de la défense et des forces armées

Rapport d'information de MM. Rachel Mazuir et Olivier Cadic, sur la cyberattaque de la plateforme ARIANE du ministère de l'Europe et des affaires étrangères.

Rapport d'information n° 299 (2018-2019)

Le but de ce rapport d'information est, à partir d'un cas de cyberattaque aux conséquences limitées contre la plateforme « ARIANE » du ministère de l'Europe et des affaires étrangères, de tirer des enseignements qui permettront d'améliorer la résilience des administrations de l'Etat.

Le ministère de l'Europe des affaires étrangères (MEAE) a mis en place, depuis 2010 une plateforme de service « ARIANE » qui permet aux ressortissants français qui s'inscrivent en ligne de recevoir des consignes de sécurité lors de leurs voyages à l'étranger.

Chacun peut donc, sur le site « diplomatie.gouv.fr », créer un « compte utilisateur » et avant chaque voyage s'enregistrer en précisant ses lieux de passage, son numéro de téléphone portable et son adresse électronique, mais aussi, dans les données du compte utilisateur, les personnes à prévenir en cas d'urgence. Au cours du séjour à l'étranger et si la situation du pays le justifie, l'usager reçoit des recommandations de sécurité du Centre de crise et de soutien du ministère, par SMS ou par courriel, et peut être contacté en cas de crise. C'est donc un service très utile et très utilisé.

Le Centre de crise et de soutien du ministère est le service responsable du traitement de ces données. Les postes diplomatiques et consulaires français en sont destinataires. La plateforme est maintenue par la direction des systèmes d'information du MEAE.

Le 5 décembre 2018, la plateforme « ARIANE » a été victime d'une cyberattaque. Cette attaque a été détectée par un dispositif de protection mis en place par l'Agence nationale de sécurité des systèmes d'information (ANSSI). Ce dispositif a pu constater qu'une partie des données stockées dans cette base de données a été piratée.

Des données personnelles enregistrées lors de l'inscription sur la plateforme ont été dérobées. Selon le MEAE, il s'agit de données extraites de la table des personnes à contacter en cas d'urgence. Au total, ce sont 540 563 personnes qui sont concernées par ce vol de données. Ni les autres données des titulaires de comptes, ni leur mot de passe, ni les dates et destinations de leurs voyages n'ont été compromis. Les données dérobées ne permettaient pas de faire de lien entre les contacts et les titulaires de compte. En outre,

DLC N° 152 (2018-2019)

MAI 2019

il a été constaté à l'occasion de l'information des personnes concernées par l'envoi d'un courriel, que plus de 200 000 de ces adresses n'étaient plus actives.

Le service n'a pas été interrompu et la sécurisation des données a été restaurée, des mesures correctives ont été prises pour empêcher la reproduction d'une attaque selon les mêmes procédures.

L'incident a été connu du grand public le 13 décembre, date à laquelle le ministère a adressé un courriel d'information aux personnes concernées et un communiqué de presse. Ce communiqué annonçait que le ministère avait saisi la Commission nationale de l'informatique et des libertés (CNIL) ainsi que la justice des faits constatés.

Sitôt l'incident connu, la commission des affaires étrangères, de la défense et des forces armées du Sénat s'est saisie de ce dossier. En effet, depuis trois ans, les avis budgétaires de la commission sur le programme 129 « Coordination du travail gouvernemental » qui porte les crédits de l'ANSSI, soulignait les résultats insuffisants de la mise en œuvre de la politique de protection et de sécurité des systèmes d'information de l'Etat (PSSIE). En outre, cette cyberattaque touchait un ministère sur lequel la commission était pleinement légitime à assurer un contrôle. Le but n'était pas de stigmatiser d'éventuelles défaillances mais au contraire de susciter un retour d'expérience dont le MEAE, et au-delà les services de l'Etat, pourraient tirer des enseignements pour **améliorer leur résilience en favorisant l'émergence en leur sein d'une culture de la cybersécurité, en affectant les moyens nécessaires à la protection de leurs systèmes d'information et en garantissant, en cas de crise, la fluidité des relations entre les différents acteurs de la prévention et la protection (ANSSI, DSI des ministères, CNIL) mais aussi de la judiciarisation.**

De cet ensemble, plusieurs recommandations à l'attention du Gouvernement ont pu être formulées.

Au ministère de l'Europe et des affaires étrangères

Accélérer les procédures de mise à jour des logiciels pour lesquels des failles ont été identifiées, considérer ces actions de protection comme prioritaires, y affecter les moyens nécessaires.

Veiller à l'application rigoureuse de la circulaire interministérielle du 17 juillet 2014 sur la politique de sécurité des systèmes d'information de l'Etat (PSSIE).

Anticiper les remplacements des hauts fonctionnaires de défense (HFD), des fonctionnaires de sécurité des systèmes d'information (FSSI) et des RSSI afin d'éviter des vacances de poste et désigner systématiquement des suppléants afin d'éviter les vacances durant les phases de recrutement.

Mettre en place un système alertant la personne concernée qu'elle vient d'être inscrite dans la base « ARIANE » comme personne à prévenir en cas d'urgence.

Se doter des moyens d'effectuer une analyse complète de l'impact potentiel de la mise en œuvre de l'obligation d'information lorsque celle-ci peut présenter un risque potentiel pour la défense nationale, la sécurité nationale ou la sécurité publique.

Associer dès le départ la direction de la communication et de la presse à la gestion de l'incident.

Soigner la présentation des messages diffusés afin de favoriser la bonne indentification et compréhension par les personnes concernées.

Diffuser d'emblée un communiqué de presse complet (FAQ incluse, par exemple) compte tenu de la complexité de l'objet.

Améliorer la procédure de dépôt de plainte en mettant en place une procédure d'alerte immédiate des services de police et du Parquet par des moyens dématérialisés dès la survenue de l'incident et un circuit de transmission de la plainte officielle.

Formaliser une procédure de gestion de crise impliquant les directions concernées par les cyberattaques : HFDS, FSSI, DSI, direction de la sécurité diplomatique, direction de la communication et de la presse, direction des affaires juridiques et direction « métier » gestionnaire des données.

Au Premier ministre

Sensibiliser avec fermeté l'ensemble des ministères pour une application rigoureuse de la circulaire interministérielle du 17 juillet 2014 sur la politique de sécurité des systèmes d'information de l'Etat (PSSIE).

Étudier rapidement les moyens juridiques et techniques permettant à l'ANSSI de contraindre les administrations de l'Etat à appliquer ses préconisations, notamment abaisser le seuil de 9 M€ établi par l'article 3 du décret n°2014-879 du 1er août 2014, qui requiert que l'ANSSI[1] formule un avis relatif à la prise en compte de la sécurité informatique pour les grands projets de l'Etat.

Conditionner l'attribution, voire le versement des crédits, pour de nouveaux projets informatiques au respect des préconisations de l'ANSSI et à l'application d'un ratio de dépenses consacrées à la cybersécurité qui pourrait être fixé à 5% des crédits consacrés par chaque ministère au développement et à la maintenance de leurs applications informatiques ou numériques, qu'elles soient pilotées par les directions des systèmes d'information ou par les directions « métiers ».

Imposer des règles strictes en matière de recrutement des directeurs des systèmes d'information : une formation solide en matière de cybersécurité évaluée par l'ANSSI pour tout recrutement des nouveaux DSI ministériels ainsi qu'aux directeurs « métiers » pilotant la mise en œuvre de projets numériques ; inscription d'objectifs en matière de sécurité informatique définis par l'ANSSI dans leurs lettres de mission et pris en compte dans leur évaluation.

Formuler des recommandations aux administrations de l'Etat sur les éléments à prendre en considération pour la mise en œuvre des obligations de déclaration et d'information du RGPD et en matière de communication.

Prévoir notamment une information immédiate des services du Premier ministre et se doter d'une capacité de coordination de la réponse à apporter lorsque la mise en œuvre de l'obligation d'information peut présenter un risque potentiel pour la défense nationale, la sécurité nationale ou la sécurité publique, ainsi que d'une capacité de conseil pour la rédaction des instruments de communication.

Prendre en considération le risque afférent à cette obligation d'information et à la communication lorsque l'incident est évoqué en C4.

Mettre en place un numéro vert unique et identifiable pour renseigner les personnes concernées ou le public.

Mettre en place sous l'égide du SGDSN des sessions d'information réunissant les DSI des administrations de l'Etat d'une part, la section spécialisée du Parquet de Paris et les services compétents du ministère de l'Intérieur d'autre part, de façon à sensibiliser les administrations de l'Etat sur la nécessité de mise en place de procédures d'alerte, de dépôt de plainte et de recueil des éléments de preuves.

Rappeler aux administrations de l'Etat l'obligation de saisir les services compétents du ministère de l'Intérieur et le Parquet en cas de cyberattaque.

Formuler des recommandations aux administrations de l'Etat sur la gestion des incidents et des crises résultant de cyberattaques.

---

[1] *Ou du COMCYBER pour les projets de nature opérationnelle du ministère des Armées.*

Etudier la mise en place de formations spécialisées à destination des cadres des administrations de l'Etat.

Au ministère de la Justice

Renforcer la section spécialisée du Parquet de Paris.

Aux ministères de l'Intérieur et de la Justice

Se doter d'un outil statistique permettant d'apprécier le suivi du traitement judicaire des attaques informatiques dirigées contre les systèmes et réseaux gouvernementaux, ceux des opérateurs d'importance vitale, des établissements disposant de zones à régimes restrictifs, ou portant atteinte aux intérêts fondamentaux de la Nation.

A la CNIL

Veiller à la prise en compte de tous les éléments d'appréciation dans l'analyse des obligations d'information et de communication dans le respect du RGPD.

Ce rapport met en évidence le sous-investissement de nos administrations publiques en matière de cybersécurité. Votre commission alerte sur les conséquences que pourraient avoir des attaques massives contre des administrations mal préparées. La culture cyber doit y être mieux diffusée. Ces premières conclusions ne doivent pas paraître alarmistes, mais doivent au contraire contribuer à la prise de conscience des risques et de leur caractère multiforme.

Ce dossier doit être porté au plus haut niveau de l'Etat.

Le Premier ministre a lancé plusieurs missions dans cette direction que votre commission va suivre avec attention.

Vos rapporteurs souhaitent que ce rapport d'information, à partir d'un cas d'école, aux conséquences fort heureusement limitées, puisse inciter les services de l'Etat à progresser pour mieux se prémunir des attaques et de leurs conséquences.

Commission des affaires étrangères, de la défense et des forces armées
http://www.senat.fr/commission/etr/index.html
15 rue de Vaugirard 75006 Paris - secretariat-affetra@senat.fr

Les rapporteurs

M. Rachel MAZUIR
Sénateur de l'Ain

M. Olivier CADIC
Sénateur des Français établis hors de France

Le rapport complet est disponible sur le site du Sénat : http://www.senat.fr/notice-rapport/2018/r18-299-notice.html