ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 75915

Texte de la question

M. Pierre Morel-A-L'Huissier attire l'attention de M. le ministre de la défense sur le développement important de l'espionnage informatique. Les outils informatiques, vitaux pour nos grandes administrations, semblent de plus en plus vulnérables aux attaques Internet. Il lui demande de lui préciser s'il estime que la politique de défense française contre le cyber-espionnage est suffisamment efficace.

Texte de la réponse

Les menaces, infections et attaques informatiques se sont multipliées ces dernières années, notamment du fait de la prolifération d'outils malveillants facilement accessibles sur internet. Parallèlement, des vulnérabilités nouvelles fragilisent nos systèmes d'information avec, notamment, le besoin d'une connectivité accrue des réseaux privatifs (intranets) avec le réseau internet ou encore la banalisation et la multiplication des supports de stockage amovibles (clés USB, disques externes) qui facilitent des échanges incontrôlés entre intranets et internet et multiplient les risques d'infections et les fuites de données. La montée en puissance des menaces informatiques est très préoccupante dans la mesure où elle représente un sérieux danger pour l'ensemble des systèmes d'information, tant publics que privés. Le Livre blanc sur la défense et la sécurité nationale a d'ailleurs parfaitement identifié cette menace en faisant de la lutte contre les attaques informatiques une priorité majeure des dispositifs de sécurité nationale. Conformément aux orientations définies par le Livre blanc, une agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n 2009-834 du 7 juillet 2009, pour permettre à la France de se doter d'une véritable capacité de défense de ses systèmes d'information. Relevant du Premier ministre et placée sous la tutelle du secrétaire général de la défense et de la sécurité nationale, l'ANSSI a notamment pour mission : de détecter les attaques informatiques et de réagir rapidement, grâce à un centre opérationnel renforcé de cyberdéfense, chargé de la surveillance permanente des réseaux les plus sensibles de l'administration et de la mise en oeuvre de mécanismes de défense adaptés ; de prévenir la menace en contribuant au développement d'une offre de produits et de services de confiance pour les administrations et les acteurs économiques ; de jouer un rôle permanent de conseil et de soutien aux administrations et aux opérateurs d'importance vitale ; d'informer régulièrement les entreprises et le grand public sur les menaces et les moyens de s'en protéger, en développant une politique de communication et de sensibilisation active ; d'entretenir des liens étroits avec ses homologues étrangers ; une coopération internationale étant indispensable compte tenu de l'absence de frontières dans l'espace numérique. Pour décliner sur l'ensemble du territoire national les mesures destinées à améliorer la sécurité des systèmes d'information (SSI), le Livre blanc a prévu la création d'un observatoire zonal de la sécurité des systèmes d'information (OZSSI) au sein de chaque zone de défense. Placés sous l'autorité des préfets de zone, ces observatoires sont notamment chargés d'une mission de soutien en formation et en conseil aux administrations locales, d'animation d'un réseau largement ouvert à l'ensemble des acteurs concernés (échelons déconcentrés de l'État, collectivités territoriales, organismes ayant une mission de service public, entreprises et opérateurs privés...) et de remontée des signaux précurseurs d'incidents. Le ministère de la défense gère un nombre considérable de systèmes d'information couvrant trois domaines : les systèmes d'information opérationnels et de

communication liés à l'emploi des forces, les systèmes d'information scientifiques et techniques, et les systèmes d'information, d'administration et de gestion. La direction générale des systèmes d'information et de communication (DGSIC) du ministère de la défense, créée en mai 2006, assure le pilotage central de l'ensemble de ces systèmes pour lesquels elle définit une politique commune. Elle définit notamment les orientations générales en matière de sécurité des systèmes et en contrôle l'application. La protection contre les attaques informatiques au sein du ministère de la défense repose sur une cyber défense active alliant prévention et réaction. S'agissant des mesures de prévention, le ministère a opté pour un décloisonnement des réseaux internet-intranet, qui est assuré par des mécanismes constitués de points d'accès surveillés, sécurisés, contrôlés et dotés de filtres particuliers. Les réseaux les plus sensibles, notamment les systèmes qui concourent à l'emploi de la force, sont totalement cloisonnés. La prévention s'inscrit également dans la conception des systèmes puis dans leur exploitation. Ainsi, dès la phase projet, la sécurité est intégrée dans l'architecture des systèmes dont le niveau de sécurité est formellement validé puis se prolonge lors de leur mise en exploitation par : la sensibilisation des agents du ministère de la défense sur la vulnérabilité du réseau internet et l'interdiction de tout échange ou traitement d'information sensible par le réseau internet ; l'installation des correctifs de sécurité sur les systèmes d'exploitation et les suites logicielles de bureautique, et la mise à jour des logiciels de protection : antivirus, anti-spam et pare-feu ; la surveillance et l'analyse en temps réel, par les administrateurs des systèmes d'information, des anomalies relevées par les dispositifs de sécurité informatique et, a posteriori, par l'examen des journaux d'événements. En termes d'organisation, une instruction ministérielle du 30 novembre 2008, portant code de bon usage des systèmes d'information et de communication du ministère de la défense, précise l'utilisation attendue par le ministère de ses systèmes d'information, les dispositions spécifiques à l'usage de certains médias, les attributions particulières des acteurs de la SSI et les moyens de contrôle mis en oeuvre. Par ailleurs, les agents du ministère de la défense sont périodiquement sensibilisés aux risques informatiques par la mise en ligne d'informations pertinentes sur l'intranet du ministère et dans le cadre de séances de formation dispensées par les officiers de sécurité des systèmes d'information des organismes de la Défense. Ces mesures de prévention sont évaluées régulièrement au travers d'audits, de contrôles et d'inspections menés par des équipes spécialisées du ministère de la défense. Pour ce qui concerne les mesures de réaction, l'instruction ministérielle du 26 septembre 2008 relative à la mise en oeuvre de la lutte informatique défensive au sein du ministère de la défense a mis en place une organisation permanente de veille, alerte et réponse (OPVAR). Disposant d'une connaissance et d'une vision de l'ensemble des réseaux, l'OPVAR a pour mission de prévenir et d'anticiper les crises et de détecter les activités hostiles (veille), d'analyser, hiérarchiser et notifier tout événement présentant un risque (alerte), ainsi que de déterminer et conduire les actions défensives correspondantes (réponse). Ces processus de détection et de gestion des incidents s'appuie sur : un centre d'analyse de lutte informatique défensive (CALID), qui assure la fonction de veille et réalise le volet technique des fonctions d'analyse et de réponse ; un centre opérationnel, qui décide des réponses appropriées en fonction des éléments techniques fournis par le CALID et des priorités liées aux missions. L'OPVAR entretient des liens étroits avec le centre opérationnel de l'ANSSI, ainsi qu'au plan international avec son entité homologue de l'Organisation du traité de l'Atlantique Nord (OTAN).

Données clés

Auteur : M. Pierre Morel-A-L'Huissier
Circonscription : Lozère (2e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 75915
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Défense
Ministère attributaire : Défense

Date(s) clée(s)

Question publiée le : 6 avril 2010, page 3809
Réponse publiée le : 15 juin 2010, page 6615