ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 53067

Texte de la question

M. Thierry Lazaro attire l'attention de M. le secrétaire d'État à la défense et aux anciens combattants sur la multiplication des virus informatiques dont la conception relève de plus en plus du domaine de la cybercriminalité. De nombreux pays se sont déjà penchés sur les conséquences dramatiques qui pourraient résulter d'une attaque menée par des cyberterroristes contre les systèmes informatiques de leurs administrations. Aussi, il lui demande de bien vouloir lui faire part des réflexions menées au sein de son ministère ainsi que des services et administrations qui en dépendent, et de le rassurer sur l'efficacité des parades mises en oeuvre en la matière, de façon à éviter que les systèmes informatiques concernés ne puissent être détruits, ou que des données confidentielles ne puissent être transmises à ces cyberterroristes.

Texte de la réponse

La montée en puissance de la cybercriminalité est très préoccupante dans la mesure où elle représente une menace sérieuse 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 de la tutelle du secrétaire général de la défense nationale, l'ANSSI a notamment pour missions de détecter les attaques informatiques et de réagir rapidement, grâce à un centre opérationnel renforcé de cyber-défense, 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. Cinq OZSSI ont déjà été créés à ce jour, les deux derniers devant être mis en place à l'automne. 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. Afin de parer les agressions dont ses systèmes d'information pourraient faire l'objet, le ministère de la défense a mis en place une organisation permanente de veille, alerte et réponse (OPVAR) en charge de la lutte informatique défensive. 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). 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). La protection contre les attaques informatiques au sein du ministère de la défense repose également sur un ensemble de mesures organisationnelles et techniques. 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 au travers de séances de formation dispensées par les officiers de sécurité des systèmes d'information des organismes de la défense. Enfin, leur sensibilité aux mesures de prévention SSI est régulièrement évaluée au travers d'audits, de contrôles et d'inspections menés par des équipes spécialisées du ministère de la défense. Au plan technique, les mesures de protection reposent sur 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 à travers le réseau internet ; la prévention, avec 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. Enfin, le décloisonnement des réseaux internet-intranet 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.

Données clés

Auteur : M. Thierry Lazaro
Circonscription : Nord (6e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 53067
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Défense et anciens combattants
Ministère attributaire : Défense

Date(s) clée(s)

Question publiée le : 23 juin 2009, page 6021
Réponse publiée le : 18 août 2009, page 8068