ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Mardi
21 mai 2013
Séance de 17 heures

Compte rendu n° 72

SESSION ORDINAIRE DE **2012-2013**

Compte rendu

Commission de la défense nationale et des forces armées

Présidence de Mme Patricia Adam, *présidente*

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-sept heures.

Mme la présidente Patricia Adam. Je suis heureuse d'accueillir l'adjoint au sous-directeur de la protection économique à la Direction centrale du renseignement intérieur (DCRI), et son collaborateur, pour une présentation sur la sécurité de l'information et la cyberdéfense. Il s'agit d'un sujet majeur du Livre blanc sur la défense et la sécurité nationale, qui met l'accent sur les menaces se développant dans le cyberespace.

L'adjoint au sous-directeur de la protection économique à la direction centrale du renseignement intérieur (DCRI). Merci de votre accueil ; nous sommes très honorés de l'opportunité exceptionnelle qui nous est offerte d'intervenir devant les représentants de la nation.

Cette démarche de sensibilisation est l'un des axes majeurs de notre mission de sécurité économique. Elle fait partie d'une action globale de prévention, constituée de contacts avec les acteurs économiques, de conseil sur la sécurité des bâtiments ou des systèmes d'information, et d'enquêtes d'habilitation au secret de la défense nationale. Nous effectuons cette mission avec l'ensemble des acteurs de la politique publique d'intelligence économique, à savoir la délégation interministérielle à l'intelligence économique, mais aussi le Secrétariat général de la défense et de la sécurité nationale (SGDSN) – qui a une mission de protection du potentiel scientifique et technique de la nation – et les principaux ministères concernés, ceux chargés de l'économie, de la recherche et de l'enseignement supérieur, ainsi y compris au sein du ministère de l'Intérieur, qui a un rôle de coordination territoriale au travers de l'action des préfets de région. Notre action est relayée par nos collègues de la direction de la protection et de la sécurité de la défense (DPSD), la gendarmerie nationale et une soixantaine de conférenciers privés, formés à l'initiative de la délégation interministérielle à l'intelligence économique et de l'Institut national des hautes études de la sécurité et de la justice (INHESJ). En 2012, notre groupe de 60 conférenciers, réparti sur l'ensemble du territoire national, a réalisé 1 400 conférences pour un public de 70 000 personnes, au sein des entreprises mais aussi des laboratoires de recherche, des universités, des grandes écoles et des administrations.

Nous nous appuyons sur des cas d'incidents de sécurité réels qui nous sont communiqués par les acteurs économiques. Nous recensons ainsi un millier d'incidents de ce type par an, ce qui nous permet d'établir un état statistique de la menace par familles de risques et par pays auteurs. Cet état nous permet de constater une forte croissance du risque informatique, qui arrive au premier rang, avec 21 % des atteintes constatées dans les 150 secteurs d'activité économique que nous suivons, devant les atteintes au savoir-faire et le risque financier.

La sphère « défense-armement-sécurité » reste pour le moment particulièrement vulnérable à ce que nous appelons les « intrusions consenties », c'est-à-dire l'ensemble des cas/circonstances où une entreprise accueille des visiteurs étrangers qui provoquent des incidents de sécurité. Les intrusions consenties représentent 25 % des incidents. je pense notamment aux visites de délégations étrangères. Quant au risque informatique, il représente 17 % des atteintes constatées dans ce secteur – la majorité concerne des vols d'ordinateurs. La DCRI apporte ainsi une contribution à l'effort de l'État en matière de cyberdéfense en lien avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Nous devons faire face à un paradoxe : alors que la menace est de mieux en mieux perçue dans sa globalité, on constate un accroissement des vulnérabilités informatiques lié à des comportements individuels inadaptés. Selon le rapport de M. James Clapper, directeur du renseignement national des États-Unis et responsable de la communauté américaine du renseignement, la cybermenace constitue désormais le principal risque de sécurité, devant le terrorisme et la prolifération des armes de destruction massive.

Je vais laisser maintenant mon collaborateur, qui est un conférencier chevronné, responsable du groupe parisien de nos conférenciers, et supervise une unité qui prodigue des conseils en matière de sécurité des bâtiments et, bientôt, des systèmes d'information, vous décrire plus concrètement la nature des menaces auxquelles nous sommes confrontés.

L'officier de la DCRI expose, à l'aide de transparents, de vidéos et de captures d'écrans, divers exemples de menaces informatiques, notamment des vols d'ordinateur portable ou de smartphone*, les diverses méthodes, légales et illégales, de collecte de l'information, en particulier grâce au* social engineering *– l'ingénierie sociale –, des techniques d'intimidation pour obtenir un virement d'un service comptable, la récupération d'informations confidentielles au travers de rapports de stage figurant sur le site Internet Oodoc.com, la reproduction d'informations d'un ordinateur utilisé dans un train par le biais d'un* smartphone*, l'exploitation des données d'un disque dur de photocopieuses dont le contrat de location n'a pas prévu expressément le maintien sur place de celui-ci, les risques liés à l'utilisation de* Bluetooth*, le piratage en quelques secondes d'une clé USB ou l'exploitation des données figurant sur les réseaux sociaux.*

L'officier de la DCRI. On ne peut aborder la protection de l'information sans parler de sécurité informatique. L'avènement du numérique provoque une accélération de l'échange des informations et une explosion du stockage de données.

Cette évolution comporte de nombreux avantages, mais elle nécessite de plus en plus de temps et d'efforts pour maîtriser la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations.

Or dans tout dispositif de sécurité, on dépasse largement le cadre de l'informatique. Le centre de gravité est le facteur humain. Derrière un ordinateur, un *smartphone* ou une tablette numérique, il y a un utilisateur : le comportement individuel est le premier verrou de sécurité. Malheureusement, beaucoup n'en ont pas suffisamment conscience.

En cas de vol de *smartphone* par exemple, il est important d'avoir les réactions appropriées : essayer de le géolocaliser, tenter d'effacer les données à distance, s'abstenir d'utiliser l'appareil s'il est retrouvé et le remettre au responsable compétent qui diligentera une analyse. L'existence d'un code d'accès est évidemment un élément de protection essentiel.

La recherche d'informations recouvre trois cercles concentriques, correspondant respectivement à l'information ouverte, dite « blanche », accessible à tous, l'information sensible, dite « grise » et l'information stratégique, c'est-à-dire confidentielle et partie du processus de décision. Elle peut faire appel à des méthodes légales ou clandestines – espionnage scientifique, technique, industriel, en matière de ressources humaines, financier, commercial – et viser des cibles intermédiaires – partenaires, collaborateurs ou environnement familial. Les réseaux sociaux constituent à cet égard une mine d'informations.

Dans un milieu ouvert, la protection de l'information, même celle qui peut paraître anodine, est essentielle pour stopper les actions de pirates, d'espions ou de criminels. La méthode d'approche est banale. Au salon du Bourget, par exemple, certains membres de services de renseignement étrangers, cherchent à faire parler les gens en les abordant sur des sujets ordinaires ou leur passion pour aboutir aux sujets professionnels. Le comportement individuel est le premier verrou.

Les modes d'ingérence informatique sont multiples.

On trouve gratuitement et légalement sur Internet des *keyloggers*, c'est-à-dire des logiciels que l'on peut placer directement sur un ordinateur ou une clé USB et qui permettent de récupérer les premières frappes sur le clavier, à savoir le login ou mot de passe ou d'accès à l'appareil.

Quatre ordinateurs disparaissent toutes les heures à l'aéroport Paris-Charles-de-Gaulle, dont la moitié environ seulement est récupérée. Parmi les victimes de perte ou de vol de matériels informatiques, 56 % indiquent que ceux-ci ne comportent pas d'informations sensibles, 23 % n'en savent rien – ce qui est inadmissible s'agissant d'informations professionnelles figurant sur des appareils professionnels – et 21 % ont conscience d'en détenir. Mais pour 93 % de ceux-ci, les informations ne sont pas chiffrées. Nous espérons notamment que grâce aux conférences de sensibilisation que nous effectuons, ce taux va descendre au-dessous de 50 %. Une entreprise pharmaceutique qui avait, par exemple, chiffré tous ses outils nomades, a vu en quelques mois chuter de façon significative le nombre de vols de ses ordinateurs portables.

Plusieurs recommandations peuvent éviter ces désagréments : utiliser un film de confidentialité pour écran d'ordinateur ; privilégier un ordinateur dédié en limitant les données à ce qui est utile à la mission ; chiffrer les données ; attribuer les droits informatiques strictement nécessaires à la réalisation de la mission concernée. Ces préconisations figurent dans le « passeport conseils aux voyageurs » édité par l'ANSSI. Nous nous appuyons d'ailleurs régulièrement sur le site de cette agence, qui s'est beaucoup étoffé et propose des informations pour tout type de public.

Tout ce qui traite, stocke et transmet de l'information est vulnérable. Une clé USB de 4 gigaoctets correspond, en volume d'informations, à une pile de papier de 400 mètres de haut, et une clé de 500 gigaoctets à des dizaines de kilomètres ! Or on emploie souvent une clé USB pour différents usages, professionnels et personnels, ce qui constitue une vulnérabilité importante. Il est préférable de disposer de clés dédiées, de même qu'il convient de bien réfléchir à la façon de connecter tous les outils informatiques.

Les attaques persistantes avancées recouvrent cinq phases qui peuvent se succéder très rapidement : la reconnaissance de la cible, le piégeage ou perçage, la découverte des informations intéressant les pirates, *via* des « chevaux de Troie », notamment leur installation, puis leur extraction, qui peut durer des mois, voire des années.

Les « attaques directes » tendent à utiliser des failles par le biais de clés USB ou de courriels piégés, dotés d'un « cheval de Troie ». Pour les éviter, il faut procéder à des mises à jour régulières, au bon moment. Les « attaques point d'eau » consistent à recourir à un intermédiaire : un site Internet auquel les personnes de la structure concernée ont tendance à se connecter – celui d'un concurrent ou d'un salon professionnel par exemple. Les pirates le

compromettent avec des virus puis sollicitent les victimes, en leur faisant parvenir notamment une invitation ou une information qui peut les intéresser.

Les *smartphones*, qui étaient 24 millions en France en 2012, sont l'objet de menaces particulières. Plus ils sont présents sur le marché, plus ils sont attaqués. 45 milliards d'applications étaient téléchargées en 2012 contre 18 milliards en 2011 ! Beaucoup d'entre elles sont gratuites, leurs auteurs se payant grâce aux informations fournies par les utilisateurs. Certaines sont particulièrement intrusives, comme celle des réseaux sociaux grand public, qui peuvent entièrement aspirer un carnet d'adresses. Le but est de construire un modèle économique à des fins lucratives.

On constate que 53 % des utilisateurs de *smartphones* s'en servent quotidiennement pour des usages professionnels. Par ailleurs, il existait 8 000 virus ou logiciels malveillants destinés à ces appareils en 2012. Or la progression des attaques auxquelles ils ont donné lieu en trois ans correspond à ce qui s'est passé en quatorze ans sur les ordinateurs. Mais, à la différence de ceux-ci, les *smartphones* comportent peu d'antivirus. Pourtant, cette précaution va devenir essentielle, faute de quoi on s'exposera à des attaques dont on n'aura même pas conscience et qui sortiront des frontières nationales. On en verra les conséquences sans pouvoir en déterminer les causes.

Certaines applications, bancaires notamment, comportent des informations particulièrement intimes.

Au cours des derniers mois, des applications contenant des données personnelles ou bancaires ont été piratées, ce qui a été bien relayé par les médias. Des milliers de logins et de mots de passe ont alors été mis en ligne, mais beaucoup d'utilisateurs ne les ont probablement pas changés et sont à la merci d'actions intrusives.

Il est recommandé, pour l'utilisation des outils numériques, une gestion stricte des droits d'accès aux réseaux, une politique rigoureuse des mots de passe, l'installation d'une station de décontamination, une gestion des clés USB, avec une même application par tous, et une généralisation du chiffrement, surtout pour les outils nomades. S'agissant de l'usage des réseaux sociaux, il est recommandé de maîtriser son affichage et la diffusion d'information ou de coordonnées privées, qui sont susceptibles d'être exploités par des acteurs malveillants.

M. Philippe Folliot. Pour l'anecdote, j'ai appris il y a quelques années, que des *hackers* avaient utilisé quelque chose qui avait été mis en marge de mon site Internet pour attaquer la banque centrale du Canada.

La collaboration entre les différents services s'opère-t-elle de manière satisfaisante ou observe-t-on des cloisonnements entre eux ? Y a-t-il une forme de coordination nationale de la cybersécurité et de la cyberdéfense ?

M. Christophe Guilloteau. Il y a quelques années, lorsque j'étais assistant parlementaire, nous recevions la visite des Renseignements généraux ; maintenant, c'est l'ambassade d'Iran qui nous demande des rendez-vous !

Je rappelle qu'il y a cinq ans, l'ordinateur du groupe UMP a été piraté. Nous avons déposé une plainte mais je n'ai jamais su ce qu'elle était devenue. J'ai moi aussi fait l'objet d'attaques informatiques dans ma permanence, à la suite d'un amendement que j'avais déposé

sur la maltraitance à l'égard des animaux ; l'auteur a été identifié : il s'agissait du gardien de nuit d'une société de maintenance d'ordinateurs.

J'estime que les informations que vous venez de nous donner devraient être plus largement diffusées parmi les parlementaires : je suis convaincu que certains collègues dans cette salle se sont déjà fait piéger.

M. Jean-Jacques Candelier. La reconduction par le ministère de la Défense de l'accord cadre avec Microsoft m'inquiète : elle présenterait des risques importants de perte de souveraineté nationale, avec l'intervention de la *National Security Agency* (NSA). Qu'en pensez-vous ?

M. Lionel Tardy. S'agissant des fichiers de police, notamment concernant les empreintes digitales, le ministère de l'Intérieur nous a assuré que toutes les dispositions de cryptage avaient été prises pour assurer leur sécurité. Or on sait que le problème n'est pas tant le cryptage que l'interface entre la machine et l'utilisateur. Comment parer ce risque alors que ces fichiers tendent à devenir énormes ? Quel est plus largement votre avis sur ce point au regard notamment du travail accompli par le législateur qui, dans beaucoup de cas, semble avoir agi assez légèrement ?

L'adjoint du sous-directeur de la protection économique. Monsieur Folliot, la coordination entre les services se met en place progressivement. S'il n'y a pas d'organisme qui, à l'image du Conseil national du renseignement (CNR), opère une coordination spécifique pour la cybersécurité ou la cyberdéfense, mais l'ANSSI monte en puissance.

Pour notre part, nous travaillons en partenariat étroit avec elle : nous y avons un interlocuteur, que nous voyons toutes les semaines et avec lequel nous échangeons sur les incidents de sécurité que nous rencontrons respectivement. Notre rôle est d'en tirer des enseignements sur les vulnérabilités informatiques et de les diffuser auprès d'un large public.

On est encore loin du compte pour être parfaitement équipé en matière de cyberdéfense : nous avons peut-être pris en compte tardivement la réalité de la menace et il nous faut maintenant démultiplier les efforts pour y faire face. Je rappelle qu'aux États-Unis, cette préoccupation a été placée au premier rang.

Je ne peux vous apporter d'éléments sur l'accord-cadre avec Microsoft, la sécurité du ministère de la défense relevant avant tout de la compétence de la DPSD.

Pour répondre à monsieur Tardy, il est en effet de plus en plus difficile de sécuriser un fichier étatique. Le seul véritable moyen pour ce faire est qu'il n'ait pas d'accès vers l'extérieur, notamment à Internet. On peut également avoir une politique de droit d'accès, en hiérarchisant celui-ci selon les personnes.

Cela étant, on ne peut sécuriser complètement l'information aujourd'hui : tout se qui passe par le numérique est vulnérable à un moment où un autre.

L'officier de la DCRI. Les réseaux dédiés deviennent indispensables, car grâce à des moteurs de recherche, on peut récupérer des informations confidentielles : il suffit que l'une des personnes destinataires d'un document l'ait rerouté sur une adresse électronique

personnelle. Alors que si un cloisonnement était respecté, il n'y aurait aucune fuite d'information.

Mme la présidente Patricia Adam. Je vous remercie pour les informations que vous nous avez apportées. Je rappelle par ailleurs que le rapport d'activité de la Délégation parlementaire au renseignement comporte des recommandations dans ce domaine.

La séance est levée à dix-huit heures quarante.

*

* *

Information relative à la commission

La commission a désigné **M. Jean-Jacques Bridey**, rapporteur pour la mission d'information commune avec la commission des finances, de l'économie générale et du contrôle budgétaire, sur l'équipement des forces armées, dans le cadre de l'examen du projet de loi de règlement pour 2012.

Membres présents ou excusés

Présents. - Mme Patricia Adam, M. Olivier Audibert Troin, M. Sylvain Berrios, M. Daniel Boisserie, M. Jean-Jacques Bridey, M. Jean-Jacques Candelier, Mme Nathalie Chabanne, M. Guy Chambefort, M. Philippe Folliot, M. Jean-Pierre Fougerat, Mme Geneviève Gosselin-Fleury, Mme Edith Gueugneau, M. Christophe Guilloteau, M. Gilbert Le Bris, M. Philippe Meunier, M. Joaquim Pueyo, M. Eduardo Rihan Cypel, M. Alain Rousset, M. Jean-Michel Villaumé

Excusés. - M. Ibrahim Aboubacar, M. Claude Bartolone, M. Philippe Briand, Mme Marianne Dubois, M. Sauveur Gandolfi-Scheit, M. Éric Jalton, M. Jean-Yves Le Déaut, M. Bruno Le Roux, M. Maurice Leroy, M. Jacques Moignard, Mme Sylvie Pichot, Mme Émilienne Poumirol, M. Gwendal Rouillard, Mme Paola Zanetti

Assistait également à la réunion. - M. Lionel Tardy