N° 299

SÉNAT

SESSION ORDINAIRE DE 2018-2019

Enregistré à la Présidence du Sénat le 6 février 2019

RAPPORT D'INFORMATION

FAIT

au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la **cyberattaque** *de la* **plateforme ARIANE** *du ministère de l'Europe et des affaires étrangères,*

Par MM. Olivier CADIC et Rachel MAZUIR,

Sénateurs

(1) Cette commission est composée de : M. Christian Cambon, *président ;* MM. Pascal Allizard, Bernard Cazeau, Robert del Picchia, Mme Sylvie Goy-Chavent, MM. Jean-Noël Guérini, Joël Guerriau, Pierre Laurent, Cédric Perrin, Gilbert Roger, Jean-Marc Todeschini, *vice-présidents ;* M. Olivier Cigolotti, Mme Joëlle Garriaud-Maylam, M. Philippe Paul, Mme Marie-Françoise Perol-Dumont, *secrétaires ;* MM. Jean-Marie Bockel, Gilbert Bouchet, Michel Boutant, Olivier Cadic, Alain Cazabonne, Pierre Charon, Mme Hélène Conway-Mouret, MM. Édouard Courtial, René Danesi, Gilbert-Luc Devinaz, Jean-Paul Émorine, Bernard Fournier, Jean-Pierre Grand, Claude Haut, Mme Gisèle Jourda, MM. Jean-Louis Lagourgue, Robert Laufoaulu, Ronan Le Gleut, Jacques Le Nay, Rachel Mazuir, François Patriat, Gérard Poadja, Ladislas Poniatowski, Mmes Christine Prunaud, Isabelle Raimond-Pavero, MM. Stéphane Ravier, Hugues Saury, Bruno Sido, Rachid Temal, Raymond Vall, André Vallini, Yannick Vaugrenard, Jean-Pierre Vial, Richard Yung.

SOMMAIRE

Pages

PRINCIPALES RECOMMANDATIONS

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.

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

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.

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

<u>Au ministère de la Justice</u>

Renforcer la section spécialisée du Parquet de Paris.

<u>Aux ministères de l'Intérieur et de la Justice</u>

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.

<u>A la CNIL</u>

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.

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) en périphérie des systèmes d'information du ministère. 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 (nom, prénom, adresse électronique) et d'une partie des identifiants téléphoniques pour lesquels il avait été sagement prévu un stockage fractionné dans deux tables différentes, afin d'empêcher la reconstitution des numéros et donc leur exploitation frauduleuse. 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, 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**, à l'initiative de vos deux rapporteurs. 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)[1]. 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 les prochains incidents qui ne manqueront pas de se produire compte tenu des vulnérabilités de nos systèmes, d'une part, de la fréquence croissante, de l'ampleur et de la sophistication des attaques, d'autre part.

Ont été entendus, dès le 19 décembre, le directeur général de l'ANSSI, le directeur des systèmes d'information et le directeur de la sécurité diplomatique du MEAE, la direction générale de la sécurité intérieure (DGSI) qui est l'un des services disposant des capacités d'investigation pour rechercher l'origine d'une cyberattaque, la CNIL et enfin la section spécialisée du parquet de Paris.

Ces auditions ont été complétées par l'envoi de questionnaires écrits et par une réunion de retour d'expérience avec les services du ministère de l'Europe et des affaires étrangères au cours de laquelle les représentants de différents services et du cabinet du ministre ont exposé leurs appréciations à

---

[1] *Sénat n° 142 Tome IX (2016-2017) par MM. Bockel et Masseret, p. 37 et suiv.* http://www.senat.fr/rap/a16-142-9/a16-142-9.html
Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 24 et suiv. http://www.senat.fr/rap/a17-110-9/a17-110-96.html#toc105
Sénat n° 149 Tome IX (2016-2017) MM. Cadic et Mazuir p. 22 et suiv. http://www.senat.fr/rap/a18-149-9/a18-149-9.html

partir des premières observations des rapporteurs et examiner les pistes d'amélioration de leurs dispositifs de protection et de gestion de crise.

L'objectif de cette mission d'information, au-delà de la mise à jour de lacunes et d'insuffisances dans les procédures et les modes de fonctionnement, est d'inciter les administrations de l'Etat à 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.

En déroulant patiemment le fil d'une cyberattaque comme celle d' « ARIANE », vos rapporteurs ont essayé de comprendre comment le MEAE avait réagi et quels enseignements il pouvait en tirer pour renforcer sa résilience.

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

ÉVALUATION DE LA CAPACITÉ DU MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES À ÉVITER UNE CYBERATTAQUE

Comme la plupart des systèmes d'information, les systèmes d'information du ministère de l'Europe et des affaires étrangères font l'objet de très nombreux incidents de cybersécurité. La direction des systèmes d'information en évalue le nombre à 65 000 par jour. La très grande majorité sont des incidents mineurs, comme des mails indésirables qui sont rejetés et constituent une forme de « bruit de fond», mais au sein de cette masse, quelques dizaines peuvent être qualifiés de tentatives d'intrusion. La plupart fort heureusement bute sur les systèmes de protection mis en place qui résultent de la combinaison de la mise à jour des socles applicatifs, de la correction des failles, de la défense périmétrique grâce au filtrage des flux au moyen de passerelles de sécurité et de la défense en profondeur qui consiste à cloisonner les systèmes d'information de façon à éviter la migration d'une attaque d'un système à l'autre.

1. Le ministère de l'Europe et des affaires étrangères bénéficie d'un niveau de protection élevé

Le ministère de l'Europe et des affaires étrangères n'est sans doute pas le plus mal loti en matière de cyberprotection, compte tenu du caractère sensible des données traitées par ses systèmes d'information. Il dispose d'une capacité de protection jugée efficace et d'un niveau comparable à celle des autres ministères régaliens.

Néanmoins, on constatera qu'il n'est pas complètement en conformité dans la mise en œuvre de la circulaire interministérielle de 2014, qu'il revendique une certaine autonomie dans la gestion de sa cyber protection et que, historiquement, sa relation avec l'ANSSI apparaît plus complexe que celle entretenue par l'Agence avec d'autres ministères.

En outre, afin de détecter les éventuelles compromissions du système d'information (SI) du MEAE, l'ANSSI[1] déploie un système de supervision de la sécurité à sa périphérie. Ce dispositif n'est pas spécifique au MEAE et est présent dans la plupart des ministères. Il est notamment constitué de dispositifs de captation du trafic du réseau et de sondes déployés dans les centres informatiques ministériels. Les sondes analysent

[1] *Le ministère de l'Europe et des affaires étrangères fait l'objet d'un accompagnement approfondi par l'ANSSI du fait de son exposition internationale et de l'intérêt que peuvent présenter pour des attaquants utilisant des modes d'action sophistiqués les informations contenues dans ses systèmes d'information.*

les flux réseaux entrants et sortants du ministère, notamment les flux des applications web exposées sur Internet.

Les alertes issues de ces analyses sont remontées à l'ANSSI où une équipe se charge de les qualifier afin de vérifier leur bien-fondé et envoyer le cas échéant un signalement aux équipes du ministère. En cas de besoin, les équipes en charge du traitement d'incidents prennent le relai pour assister le ministère.

2. Ce niveau élevé de protection n'a pas empêché la survenue d'une cyberattaque visant un système ouvert sur l'Internet, le système « ARIANE »

Les systèmes d'information ouverts sur l'extérieur, notamment ceux interfacés avec le réseau Internet, sont les plus vulnérables. Les attaquants ont profité d'une faille dans une brique logicielle utilisée pour construire cette plateforme. L'éditeur du logiciel avait identifié cette faille et livré à la DSI du MEAE le correctif nécessaire. La mise à jour n'avait pas encore été installée.

La gestion des failles informatiques

Le renforcement des socles applicatifs par la mise à jour et la correction des failles est un moyen important de protection. Mais c'est un travail sans fin. L'insécurité est consubstantielle aux systèmes informatiques. L'acquisition d'un produit ne garantit pas l'exploitant contre des failles. Il n'existe pas de garantie contractuelle de stabilité des produits, ni de mise à jour au-delà d'un certain temps. On considère, habituellement, qu'une ligne de code sur 10 000 est défectueuse. Les éditeurs, lorsqu'ils détectent ces défaillances produisent des mises à jour des logiciels mais toutes les mises à jour ne sont pas utiles. Tout dépend de l'utilisation faite du logiciel qui peut induire ou non une vulnérabilité. Elle nécessite donc une analyse préalable à réception et avant son implantation. Elle peut avoir une incidence sur la stabilité d'ensemble du système d'information et son implantation peut entraîner une charge de travail plus ou moins importante qu'il faut évaluer et programmer. La direction des systèmes d'information du ministère de l'Europe et des affaires étrangères gère environ 300 applications et donc une dizaine de milliers d'applicatifs qui ont leur propre vie. Il convient donc de définir également des priorités dans la programmation de ces travaux et de disposer des ressources humaines disponibles pour absorber les périodes de suractivité sans nuire au développement des projets en cours. Ce travail est organisé par la DSI du MEAE par des réunions régulières dédiées.

En l'espèce, cette mise à jour n'avait pas été considérée comme une absolue priorité. Les assaillants ont su habilement profiter de cette vulnérabilité.

La faille a, depuis, été corrigée en urgence par la DSI du MEAE avec le concours de l'ANSSI[1].

3. De cette situation, cinq enseignements peuvent être tirés

Premièrement, si quelques attaquants connaissent les failles, l'édition d'un correctif en révèle plus largement l'existence et suscite des appétits. Plus on tarde à installer une mise à jour, plus un système d'information est vulnérable.

Deuxièmement, comme d'autres ministères, le MEAE dispose d'un budget et d'effectifs dédiés au système d'information 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. Il consacre des moyens globalement insuffisants à la cybersécurité et concentre ceux-ci - on ne peut le lui reprocher - sur les systèmes d'information et de communication les plus stratégiques comme la sécurité des postes et des réseaux diplomatiques.

Crédits et Effectifs de la DSI du MEAE

	2015 (exécuté)	2016 (exécuté)	2017 (exécuté)	2018 (prévision exécution)	2019 (prévision LFI, préciser si gel)
Crédits de la DSI	38 671 000 €	38 671 000 €	38 671 000 €	38 671 000 €	38 671 000 €
T3	30 744 606 €	29 952 937 €	32 146 329 €	31 798 957 €	n.c (gel)
T5	4 324 316 €	6 148 807 €	3 959 521 €	5 140 241 €	2 783 550 €
Total	35 068 922 €	36 101 745 €	36 105 850 €	36 939 198 €	
T2 (hors CAS pension)	41 488 980 €	42 157 636 €	42 664 139 €	43 228 150 €	n.c.
Effectifs de la DSI	500	505	507	500	n.c.

Troisièmement, vos rapporteurs ont été informés que le ministère avait subi, par le passé, des vacances de postes au niveau de la chaîne de sécurité placée sous la responsabilité du Haut fonctionnaire de défense et de sécurité, dont l'une des missions est la gouvernance de la sécurité des systèmes d'information. Le recrutement des fonctionnaires de sécurité des systèmes d'information (FSSI) chargés de la mise en place de la politique de sécurité des systèmes d'information est difficile en raison du nombre limité

[1] *L'incident ARIANE a été pris en compte et des préconisations ont été formulées par l'ANSSI en lien avec les équipes du ministère de l'Europe et des affaires étrangères.*

de personnes susceptibles d'exercer des responsabilités de ce niveau et de la concurrence observée sur le marché du travail pour de tels profils. Il s'agit de contractuels. Le ministère emploie 2 FSSI, au sein de la direction de la sécurité diplomatique et plusieurs responsables de la sécurité des systèmes d'information (RSSI) au sein de la DSI où ils sont chargés de la mise en œuvre des directives de sécurité. Ce sont les FSSI qui assurent les remontées d'information vers la CNIL et l'ANSSI. Actuellement, l'ensemble des postes sont pourvus. Il importe autant que faire se peut d'anticiper les vacances de postes et d'assurer une redondance afin d'éviter une éventuelle vacance durant la phase de recrutement.

Quatrièmement, la circulaire interministérielle du 17 juillet 2014 sur la politique de sécurité des systèmes d'information de l'Etat (PSSIE) est appliquée de façon hétérogène, ce qui montre le caractère très limité des interventions réglementaires : sans affectation de moyens, elles risquent de demeurer un seul instrument de communication.

Dans leur avis sur les PLF 2017[1], 2018[2] et 2019[3], vos rapporteurs s'inquiétaient de la lenteur de ce processus. Les résultats ne se sont guère améliorés. Le niveau effectif de conformité, qui fait l'objet d'un indicateur[4] sous l'objectif 6 du programme 129 « *améliorer la sécurité et la performance des systèmes d'information de l'Etat* », tarde toujours à atteindre des niveaux en adéquation avec les enjeux. Si l'on constate une meilleure prise en compte des enjeux par les autorités, celle-ci reste insuffisante. Cette situation consternante et alarmante a été confirmée par la *Revue stratégique de cyberdéfense de février 2018*[5].

Cinquièmement, tout cela pose concrètement la question d'un pilotage interministériel par affectation de moyens notamment par le respect d'un ratio obligatoire consacré à la cybersécurité. L'ANSSI n'a pas aujourd'hui de telles capacités.

Vos rapporteurs observaient, dans leur avis sur le PLF 2019[6] **,** que ce constat a pu être partagé dans le cadre des travaux interministériels du projet « *Action publique 2022* ». Plusieurs chantiers ont été lancés afin de renforcer le niveau de sécurité des systèmes d'information de l'État.

---

[1] *Sénat n° 142 Tome IX (2016-2017) par MM., Bockel et Masseret, p. 37 et suiv.* http://www.senat.fr/rap/a16-142-9/a16-142-9.html

[2] *Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 24 et suiv.* http://www.senat.fr/rap/a17-110-9/a17-110-96.html#toc105

[3] *Sénat n° 149 Tome IX (2016-2017) MM. Cadic et Mazuir p. 22 et suiv.* http://www.senat.fr/rap/a18-149-9/a18-149-9.html

[4] *Indicateur 6-1 « Niveau de sécurité des systèmes d'information de l'Etat »*

[5] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf *page 56 et suiv.*

[6] [6] *Sénat n° 149 Tome IX (2016-2017) MM. Cadic et Mazuir p. 23 et suiv.* http://www.senat.fr/rap/a18-149-9/a18-149-9.html

Ils estimaient néanmoins que sans volonté politique affirmée, sans moyens financiers significatifs et sans outils réglementaires coercitifs, il sera difficile de lutter contre une logique qui valorise la multiplication de systèmes d'information et des applications numériques, pour apporter de nouveaux services, et parfois pour se substituer à moindre coût à des services existants.

Recommandations

<u>Au ministère de l'Europe et des affaires étrangères</u>

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 et de sécurité (HFDS), 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.

<u>Au Premier ministre</u>

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 ».

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

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.

LA DÉCLARATION DU VOL DE DONNÉES PERSONNELLES À LA CNIL ET SES CONSÉQUENCES

Conformément aux dispositions légales, l'application « ARIANE » a fait l'objet d'une déclaration à la CNIL lors de sa mise en oeuvre.

1. L'inscription des données de tiers et leur conservation : une information insuffisante

La notice explicative de l'application[1] indique que « *le service Ariane conçu en concertation avec la CNIL offre toutes les garanties de sécurité et de confidentialité des données personnelles* » et que « *les données sont effacées un mois après la date retour* ».

Cette durée de conservation semble ne concerner que les données relatives aux déplacements, non les données de base du dossier, dont les données relatives aux contacts puisque plus de 500 000 noms étaient stockés dans cette table.

Le ministère de l'Europe et des affaires étrangères a précisé le 24 janvier 2019[2] que **ces données faisaient l'objet d'une destruction automatique au bout de trois années d'inactivité du compte.**

Cela pose au demeurant la question du statut des données personnelles des contacts enregistrées par leurs proches avec ou sans leur consentement, présumé tacite. Le Règlement (européen) général sur la protection des données (RGPD), récemment entré en vigueur dans son article 14 précise les informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée[3].

Si cet enregistrement de données personnelles par un tiers a pu être admis initialement par la CNIL, il n'en a pas moins suscité des interrogations des personnes concernées lorsqu'elles ont reçu le courriel du ministère les informant du vol de leurs données personnelles. Un système de génération automatique d'un courriel indiquant à la personne concernée qu'elle vient d'être inscrite dans la base « ARIANE » comme personne à prévenir en cas d'urgence par M. X. aurait permis de l'éviter.

---

[1] *Site France Diplomatie* https://www.diplomatie.gouv.fr/fr/le-ministere-et-son-reseau/actualites-du-ministere/article/vous-partez-en-voyage-inscrivez-vous-sur-ariane *voir le document en Annexe*

[2] *Dans une modification de la réponse à la FAQ (foires aux questions) mise en ligne à l'appui du communiqué de presse rendant public la cyberattaque le 13 décembre 2019*

[3] *Article 14 du* Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article14

2. L'application des obligations du RGPD en cas de perte de données

Depuis l'entrée en application du Règlement général sur la protection des données (RGPD), la compromission de données personnelles doit faire l'objet d'une déclaration à la CNIL dans les 72 heures de sa détection[1].

Le MEAE s'est conformé à cette obligation puisque la déclaration a été faite via un formulaire en ligne dès le 7 décembre.

La question s'est alors posée pour le ministère de savoir si cette attaque présentait des risques tels, qu'outre son signalement à la CNIL, il devait faire l'objet d'une communication aux personnes concernées d'une part, au public d'autre part[2]. Du dialogue entre les deux parties, la DSI et la CNIL, et parce qu'il y avait un risque d'utilisation des données pour des opérations d'hameçonnage ou d'escroquerie[3], qui, le cas échéant, auraient pu engager la responsabilité du ministère, la décision a été prise de communiquer.

Cet échange illustre bien la difficulté à peser le poids des différents arguments et l'intérêt en termes de réputation[4], de protection, de sécurité, de risque juridique, d'atteinte à la sécurité nationale. D'où l'intérêt à capitaliser les retours d'expérience afin d'améliorer les prises de décision futures.

D'après les informations communiquées à vos rapporteurs, ce dialogue est resté confiné dans un premier temps, entre la DSI et le FSSI côté ministère, et la CNIL. L'atteinte à la réputation du ministère par l'affichage la vulnérabilité de l'une de ses applications et le fait que les personnes concernées pouvaient découvrir leur présence dans cette base à l'occasion de cette communication n'a probablement pas été pleinement pris en compte lors de la préparation de ces décisions. Ceci aurait permis, le cas échéant, d'orienter différemment la communication.

Il faut dire que le non-respect de ces nouvelles obligations pouvait entraîner des sanctions pénales.

Il existait pourtant des marges d'appréciation qui n'ont pas été complètement exploitées. Le RGPD prévoit en effet dans son article 23 des

---

[1] *Article 33 du* Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article33

[2] *Article 34 du* Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article34

[3] *par exemple en demandant l'envoi d'argent en invoquant la détresse d'un parent séjournant à l'étranger*

[4] *Qui pouvait être évalué à charge comme à décharge : la reconnaissance par le ministère lui-même de sa vulnérabilité pouvant être le but recherché par l'assaillant pour porter préjudice à la réputation du ministère. A l'inverse, ne pas communiquer présenter le risque de révéler qu'une administration de l'Etat qui plus est en charge de la politique européenne était la première à enfreindre le RGPD.*

possibilités de dérogation permettant de s'exonérer de cette information en cas de risque pour la défense et le sécurité nationale[1].

Faute sans doute d'une gestion de la crise à un niveau plus approprié élargissant les parties prenantes à la décision (interministériel par exemple), l'analyse est restée principalement fondée sur les risques juridiques et techniques.

Le Centre de coordination des crises cyber est pourtant l'instance appropriée pour la coordination interministérielle[2]. Le cas de la cyberattaque contre « ARIANE » a fait l'objet d'un signalement et d'échanges au sein du C4 sans toutefois être un sujet d'intérêt majeur pour l'ensemble des parties prenantes à cette enceinte. Il est probable que la question n'a été abordée que du point de vue technique.

Vos rapporteurs ne considèrent pas que l'information et la communication, en le cas d'espèce, ne se justifient pas ; les arguments en faveur de la décision prise sont parfaitement recevables. Ils regrettent simplement que les différents risques et impacts qu'entraînait une communication large n'aient pas été évalués et que le nombre de parties prenantes à la préparation de la décision n'ait pas été élargi ce qui aurait sans doute permis cette évaluation plus complète.

Recommandations :

<u>Au ministère de l'Europe et des affaires étrangères</u>

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.

<u>A la CNIL</u>

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

---

[1] *Article 23 du* Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article23*

[2] *Le C4 est l'enceinte privilégiée de partage de l'information entre les services de l'Etat chargés d'une mission de cybersécurité. Ainsi les détails opérationnels font l'objet d'échanges fréquents, et ce dans les diverses formations du C4, en tant que de besoin et en fonction de l'expertise de chaque membre. Voir également la Revue stratégique de cyberdéfense p. 54* *http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf*

Au Premier ministre

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.

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.

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

LA COMMUNICATION SUR L'ATTAQUE ET SES CONSÉQUENCES

Compte tenu de cette demande de la CNIL, une réunion s'est tenue le 12 décembre sous la présidence du Secrétaire général du ministère de l'Europe et des affaires étrangères au cours de laquelle il a été décidé du contenu du message à adresser aux personnes concernées et des éléments devant figurer dans le communiqué de presse.

Cette réunion a déterminé les éléments à faire figurer dans le communiqué de presse qui a été diffusé le 13 décembre à l'issue de l'envoi des courriels. Les grandes lignes de la communication et le communiqué de presse ont été validés par le cabinet du Ministre.

1. L'information directe des personnes concernées

Le 13 décembre était adressé un courriel aux plus de 500 000 personnes concernées[1] en différents envois.

Sur ce nombre important de courriels, 230 000 adresses étaient en réalité inactives ou erronées compte tenu de l'ancienneté de leur recueil.

L'ANSSI et la CNIL, dont le nom et l'adresse des sites Internet figuraient dans le courriel, ont reçu, dans la foulée, des dizaines de demandes d'information. Le ministère de l'Europe et des affaires étrangères lui-même a recueilli des réactions montrant que l'envoi massif de ce message a eu pour effet d'inquiéter nombre de destinataires qui, soit n'étaient pas informés de leur présence dans ce fichier, soit n'avaient aucune idée des données contenues dans celui-ci, et qui pensaient être victimes d'une opération d'hameçonnage sous couvert d'un message falsifié du ministère, soit qui craignaient que leurs données bancaires ou d'autres données personnelles aient été dérobées[2].

Ce courriel, qui ne présentait aucun logo, ni aucun autre avertissement, et contenait des liens à activer, a même pu paraître frauduleux à certains destinataires compte tenu des pratiques courantes d'hameçonnage. Le service de la communication et de la presse du ministère qui était confronté pour la première fois à ce cas de figure, a reconnu au cours du retour d'expérience organisé à notre demande qu'il avait une marge d'amélioration dans la formalisation des communications de cette nature.

---

[1] *Texte en annexe*

[2] *« merci d'avoir prévenu, je vous redonne mes coordonnées », « est-ce que d'autres données ont été volées » ? (même si elles ne sont pas recueillies par Ariane), « qui a donné mon nom » ? « pourquoi suis-je dans cette base ? », « supprimer mes données !»….*

Les personnes, qui ont pris contact, ont pu être rassurées mais personne dans les organisations concernées n'était véritablement préparé aux réactions des personnes concernées[1], l'ANSSI tout particulièrement qui a déclaré n'avoir été informée de la communication du MEAE qu'a posteriori lorsqu'elle a été confrontée à des appels du public à la suite du courriel.

2. La communication publique

Il a été décidé également de rendre publique cette attaque et ses conséquences. Un communiqué de presse a été préparé par la direction de la communication et de la presse à partir d'éléments techniques fournis la DSI.

Il avait pour but de dissiper les doutes qui auraient pu naître de l'envoi du courriel et de répondre aux questions des journalistes forcément alertés par la réception des courriels (certains journalistes donnant le nom de collègues ou de cadres de leurs rédactions comme personnes à prévenir en cas d'incident lors de leurs déplacements).

Ce communiqué de presse[2] a été repris parfois de façon alarmiste par les médias voire déformée par certains médias, ce qui a pu ajouter à la confusion[3].

Une version du communiqué assortie d'« une foire aux questions » (FAQ) a été mise en ligne sur le site « France Diplomatie ».

On notera, en premier lieu, qu'il y a eu deux communiqués successifs, le premier impliquant, dans les réponses à la FAQ, l'ANSSI sans son consentement et sans qu'elle ait été associée ni à la mise en place des correctifs, ni à la préparation de cette communication, le second ayant retiré la mention la concernant.

Compte tenu de l'effet de cette communication, vos rapporteurs s'interrogent sur un élargissement du nombre de parties prenantes à la décision de communiquer et sur le contenu de la communication.

Enfin, sur le fond, vos rapporteurs, s'interrogent également sur l'opportunité d'indiquer que la cyberattaque n'a rien d'un évènement exceptionnel, que « *le ministère fait l'objet d'attaques de toutes natures et de toutes origines et s'est organisé en conséquence avec l'aide de ses partenaires*

---

[1] Le Ministère de l'Europe et des affaires étrangères avait toutefois fourni des éléments d'information aux opérateurs de son standard téléphonique en cas de demande des personnes ayant reçu le courriel.

[2] Textes joints en annexe

[3] Un média en ligne titrant : « Le ministère des affaires étrangères a été victime d'un piratage – certaines données personnelles de Français partant à l'étranger ont été exposées ». Et dans le texte, il est écrit « les noms prénoms, numéros de téléphone portable et adresse mail des voyageurs ont été exposés, mais pas leur destinations de voyage, ni le nom des personnes à prévenir en cas de besoin ». Alors que le communiqué indiquait bien que seules les données relatives aux personnes à prévenir en cas de besoin ont été exfiltrées.

interministériels, notamment l'ANSSI », message peu crédible au moment où il révèle la vulnérabilité d'une de ses plateformes.

Recommandations

<u>Au ministère de l'Europe et des affaires étrangères</u>

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.

<u>Au Premier ministre</u>

Formuler des recommandations aux administrations de l'Etat sur les éléments à prendre en considération en matière de communication.

Prévoir notamment une information immédiate des services du Premier ministre et se doter d'une capacité de conseil pour la rédaction des instruments de communication 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.

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

Prendre en considération le risque afférent à la communication lorsque l'incident est évoqué en C4.

LES MODALITÉS DE SAISINE DE L'AUTORITÉ JUDICIAIRE

1. Le communiqué du 13 décembre indiquait que le ministère avait déposé une plainte auprès du Procureur

Le dépôt d'une plainte est tout à fait souhaitable. Même si l'attaque ne se traduit pas par un dommage matériel important pour le ministère, reste l'atteinte à sa réputation. **Il faut d'ailleurs féliciter le ministère de l'Europe et de affaires étrangères pour cette décision judicieuse qui reste exceptionnelle au sein des administrations pourtant victimes régulières de cyberattaques**, alors même que le discours de la puissance publique et notamment de l'ANSSI consiste à inciter les administrations, les entreprises et même les particuliers à signaler les incidents et à porter plainte. **En outre, il s'agit d'infractions, de délits, voire de crimes dont la commission doit être portée à la connaissance de la justice, obligation sanctionnée pénalement pour les fonctionnaires en application de l'article 40 du code de procédure pénale.**

Vos rapporteurs ont souhaité dans le strict respect de l'indépendance et des compétences de l'autorité judiciaire comprendre comment fonctionnait ce que la Revue stratégique de cybersécurité de février 2018 appelle la chaîne d'« investigation judiciaire [1]» et comment était mise en œuvre cette chaîne en cas d'attaque des administrations de l'Etat.

Vos rapporteurs ont entendu les magistrats du parquet de Paris et notamment de sa section spécialisée (F1), créée en 2014 et dotée d'une compétence concurrente nationale depuis 2016 en matière d'atteintes aux systèmes informatisés de données. Cette section reçoit 2 000 à 2 500 plaintes par an. Elle est en mesure de déclencher des procédures d'entraide internationale et jouit d'une solide réputation puisqu'elle coordonne à l'échelon européen l'enquête sur la cyberattaque *Notpetya*. Vos rapporteurs se sont également entretenus avec la DGSI[2], qui peut être saisie pour constater les faits et rechercher des preuves et les auteurs.

Il va de soi que vos rapporteurs, ne se sont en aucune façon substitués à l'autorité judiciaire dont ils respectent la pleine indépendance,

---

[1] *Revue stratégique de cyberdéfense p.71 et suiv.*
http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

[2] *La direction générale de la sécurité intérieure, dispose, au sein de sa sous-direction des affaires judiciaires, d'une section spécialisée dans le traitement des affaires liées à la cybercriminalité. Ce service dispose d'une compétence exclusive pour évoquer toutes les infractions résultant d'une violation des articles inscrits au chapitre 3 du code pénal (art. 323 - 1 à 323 - 7), dans la mesure où ces actions sont directement menées contre les intérêts fondamentaux de la Nation. Il s'agit de toutes les attaques informatiques dirigées contre les systèmes et réseaux gouvernementaux, les attaques contre les systèmes et réseaux appartenant à des opérateurs d'importance vitale (OIV) ou des établissements disposant de zones à régimes restrictifs, et, enfin, toute atteinte à un système susceptible de porter atteinte aux intérêts fondamentaux ce la Nation.*

garantie par la Constitution. Ils se sont limités, au cas d'espèce, aux modalités de saisines de l'autorité judicaire. En aucun cas, ils n'ont évoqué le fond de ce dossier.

2. De ces entretiens, il ressort une absence de procédure formalisée au sein des administrations

La DGSI n'a été saisie ni par le ministère de l'Europe et des affaires étrangères, ni par l'ANSSI auprès de laquelle le ministère de l'Intérieur dispose pourtant d'un officier de liaison[1]. Même si la DSI, en collaboration avec l'ANSSI a pris les dispositions nécessaires pour conserver les traces de l'attaque pour des investigations ultérieures, une saisine de la DGSI eût été préférable, dès la constatation de l'attaque.

Le Parquet, quant à lui, a été informé le 14 décembre en lisant la presse suite à la publication du communiqué du 13, lequel mentionnait pourtant la saisine du Procureur.

En réalité, la plainte dont le ministère a communiqué le texte à vos rapporteurs, sous forme d'une déclaration du Ministre au Procureur de Paris, signé par le sous-directeur des affaires juridiques internes du ministère de l'Europe et des affaires étrangères, ne parviendra au palais de Justice de Paris que le 4 janvier où elle est enregistrée par le service du courrier avant d'être transmise au destinataire.

Il aura donc fallu trois semaines pour que cette saisine soit effective. On aurait pu imaginer des circuits d'information plus rapides.

La plainte officielle n'aboutira au cabinet du Procureur de Paris que le 7 janvier et à la section chargée de la délinquance et de la criminalité cyber que le 15 janvier montrant une viscosité interne à l'administration du Parquet. La DGSI ne sera officiellement saisie que le 10 janvier et ne recevra la plainte officielle en provenance du Parquet que le 15, soit 6 semaines après le déroulement de l'attaque.

Au demeurant, on peut aussi s'interroger sur le manque d'initiative des services de police et du Parquet qui auraient pu, dès la publicité donnée à l'attaque, se saisir sans attendre le dépôt d'une plainte.

Cette absence de réactivité montre à l'évidence que personne ne savait quelle conduite tenir et n'était préparé à faire face à ce type d'attaque. Les procédures d'activation de la chaîne judiciaire, pourtant parfaitement identifiées par la Revue stratégique de cyberdéfense de février 2018, n'étaient pas effectivement mises en place au sein du ministère de l'Europe

[1] *Cet officier de liaison est chargé de coordonner les échanges de l'ANSSI avec les services enquêteurs saisis des incidents que l'agence est amenée à traiter et a fortiori lorsqu'elle est auditionnée ou lorsqu'une réquisition a été émise.*

et des affaires étrangères. Existait-il un doute chez les responsables de ce ministère sur l'utilité des poursuites, motivant cette absence de célérité ?

Or, il est clair, comme il a pu l'être constaté dans d'autres domaines, que le taux d'élucidation des crimes et délits progresse en fonction du nombre de plaintes déposées et de la rapidité des dépôts. Des catalogues des modes d'attaques peuvent être dressés qui permettent d'identifier des signatures et de remonter des filières, l'utilisation de l'intelligence artificielle permettra à l'avenir en scannant les modes d'attaque et en les comparant d'accélérer ces processus d'identification.

Même si les données relatives à l'attaque ont pu être conservées sans être altérées, on imagine que l'intervention dans les premières heures des services compétents peut avoir un intérêt pour recueillir des preuves, ou des traces qu'un attaquant peut effacer progressivement ou, en tous cas, pour vérifier si les données font l'objet d'un commerce illicite, ce qui n'entre évidemment pas dans les compétences de la DSI du ministère. Ceci a été confirmé à vos rapporteurs par les magistrats du Parquet

Il n'est pas non plus évident, faute d'informations réciproques et de procédures préalables, que les preuves conservées répondent aux besoins de la procédure judicaire. En toute bonne foi, les agents de la DSI ont pu conserver des éléments qui ne correspondraient pas strictement aux besoins particuliers d'une enquête judiciaire.

Sans doute, la mise en place du RGPD permettra-t-elle d'avancer grâce à l'obligation de déclaration et de publicité, mais manifestement, un travail d'information sur la mise en œuvre de la chaîne judicaire et de coordination semble nécessaire auprès des décideurs des administrations de l'Etat.

Il serait souhaitable par ailleurs que les ministères de l'Intérieur et de la Justice, en lien avec l'INSEE, se dotent 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, en recensant le nombre d'infractions, délits ou crimes constatés, le nombre de plaintes déposées et en calculant les taux d'élucidation, de classement sans suite et de réponse pénale comme cela existe dans d'autres domaines. Vos rapporteurs comprennent que la nouveauté de ce domaine et l'hétérogénéité des incidents ont pu retarder la mise en œuvre d'un tel outil mais il devient désormais urgent d'opérer ce travail si l'on veut crédibiliser les actions de la police et de la justice en ce domaine

Recommandations

<u>Au ministère de l'Europe et des affaires étrangères</u>

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.

<u>Au Premier ministre</u>

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.

<u>Au ministère de la Justice</u>

Renforcer la section spécialisée du Parquet de Paris.

<u>Aux ministères de l'Intérieur et de la Justice</u>

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.

UN SENSIBILISATION NÉCESSAIRE AU PILOTAGE DE LA GESTION DE CRISE EN CAS DE CYBERATTAQUE

L'examen de ce dossier a montré, vos rapporteurs n'en sont pas surpris, que les administrations, à l'exception de l'ANSSI dont c'est la raison d'être, ne étaient guère préparées, qu'à chaque étape, elles hésitaient sur la conduite à tenir parce qu'elles n'avaient pas expérimenté auparavant les mêmes difficultés, parce que les précédents étaient peu nombreux, et qu'elles n'avaient pas anticipé des scénarios de crise.

Vos rapporteurs estiment qu'une réflexion doit être engagée au sein des ministères et sans doute, au moins dans la phase initiale, au niveau interministériel en matière de gestion de crise cyber. Quels sont les acteurs internes et externes concernés ? Quels sont les niveaux de décisions adéquats ? Qui pilote la gestion de crise ? Selon quelles procédures ? Comment communiquer et à quel moment pour ne pas ajouter une crise à la crise ?... Des modes d'action restent à construire et à éprouver sous forme d'exercices. Il existe des plans à l'échelle interministérielle pilotés par le SGDSN pour des attaques du haut du spectre, mais pour des attaques de moyenne ampleur, les ministères restent démunis et l'ANSSI ne peut pourvoir à tout. En l'espèce, cette attaque n'a pas été considérée comme relevant du haut du spectre par le centre opérationnel de sécurité des systèmes d'information (COSSI) compte tenu de sa nature et l'ANSSI, qui l'a détectée, a très vite passé le relais au ministère.

Pour autant, elle relevait d'un ministère régalien et elle aurait pu comporter un risque potentiel pour la sécurité nationale. Il s'agissait d'un premier cas de mise en œuvre de la RGPD, elle était susceptible de faire l'objet d'une publicité et devait déboucher sur une procédure judiciaire, vos rapporteurs estiment que cette attaque aurait mérité un suivi interministériel plus solide et plus complet portant sur l'ensemble des aspects de gestion de l'incident. Mais cela n'est pas toujours bien perçu ou accepté par des administrations souvent soucieuses de leur autonomie de gestion….

Recommandations

<u>Au ministère des affaires étrangères</u>

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

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

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

CONCLUSION

Ces premières conclusions de vos rapporteurs ne doivent pas paraître alarmistes, mais doivent au contraire contribuer à la prise de conscience des risques et de leur caractère multiforme. En déroulant modestement le « fil d'ARIANE », 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.

Une prise de conscience est nécessaire et 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. En attendant vos rapporteurs continueront à l'occasion de leurs travaux annuels sur les crédits du programme 129 « coordination du travail gouvernemental » à vérifier les efforts entrepris pour la sécurité de l'ensemble des systèmes d'information des ministères, y compris naturellement celui des affaires étrangères en étroite liaison avec les rapporteurs du programme 105 de la Mission « Action extérieure de l'Etat ».

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.

EXAMEN EN COMMISSION

Mercredi 6 février 2019, la commission des affaires étrangères, de la défense et des forces armées, sous la présidence de M. Cédric Perrin, vice-président, a examiné le rapport de MM. Rachel Mazuir et Olivier Cadic, sur la cyberattaque de la plateforme ARIANE du ministère de l'Europe et des affaires étrangères.

M. Rachel Mazuir, rapporteur. - Le ministère des affaires étrangères a mis en place, depuis 2010, une plateforme de service Ariane permettant aux ressortissants français préalablement inscrits en ligne de recevoir des consignes de sécurité lors de leurs voyages à l'étranger. Chacun peut ainsi créer un compte utilisateur sur le site diplomatie.gouv.fr et s'enregistrer avant chaque voyage en précisant ses lieux de passage, son numéro de téléphone portable et son adresse électronique, ainsi que les coordonnées des personnes à prévenir en cas d'urgence. Si la situation du pays le justifie, l'usager reçoit lors de son voyage 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. Ce service est très utile et très utilisé.

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

Le 5 décembre 2018, la plateforme Ariane a été victime d'une cyberattaque, détectée par le dispositif de protection mis en place par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en périphérie des systèmes d'information du ministère. Une partie des données stockées dans cette base de données a été piratée.

Des données personnelles ont été dérobées : il s'agit de données extraites de la table des personnes à contacter en cas d'urgence : noms, prénoms, adresses électroniques, ainsi qu'une partie des identifiants téléphoniques pour lesquels il avait sagement été prévu un stockage fractionné dans deux tables différentes afin d'empêcher toute exploitation frauduleuse. Au total, 540 563 personnes 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 compromises. Les données dérobées ne permettent pas d'établir de lien entre les contacts et les titulaires de compte. En outre, il a été constaté lors de l'opération d'information des personnes concernées par courriel que plus de 200 000 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 aux personnes concernées et a publié un communiqué de presse annonçant que la Commission nationale de l'informatique et des libertés (CNIL) et la justice avaient été saisies des faits constatés.

Sitôt l'incident connu, nous avons demandé à organiser des auditions pour recueillir des éléments d'information sur cette attaque et, plus largement, sur la sécurité des systèmes d'information du ministère des affaires étrangères, sur lequel notre commission est fondée à exercer un contrôle, sachant en outre que cela faisait deux ans qu'elle signalait dans son avis budgétaire sur l'Anssi les résultats insuffisants de la politique de protection et de sécurité des systèmes d'information de l'État (PSSIE). La commission a validé cette démarche lors de sa réunion du 16 janvier.

Nous nous sommes naturellement concentrés dans un premier temps sur cette cyberattaque dans l'intention non pas de chercher des responsables, mais de susciter un retour d'expérience dont le ministère et, au-delà, les services de l'État pourraient tirer des enseignements à l'occasion d'autres incidents, sachant qu'il y en aura d'autres, compte tenu des vulnérabilités de nos systèmes, d'une part, de la fréquence, de l'ampleur et de la sophistication des attaques, d'autre part.

Nous avons donc entendu, dès le 19 décembre, le directeur général de l'Anssi, le directeur des systèmes d'information et le directeur de la sécurité diplomatique du ministère des affaires étrangères, puis la direction générale de la sécurité intérieure (DGSI), qui est l'un des services disposant des capacités d'investigation pour rechercher l'origine d'une cyberattaque, la CNIL et enfin la section spécialisée du parquet de Paris. Nous entendrons dans les prochains jours, lorsqu'elle aura rendu son rapport, la mission interministérielle d'inspection chargée par le Premier ministre de cartographier les moyens budgétaires et en effectifs des ministères dédiés à l'action numérique, dont la sécurité. Enfin, nous attendons de l'ANSSI et du ministère des affaires étrangères les réponses à des questions complémentaires que nous leur avons adressées.

Ces éléments nous permettront de compléter notre analyse et de préciser ou de nuancer nos observations sur la capacité du ministère à éviter cette attaque, sur la déclaration du vol de données personnelles à la CNIL et ses conséquences, sur la communication sur l'attaque et ses conséquences, sur l'attribution de l'attaque et ses suites judiciaires, et sur le pilotage de la gestion de crise en cas de cyberattaque.

J'évoquerai tout d'abord la capacité du ministère à éviter cette attaque. Les attaquants ont profité d'une faille dans une brique logicielle utilisée pour construire cette plateforme. L'éditeur du logiciel avait identifié cette faille et livré à la DSI le correctif nécessaire, mais la mise à jour n'avait pas encore été installée. Elle nécessite en effet une programmation de

moyens, notamment en effectifs, et n'avait pas été considérée comme une absolue priorité.

De cette situation, nous tirons deux enseignements. Premièrement : quelques attaquants connaissent les failles, l'édition d'un correctif révèle plus largement l'existence de failles et suscite des appétits, plus on tarde à installer une mise à jour, plus un système d'information est vulnérable. Deuxièmement, comme d'autres ministères, le ministère des affaires étrangères dispose d'un budget dédié aux systèmes 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 créé une interface de vulnérabilité. Il consacre des moyens globalement insuffisants à la cybersécurité et concentre ceux-ci - on ne peut le lui reprocher - sur les systèmes d'information et de communication les plus stratégiques, comme la sécurité des postes et des réseaux diplomatiques.

La circulaire interministérielle de 2014 sur la politique de sécurité des systèmes d'information de l'État est appliquée de façon hétérogène, ce qui montre le caractère très limité des interventions réglementaires. Sans affectation de moyens, elle demeure un instrument de communication. De surcroît les fonctions-clés de la chaîne de sécurité - haut fonctionnaire de défense et de sécurité (HFDS) et fonctionnaire de sécurité des systèmes d'information (FSSI) - ont été exercées de façon intermittente ces derniers mois. Tout cela pose concrètement la question d'un pilotage interministériel par affectation de moyens, notamment par le respect d'un ratio obligatoire consacré à la cybersécurité. L'Anssi n'a pas aujourd'hui de telles capacités.

M. Olivier Cadic, rapporteur. - Pour ma part, j'évoquerai la déclaration du vol de données personnelles à la CNIL et ses conséquences.

L'application Ariane a fait l'objet d'une déclaration à la CNIL. La notice de l'application indique que « le service Ariane, conçu en concertation avec la CNIL, offre toutes les garanties de sécurité et de confidentialité des données personnelles » et que « les données sont effacées un mois après la date retour ». Il s'agit des données relatives aux déplacements, non des données de base du dossier, dont les données relatives aux contacts. Plus de 500 000 noms étaient stockés dans cette table depuis l'origine, semble-t-il. Cela pose au demeurant une question, qui aura quelques conséquences lors de la communication sur la cyberattaque, celle du statut des données personnelles des contacts enregistrées par leurs proches, avec ou sans leur consentement, présumé tacite.

En outre, depuis l'entrée en application du Règlement général sur la protection des données (RGPD), la compromission de données personnelles doit faire l'objet d'une déclaration à la CNIL dans les soixante-douze heures de sa détection. Cette déclaration a été faite via un formulaire en ligne dès le 7 décembre. Le ministère s'est ensuite demandé si cette attaque présentait des risques justifiant, outre son signalement, une communication aux

personnes concernées et au public. À l'issue du dialogue entre les deux parties, la DSI et la CNIL, la décision a été prise de communiquer en raison du risque d'utilisation des données pour des opérations d'hameçonnage ou d'escroquerie.

Pour autant que nous le sachions, ce dialogue est resté limité à la DSI et à la CNIL, sans appréciation externe. Nul ne s'est demandé si l'attaque visait simplement à porter atteinte à la réputation du ministère en affichant la vulnérabilité de ses applications ou n'a pris en compte le fait que les personnes concernées pouvaient découvrir leur présence dans cette base à cette occasion. Cela aurait permis, le cas échéant, d'orienter différemment la communication. La DSI expérimentait ces nouvelles obligations avec une certaine appréhension, leur non-respect pouvant entraîner des sanctions pénales. Le secrétariat général de la CNIL s'en est tenu à une vision juridique et factuelle, sur la base des seuls éléments transmis par la DSI.

J'évoquerai maintenant la communication sur l'attaque et ses conséquences.

Le 13 décembre, un courriel a été adressé aux personnes concernées, dont nous n'avons pas pu prendre connaissance à ce stade. Nous savons par l'Anssi et par la CNIL, qui ont reçu, dans la foulée, des dizaines de demandes d'information, que ce courriel a eu pour effet d'inquiéter nombre de destinataires. Soit ces deniers n'étaient pas informés de leur présence dans ce fichier, soit ils n'avaient aucune idée des données qu'il contenait. Ces personnes pensaient avoir reçu un message falsifié du ministère et être victimes d'une opération d'hameçonnage ou craignaient que leurs données bancaires ou d'autres données personnelles aient pu avoir été altérées. À mes yeux, cela constitue un début de trouble à l'ordre public. À échelle réduite, les personnes contactées ont pu être rassurées, mais personne, dans les organisations concernées, n'avait envisagé un retour de cette nature et n'y était préparé, en particulier l'Anssi, qui n'a été informée de la communication que lorsqu'elle a été confrontée à ces appels.

Le communiqué de presse a été repris par les médias, parfois de façon alarmiste, et complété sur le site du ministère par une foire aux questions. On notera que deux communiqués successifs ont été publiés, le premier mentionnant l'Anssi sans son consentement et sans qu'elle ait été associée à la mise en place des correctifs et à la préparation de cette communication, le second ne la mentionnant plus.

Ce communiqué a été mis au point par le service de la communication du ministère à partir d'éléments techniques fournis la DSI. À notre connaissance, le Centre de crise et de soutien, responsable du traitement, n'y a pas été associé. Compte tenu de l'effet de cette communication, il y a lieu de s'interroger sur un élargissement du nombre de parties impliquées dans la décision de communiquer et dans l'élaboration du contenu la communication. Enfin, nous nous interrogeons également sur

l'intérêt de relativiser les faits en indiquant que la cyberattaque n'a rien d'un événement exceptionnel, que « le ministère fait l'objet d'attaques de toutes natures et de toutes origines et s'est organisé en conséquence avec l'aide de ses partenaires interministériels, notamment l'Anssi», et ce au moment où il affiche la vulnérabilité de l'une de ses plateformes.

J'évoquerai ensuite l'attribution de l'attaque et ses suites judiciaires.

Le communiqué du 13 décembre indique que le ministère a déposé une plainte auprès du Procureur. Cela est tout à fait souhaitable. Même si l'attaque ne se traduit pas par un dommage matériel pour le ministère, elle a porté atteinte à sa réputation. Il faut d'ailleurs féliciter le ministère de cette décision, qui reste exceptionnelle au sein des administrations, lesquelles sont régulièrement victimes de cyberattaques. La puissance publique incite pourtant les entreprises à porter plainte. En outre, il s'agit d'infractions, de délits, voire de crimes, dont la commission doit être portée à la connaissance de la justice, conformément à l'article 40 du code de procédure pénale, sous peine de sanctions pénales.

Nous avons donc souhaité, dans le strict respect de l'indépendance et des compétences de l'autorité judiciaire, comprendre comment fonctionnait ce que la Revue stratégique de cyberdéfense de février 2018 appelle la chaîne « investigation judiciaire » et comment s'articulait la mise en œuvre de cette chaîne lorsque des attaques portent contre des administrations de l'État. Nous avons reçu la section spécialisée du parquet de Paris créée en 2014 et dotée d'une compétence concurrente nationale depuis 2016, laquelle reçoit entre 2 000 et 2 500 plaintes par an. Elle est en mesure de déclencher des procédures d'entraide internationale et jouit d'une solide réputation puisqu'elle coordonne à l'échelon européen l'enquête sur la cyberattaque Notpetya et un service de police, en l'occurrence la DGSI, qui peut être actionné pour constater les faits, rechercher des preuves et les auteurs.

De ces entretiens, il ressort une absence de concertation et de procédure formalisée. Le Parquet a été informé le 14 décembre par la presse, à la suite de la publication du communiqué du 13, lequel indiquait la saisine du Procureur. En réalité, la plainte ne sera déposée au Parquet que le 7 janvier, soit un mois après la détection de l'attaque. La DGSI sera officiellement saisie le 10. Cela montre que personne ne savait quelle conduite tenir et n'était préparé à ce qui devrait être un réflexe ordinaire. Même si les données relatives à l'attaque ont pu être conservées sans être altérées, on imagine qu'une intervention dans les premières heures peut avoir un intérêt : pour recueillir des preuves ou des traces susceptibles d'être effacées progressivement, comme nous l'ont confirmé les magistrats du Parquet, ou pour vérifier si les données font l'objet d'un commerce sur le Darknet.

Sans doute la mise en place du RGPD permettra-t-elle d'avancer grâce à l'obligation de déclaration et de publicité, mais un travail d'information et de coordination semble nécessaire auprès des décideurs des administrations de l'État.

J'en viens au pilotage de la gestion de crise en cas de cyberattaque. Nous voyons bien, à l'examen de ce dossier, que les administrations, à l'exception de l'Anssi, ne sont guère préparées, qu'elles hésitent à chaque étape sur la conduite à tenir parce qu'elles n'ont pas expérimenté les difficultés, parce que les précédents sont peu nombreux et parce qu'elles n'ont pas anticipé de scénarios de crise.

Une réflexion au sein des ministères et à l'échelon interministériel, impliquant l'Anssi, doit être engagée sur la gestion de crise : qui sont les acteurs internes et externes concernés ? Quels sont les niveaux de décisions adéquats ? Qui pilote ? Selon quelles procédures ? Comment communiquer et à quel moment pour ne pas ajouter une crise à la crise ? Beaucoup de choses restent à construire et à éprouver sous forme d'exercices. Il existe des plans à l'échelle interministérielle en cas d'attaques du haut du spectre pilotés par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), mais les ministères restent démunis face à des attaques de moyenne ampleur.

Telles sont nos premières conclusions, à la fois alarmistes et réalistes. Elles doivent contribuer à la prise de conscience des risques et de leur caractère multiforme. En déroulant modestement le fil d'Ariane, nous mettons en évidence le sous-investissement de nos administrions publiques en matière de cybersécurité et nous lançons, comme Guillaume Poupard récemment, un cri d'alarme sur les conséquences que pourraient avoir des attaques massives contre nos administrations. Un redressement est nécessaire. Ce dossier doit être porté au plus haut niveau de l'État. Le Premier ministre a lancé plusieurs missions à cet égard, que nous allons suivre avec attention.

En attendant, nous souhaitons poursuivre cette mission, en y associant naturellement les rapporteurs du programme 105, afin de compléter la documentation du dossier Ariane et de vérifier les efforts entrepris pour la sécurité de l'ensemble des systèmes d'information du ministère des affaires étrangères. Nous solliciterons des entretiens aux niveaux appropriés du ministère des affaires étrangères et du SGDSN pour partager ce retour d'expérience, inciter les services de l'État à progresser et à mieux se prémunir contre les attaques et leurs conséquences.

M. Cédric Perrin, président. - Pour information, je viens de vous envoyer le communiqué du ministère des affaires étrangères que vous n'aviez pas reçu.

M. Jacques Le Nay. - Pensez-vous qu'une plateforme de coopération européenne soit aujourd'hui essentielle pour lutter contre les cyberattaques ?

Estimez-vous pertinent l'appel du Parlement européen à renforcer la coopération entre l'Union européenne et l'OTAN afin de prévenir, de détecter et de dissuader les cyberattaques ?

M. Jean-Marie Bockel. - Votre travail est de très bonne facture. Il rencontrera forcément un certain écho auprès des administrations et des politiques. Il faut toutefois qu'il soit bien clair pour l'extérieur que tant le Secrétariat général que l'ANSSI, s'ils ont des marges de progression, font leur travail, n'hésitant pas à signaler leurs problèmes et leurs besoins complémentaires. Le problème, c'est le niveau administrativo-politique, les administrations ayant une vieille culture et préférant vivre cachées. Or il faut qu'elles apprennent à se protéger, car c'est une preuve de force. Quant au niveau politique, il doit donner les impulsions nécessaires.

M. Ronan Le Gleut. - A-t-on des éléments sur les origines de l'attaque ? Est-elle le fait de hackers isolés ou d'une puissance étrangère ? Peut-on tirer des conclusions de la nature de cette attaque et du mode opératoire choisi ? Des enseignements ont-ils été tirés pour éviter que d'autres ministères ne soient à leur tour attaqués ?

M. Joël Guerriau. - Est-il possible de voir comment certains États se sont organisés contre les cyberattaques ? Taïwan, qui est particulièrement agressé par la Chine, a mis en place une organisation remarquable et une agence fédérale dotée de moyens. La France ne manque-t-elle pas d'une telle organisation ? Ne devons-nous pas remettre à plat notre organisation ?

M. Bernard Cazeau. - Le Bleu budgétaire ne nous permet pas de lire facilement les efforts dédiés à la cybersécurité. Les crédits budgétaires sont en nette diminution en 2019, cette baisse étant compensée dans le cadre d'un compte d'affectation spéciale (CAS). Or, on le sait, les recettes d'un CAS varient d'une année sur l'autre. Il faudra à l'avenir veiller au niveau de ces crédits.

M. Rachel Mazuir, rapporteur. - L'Europe consacre des moyens insuffisants à la cybersécurité. Il est sûr qu'une coordination européenne est nécessaire, mais la démarche reste encore timide pour l'instant.

Comme Jean-Marie Bockel, je pense que les administrations ne sont pas suffisamment sensibilisées aux cyberattaques. Or on estime à 80 millions le nombre de tentatives de fraude en Europe en 2017. Il faut en particulier veiller aux opérateurs d'importance vitale - les services d'approvisionnement en eau et en énergie, les transports.

D'après les spécialistes, la France n'est pas mal placée en matière de cybersécurité, mais elle souffre d'un manque considérable de coordination et de process permettant à chacun de savoir ce qu'il doit faire lorsqu'il découvre une cyberattaque. Les choses se font au doigt mouillé, comme on l'a vu dans le cas d'Ariane.

M. Olivier Cadic, rapporteur. - Il est nécessaire de renforcer la coopération entre l'Union européenne et l'OTAN, face à une volonté d'attaquer les démocraties, leur réputation et de faire en sorte que le peuple perde confiance dans ses élites. On parle de « hack and leak » : on attaque et on fait savoir que des données ont été volées. La question se pose donc, en cas d'attaque, de savoir s'il faut communiquer ou non. Si on communique, l'objectif des hackers est peut-être atteint.

Toutes les personnes que nous avons auditionnées ont mesuré à quel point notre retour d'informations était précieux pour elles et ont pris conscience de la nécessité de travailler ensemble.

Si nous disions quelque chose de l'attaque, de son origine, de sa nature, on communiquerait sur le sujet. Or qui doit décider de communiquer ou non ? Le politique ? Le Parlement, comme le procureur, a appris l'attaque par le communiqué de presse. Est-ce normal, sachant que, pour le peuple, les responsables, au final, ce sont les élus ? Des procédures doivent être mises en place pour permettre aux uns et aux autres de travailler ensemble. C'est l'enseignement qui a été tiré de ce qu'il s'est passé.

En matière de cybersécurité, chacun ne va pas réinventer la roue de son côté. L'organisation de Taïwan a été évoquée. Pour ma part, je citerai l'exemple d'Israël, qui a mis en place un numéro de téléphone permettant aux administrations, aux entreprises et aux particuliers de signaler une cyberattaque. Les États les plus attaqués - Taïwan, Israël et l'Estonie - sont les plus moteurs dans ce domaine.

Enfin, le budget est une problématique importante. Ce que nous aimerions, c'est que lorsqu'on investit 100 dans un logiciel, 5 soient consacrés à la cybersécurité. Le problème d'Ariane, c'est que les services n'ont pas eu le temps d'installer le correctif. On en mesure aujourd'hui les conséquences.

Notre but est non pas de pointer du doigt quelqu'un, mais de trouver ensemble des solutions et des process afin d'être plus efficaces.

La commission autorise la publication du rapport.

LISTE DES PERSONNES AUDITIONNÉES

Auditions au Sénat

19 décembre 2019

M. Guillaume Poupard, directeur général de l'agence nationale de sécurité des systèmes d'information

M. Philippe Lefort, directeur des systèmes d'information et le **Général Hubert Bonneau**, directeur de la sécurité diplomatique

23 janvier 2019

M. Guyonneau, directeur technique et le **Commissaire Olivier Berbach**, chef de division, Direction générale de la sécurité intérieure

M. Jean Lessi, Secrétaire général de la CNIL et **Mme Tiphaine Havel**, Conseillère pour les questions institutionnelles et parlementaires

5 février 2019

M. Christophe Perruaux, procureur-adjoint, et **Mme Alice Cherif**, chef de la section F1 du parquet de Paris

13 mars 2019

Réunion de retour d'expérience au ministère de l'Europe et des affaires étrangères

M. Philippe Lefort, directeur des systèmes d'information et **M. Domenico Ditaranto**, directeur adjoint, **M. Olivier Gauvin**, directeur adjoint de la communication et de la presse, **M. Yann Belot**, responsable de la communication digitale, **Mme Marion Flavier**, Cellule de crise et de soutien, **M. Rémy Prudhomme**, conseiller parlementaire du ministre

ANNEXES

(1) Chronologie

5 décembre 2018 : détection de la cyberattaque

À partir du 5 décembre : mise en œuvre des solutions de remédiation avec le concours de l'ANSSI

7 décembre 2018 : déclaration de la compromission de données personnelles à la CNIL

Entre le 7 et le 12 décembre : dialogue entre le MEAE et la CNIL sur la communication à mettre en œuvre

13 décembre 2018 : communication en direction des titulaires des adresses électroniques compromises, communiqué à la presse, information en ligne sur le site du MEAE, rédaction d'une plainte à adresser au Parquet du Tribunal de Paris

14 décembre 2018 : décision de la commission des affaires étrangères, de la défense et des forces armées du Sénat de recueillir des éléments d'information sur cette cyberattaque

19 décembre 2018 : premières auditions des rapporteurs

4 janvier 2019 : enregistrement de la plainte au Tribunal de Paris

7 janvier 2019 : arrivée de la plainte au bureau du Procureur

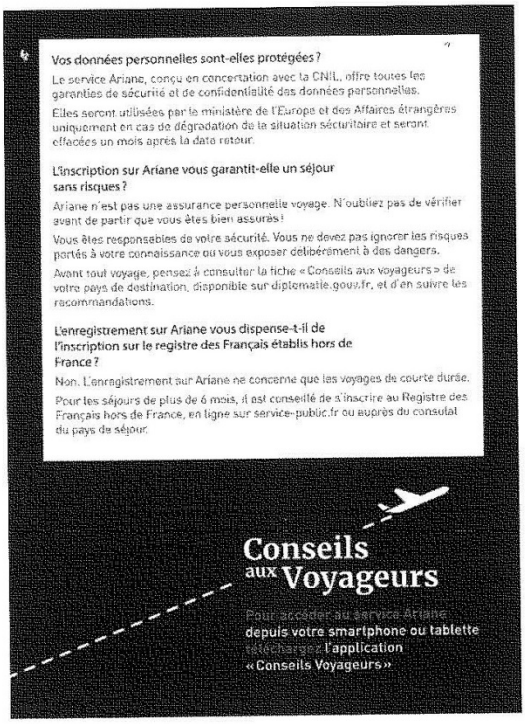
10 janvier 2019 : saisine de la DGSI

15 janvier 2019 : arrivée de la plainte à la section spécialisée du parquet et transmission du courrier de saisine officielle à la DGSI

6 février 2020 : communication des rapporteurs à la commission des affaires étrangères, de la défense et des forces armées du Sénat

13 mars 2020 : réunion de retour d'expérience avec l'administration du ministère de l'Europe et des affaires étrangères

(2) Notice de présentation de l'application Ariane



(3) Courriel adressé le 13 décembre aux personnes concernées

Début du message réexpédié :

De: mesdonnees.ariane@diplomatie.gouv.fr
Objet: Ministère de l'Europe et des Affaires Etrangères - Message aux usagers
Date: 13 décembre 2018 à 08:23:44 UTC+1
À: "fil-d-ariane.information@liste.diplomatie.gouv.fr" <fil-d-ariane.information@liste.diplomatie.gouv.fr>
Répondre à: mesdonnees.ariane@diplomatie.gouv.fr

Madame, Monsieur,

A la suite d'un piratage informatique, certaines de vos données personnelles confiées au Ministère de l'Europe et des Affaires étrangères ont été dérobées. Il s'agit :

- de votre nom et de votre prénom ;
- de votre numéro de téléphone mobile ;
- de votre adresse courriel.

Ces informations ont été renseignées par un proche ou un collègue lorsqu'il s'est inscrit sur le service Ariane. Il vous a déclaré « personne à prévenir » en cas de difficultés lors d'un voyage ou d'une mission à l'étranger.

On ne peut exclure que ces données puissent être utilisées par des tiers à des fins publicitaires (par courriels ou sms), d'hameçonnage (« phishing ») ou de tentatives d'escroquerie. Nous vous invitons à vous montrer vigilant à l'égard des messages de source douteuse, cherchant à usurper l'identité du Ministère de l'Europe et des Affaires étrangères ou d'un proche en déplacement ou en mission à l'étranger et qui vous inviteraient à préciser des informations personnelles ou des données d'identification, à ouvrir une pièce jointe ou encore à cliquer sur un lien vers un site internet.

Des conseils plus précis sur la protection sur internet sont disponibles sur les sites de la Commission Nationale sur l'Informatique et les Libertés (https://www.cnil.fr) et de l'Agence Nationale pour la Sécurité des Systèmes d'Information (https://www.ssi.gouv.fr).

Nous avons engagé tous les efforts nécessaires pour éviter que cet incident ne puisse se reproduire. Le Ministère de l'Europe et des Affaires étrangères a informé la CNIL et a saisi la justice.

Si vous avez des questions concernant cet incident, vous pouvez également nous contacter à mesdonnees.ariane@diplomatie.gouv.fr

Le Ministère de l'Europe et des Affaires étrangères connait l'importance de vos informations personnelles. Nous prenons la protection de vos données très au sérieux et nous regrettons de devoir vous écrire dans ces circonstances.

(4) Communiqué à la presse

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

Paris, le 13 décembre 2018

COMMUNIQUÉ DU
MINISTÈRE DE L'EUROPE
ET DES AFFAIRES ÉTRANGÈRES

Piratage de données

Le ministère de l'Europe et des affaires étrangères a mis en place depuis 2010 le service *Ariane*, permettant aux personnes prévoyant une mission ou un voyage à l'étranger de s'inscrire en ligne afin notamment de recevoir les informations relatives à la sécurité de leur déplacement.

Des données personnelles enregistrées lors de l'inscription sur la plate-forme *Ariane* ont été dérobées. Ces données pourraient donner lieu à des utilisations détournées mais limitées dans leur effet puisque les renseignements ne comprennent pas de données sensibles, financières ou susceptibles de dévoiler les destinations des voyages déclarées dans *Ariane*.

Nous avons pris immédiatement les mesures qui s'imposaient pour éviter que des événements de ce type ne se reproduisent.

Nous avons saisi la Commission nationale de l'informatique et les libertés (CNIL), ainsi que la justice des faits constatés. Des messages d'information aux personnes concernées sont également en cours d'envoi.

Le service *Ariane* reste en fonction. Ces incidents ne remettent pas en cause sa fiabilité et son utilité pour la sécurité des déplacements des Français à l'étranger.

(5) Communiqués et FAQ successifs publiés sur le site France Diplomatie

a) *13 décembre 2018*

France Diplomatie

Ariane – piratage de données : communiqué – F.A.Q (13 décembre 2018)

Sommaire

Communiqué de presse

Le ministère de l'Europe et des affaires étrangères a mis en place depuis 2010 le service Ariane, permettant aux personnes prévoyant une mission ou un voyage à l'étranger de s'inscrire en ligne afin notamment de recevoir les informations relatives à la sécurité de leur déplacement.

Des données personnelles enregistrées lors de l'inscription sur la plate-forme Ariane ont été dérobées. Ces données pourraient donner lieu à des utilisations détournées mais limitées dans leur effet puisque les renseignements ne comprennent pas de données sensibles, financières ou susceptibles de dévoiler les destinations des voyages déclarées dans Ariane.

Nous avons pris immédiatement les mesures qui s'imposaient pour éviter que des événements de ce type ne se reproduisent.

Nous avons saisi la Commission nationale de l'informatique et les libertés (CNIL), ainsi que la justice des faits constatés. Des messages d'information aux personnes concernées sont également en cours d'envoi.

Le service Ariane reste en fonction. Ces incidents ne remettent pas en cause sa fiabilité et son utilité pour la sécurité des déplacements des Français à l'étranger.

F.A.Q

Quand cette attaque a-t-elle été détectée ?

Le Ministère de l'Europe et des Affaires étrangères a pris connaissance de l'attaque le 5 décembre 2018.

Quelle est l'origine de cette attaque ?

Aucune attribution ne peut être effectuée à ce stade. Le ministère a déposé une plainte auprès du Procureur.

Quelles mesures ont été prises par le Ministère de l'Europe et des Affaires étrangères ?

Dès que nous avons pris connaissance de cette attaque, nous avons mis en place des mesures, sur le plan technique pour empêcher toute nouvelle intrusion de ce type. En concertation avec l'ANSSI, nous avons renforcé la sécurité de la base de données concernée par l'attaque.
Conformément aux exigences légales, le Ministère de l'Europe et des Affaires étrangères en a informé la CNIL dans les 72 heures. Nous avons ensuite lancé une procédure d'information auprès de toutes les personnes concernées.

Quelle est la nature et le volume des données personnelles compromises ?

Il s'agit d'une partie de la base de données de l'application Ariane. Cette partie de la base comprend uniquement les données des personnes déclarées comme contact en cas d'urgence par les utilisateurs d'Ariane. Les données dérobées sont : noms, prénoms, numéro de téléphone et adresse e-mail. 540 563 personnes sont concernées.
Les données des utilisateurs d'Ariane titulaires des comptes et déclarant leurs voyages ne sont pas concernées.

Pourquoi ai-je reçu un courriel d'information du Ministère de l'Europe et des Affaires étrangères ?

Vous avez été destinataire de ce courriel parce que vous étiez déclaré personne de contact à prévenir en cas d'urgence par un de vos proches titulaires d'un compte sur Ariane. A ce titre, ce proche avait enregistré des données vous concernant. Les données dérobées sont : noms, prénoms, numéro de téléphone et adresse e-mail.

Je suis titulaire d'un compte Ariane. Mes données ont-elles été dérobées ?
Non.

Est-ce que des mots de passe ont été dérobés ?
Non.

Est-ce que des dates et détails des destinations des voyages ont été dérobés ?
Non.

Est-ce que les données dérobées permettent de faire un lien entre les personnes contact et les titulaires des comptes ?
Non.

Quels sont les risques encourus par les personnes dont les données ont été dérobées ?
Ces données dérobées peuvent notamment être utilisées pour des campagnes d'hameçonnage ou d'escroquerie.

Le service Ariane est-il actuellement disponible ?
Oui. Le service est opérationnel et la sécurisation des données restaurée. Des messages en cas d'évènement pouvant affecter la sécurité de nos compatriotes à l'étranger continuent à être envoyés aux titulaires des comptes Ariane.

Cette attaque constitue-t-elle un évènement exceptionnel ?
Le Ministère de l'Europe et des Affaires étrangères fait l'objet régulièrement de cyber-attaques de toutes natures et de toutes origines et s'est organisé en conséquence avec l'aide de ses partenaires interministériels, notamment l'ANSSI.

Quelles mesures sont prises pour protéger le système informatique du ministère ?
Des mesures correctives ont été prises pour empêcher la reproduction d'une attaque selon les mêmes procédures.

Pour toute autre question, vous pouvez également nous contacter via l'adresse

: mesdonnees.ariane@diplomatie.gouv.fr (/fr/salle-de-presse/communiques-techniques/article/ariane-piratage-de-donnees-communique-f-a-g-13-12-18#mesdonnees.ariane#mc#diplomatie.gouv.fr#)

En savoir plus sur la protection sur Internet :

- Site cybermalveillance.gouv.fr (http://www.cybermalveillance.gouv.fr)
- Site de la Commission Nationale sur l'Informatique et les Libertés (https://www.cnil.fr)
- Site de l'Agence Nationale pour la Sécurité des Systèmes d'Information (https://www.ssi.gouv.fr)

b) *14 décembre 2018*

France Diplomatie

Ariane - piratage de données : communiqué - F.A.Q (13 décembre 2018)

Sommaire

Communiqué de presse

Le ministère de l'Europe et des affaires étrangères a mis en place depuis 2010 le service Ariane, permettant aux personnes prévoyant une mission ou un voyage à l'étranger de s'inscrire en ligne afin notamment de recevoir les informations relatives à la sécurité de leur déplacement.

Des données personnelles enregistrées lors de l'inscription sur la plate-forme Ariane ont été dérobées. Ces données pourraient donner lieu à des utilisations détournées mais limitées dans leur effet puisque les renseignements ne comprennent pas de données sensibles, financières ou susceptibles de dévoiler les destinations des voyages déclarées dans Ariane.

Nous avons pris immédiatement les mesures qui s'imposaient pour éviter que des événements de ce type ne se reproduisent.

Nous avons saisi la Commission nationale de l'informatique et les libertés (CNIL), ainsi que la justice des faits constatés. Des messages d'information aux personnes concernées sont également en cours d'envoi.

Le service Ariane reste en fonction. Ces incidents ne remettent pas en cause sa fiabilité et son utilité pour la sécurité des déplacements des Français à l'étranger.

F.A.Q

Quand cette attaque a-t-elle été détectée ?

Le Ministère de l'Europe et des Affaires étrangères a pris connaissance de l'attaque le 5 décembre 2018.

Quelle est l'origine de cette attaque ?

Aucune attribution ne peut être effectuée à ce stade. Le ministère a déposé une plainte auprès du Procureur.

Quelles mesures ont été prises par le Ministère de l'Europe et des Affaires étrangères ?

Dès que nous avons pris connaissance de cette attaque, nous avons mis en place des mesures, sur le plan technique pour empêcher toute nouvelle intrusion de ce type. Nous avons renforcé la sécurité de la base de données concernée par l'attaque.
Conformément aux exigences légales, le Ministère de l'Europe et des Affaires étrangères en a informé la CNIL dans les 72 heures. Nous avons ensuite lancé une procédure d'information auprès de toutes les personnes concernées.

Quelle est la nature et le volume des données personnelles compromises ?

Il s'agit d'une partie de la base de données de l'application Ariane. Cette partie de la base comprend uniquement les données des personnes déclarées comme contact en cas d'urgence par les utilisateurs d'Ariane. Les données dérobées sont : noms, prénoms, numéro de téléphone et adresse e-mail. 540 563 personnes sont concernées.
Les données des utilisateurs d'Ariane titulaires des comptes et déclarant leurs voyages ne sont pas concernées.

Pourquoi ai-je reçu un courriel d'information du Ministère de l'Europe et des Affaires étrangères ?

Vous avez été destinataire de ce courriel parce que vous étiez déclaré personne de contact à prévenir en cas d'urgence par un de vos proches titulaires d'un compte sur Ariane. A ce titre, ce proche avait enregistré des données vous concernant. Les données dérobées sont : noms, prénoms, numéro de téléphone et adresse e-mail.

Je suis titulaire d'un compte Ariane. Mes données ont-elles été dérobées ?
Non.

Est-ce que des mots de passe ont été dérobés ?
Non.

Est-ce que des dates et détails des destinations des voyages ont été dérobés ?
Non.

Est-ce que les données dérobées permettent de faire un lien entre les personnes contact et les titulaires des comptes ?
Non.

Quels sont les risques encourus par les personnes dont les données ont été dérobées ?
Ces données dérobées peuvent notamment être utilisées pour des campagnes d'hameçonnage ou d'escroquerie.

Le service Ariane est-il actuellement disponible ?
Oui. Le service est opérationnel et la sécurisation des données restaurée. Des messages en cas d'évènement pouvant affecter la sécurité de nos compatriotes à l'étranger continuent à être envoyés aux titulaires des comptes Ariane.

Cette attaque constitue-t-elle un évènement exceptionnel ?
Le Ministère de l'Europe et des Affaires étrangères fait l'objet régulièrement de cyber-attaques de toutes natures et de toutes origines et s'est organisé en conséquence avec l'aide de ses partenaires interministériels, notamment l'ANSSI.

Quelles mesures sont prises pour protéger le système informatique du ministère ?
Des mesures correctives ont été prises pour empêcher la reproduction d'une attaque selon les mêmes procédures.

Pour toute autre question, vous pouvez également nous contacter via l'adresse

: mesdonnees.ariane@diplomatie.gouv.fr (/fr/salle-de-presse/communiques-techniques/article/ariane-piratage-de-donnees-communique-f-a-q-13-12-18#mesdonnees.ariane#mc#diplomatie.gouv.fr#)

En savoir plus sur la protection sur Internet :

- Site cybermalveillance.gouv.fr (http://www.cybermalveillance.gouv.fr)
- Site de la Commission Nationale sur l'Informatique et les Libertés (https://www.cnil.fr)
- Site de l'Agence Nationale pour la Sécurité des Systèmes d'Information (https://www.ssi.gouv.fr)

c) *24 janvier 2019*

France Diplomatie

Ariane – piratage de données : communiqué – F.A.Q

Sommaire

Communiqué de presse

Le ministère de l'Europe et des affaires étrangères a mis en place depuis 2010 le service Ariane, permettant aux personnes prévoyant une mission ou un voyage à l'étranger de s'inscrire en ligne afin notamment de recevoir les informations relatives à la sécurité de leur déplacement.

Des données personnelles enregistrées lors de l'inscription sur la plate-forme Ariane ont été dérobées. Ces données pourraient donner lieu à des utilisations détournées mais limitées dans leur effet puisque les renseignements ne comprennent pas de données sensibles, financières ou susceptibles de dévoiler les destinations des voyages déclarées dans Ariane.

Nous avons pris immédiatement les mesures qui s'imposaient pour éviter que des événements de ce type ne se reproduisent.

Nous avons saisi la Commission nationale de l'informatique et les libertés (CNIL), ainsi que la justice des faits constatés. Des messages d'information aux personnes concernées sont également en cours d'envoi.

Le service Ariane reste en fonction. Ces incidents ne remettent pas en cause sa fiabilité et son utilité pour la sécurité des déplacements des Français à l'étranger.

F.A.Q

Quand cette attaque a-t-elle été détectée ?

Le Ministère de l'Europe et des Affaires étrangères a pris connaissance de l'attaque le 5 décembre 2018.

Quelle est l'origine de cette attaque ?

Aucune attribution ne peut être effectuée à ce stade. Le ministère a déposé une plainte auprès du Procureur.

Quelles mesures ont été prises par le Ministère de l'Europe et des Affaires étrangères ?

Dès que nous avons pris connaissance de cette attaque, nous avons mis en place des mesures, sur le plan technique pour empêcher toute nouvelle intrusion de ce type. Nous avons renforcé la sécurité de la base de données concernée par l'attaque.
Conformément aux exigences légales, le Ministère de l'Europe et des Affaires étrangères en a informé la CNIL dans les 72 heures. Nous avons ensuite lancé une procédure d'information auprès de toutes les personnes concernées.

Quelle est la nature et le volume des données personnelles compromises ?

Il s'agit d'une partie de la base de données de l'application Ariane. Cette partie de la base comprend uniquement les données des personnes déclarées comme contact en cas d'urgence par les utilisateurs d'Ariane. Les données dérobées sont : noms, prénoms, numéro de téléphone et adresse e-mail. 540 563 personnes sont concernées. Les données des utilisateurs d'Ariane titulaires des comptes et déclarant leurs voyages ne sont pas concernées.

Pourquoi ai-je reçu un courriel d'information du Ministère de l'Europe et des Affaires étrangères ?

Vous avez été destinataire de ce courriel parce que vous étiez déclaré personne de contact à prévenir en cas d'urgence par un de vos proches titulaires d'un compte sur Ariane. A ce titre, ce proche avait enregistré des données vous concernant. Les données dérobées sont : noms, prénoms, numéro de téléphone et adresse e-mail.

Je suis titulaire d'un compte Ariane. Mes données ont-elles été dérobées ?
Non.

Est-ce que des mots de passe ont été dérobés ?
Non.

Est-ce que des dates et détails des destinations des voyages ont été dérobés ?
Non.

Est-ce que les données dérobées permettent de faire un lien entre les personnes contact et les titulaires des comptes ?
Non.

Quels sont les risques encourus par les personnes dont les données ont été dérobées ?
Ces données dérobées peuvent notamment être utilisées pour des campagnes d'hameçonnage ou d'escroquerie.

J'ai été destinataire du message du ministère de l'Europe et des affaires étrangères concernant le vol de mes données en tant que personne de contact d'un titulaire d'un compte Ariane. Comment désormais supprimer mes données ?
Vos données (nom, prénom, numéro de téléphone et éventuellement adresse mail) en tant que personne de contact ont été renseignées par un de vos proches sur son compte utilisateur Ariane. Seul votre proche peut supprimer vos données à partir de son compte Ariane.

Je suis titulaire d'un compte Ariane. Comment puis-je supprimer mon compte ?
Un formulaire dédié à la suppression est disponible dans votre compte. Une fois l'action entreprise, toutes vos données seront immédiatement effacées.

J'ai créé un compte Ariane il y a quelques années sans m'en servir, je n'arrive plus à me reconnecter.
Après trois ans d'inactivité un compte Ariane est automatiquement supprimé et toutes les données effacées.

Combien de temps les renseignements sur mes voyages sont conservés dans mon compte Ariane ?
Les renseignements et détails concernant les voyages du titulaire d'un compte Ariane sont conservés pendant 1 mois après la date retour du voyage renseignée. Passé ce délai d' 1 mois, ils sont supprimés automatiquement.

Le service Ariane est-il actuellement disponible ?
Oui. Le service est opérationnel et la sécurisation des données restaurée. Des messages en cas d'évènement pouvant affecter la sécurité de nos compatriotes à l'étranger continuent à être envoyés aux titulaires des comptes Ariane.

Cette attaque constitue-t-elle un évènement exceptionnel ?
Le Ministère de l'Europe et des Affaires étrangères fait l'objet régulièrement de cyber-attaques de toutes natures et de toutes origines et s'est organisé en conséquence avec l'aide de ses partenaires interministériels, notamment l'ANSSI.

Quelles mesures sont prises pour protéger le système informatique du ministère ?
Des mesures correctives ont été prises pour empêcher la reproduction d'une attaque selon les mêmes procédures.

Mise à jour le 24.01.2019

En savoir plus sur la protection sur Internet :

- Site cybermalveillance.gouv.fr (http://www.cybermalveillance.gouv.fr)
- Site de la Commission Nationale sur l'Informatique et les Libertés (https://www.cnil.fr)
- Site de l'Agence Nationale pour la Sécurité des Systèmes d'Information (https://www.ssi.gouv.fr)

(6) Circulaire interministérielle de 2014

http://circulaire.legifrance.gouv.fr/pdf/2014/08/cir_38641.pdf

(7) Guide de la CNIL sur la sécurité des données personnelles.

https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles