ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 53061

Texte de la question

M. Thierry Lazaro attire l'attention de M. le ministre du budget, des comptes publics et de la fonction publique 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

Le ministre du budget, des comptes publics, de la fonction publique et de la réforme de l'État a pris connaissance avec intérêt de la question relative à la multiplication des virus informatiques. D'une façon générale, la sécurité des systèmes d'information (SSI) repose sur l'application de règles de comportement prudentes, d'une réglementation et de méthodes efficaces et, enfin, sur la mise en place et l'exploitation de dispositifs techniques de protection et de surveillance ; cet ensemble doit être soutenu par une organisation adaptée et une veille permanente sur les menaces et modes d'attaque. Le décret n° 2009-834 du 7 juillet 2009 a créé l'Agence nationale de la sécurité des systèmes d'information (ANSSI) placée sous l'autorité du secrétaire général de la défense nationale ; elle se substitue à la direction centrale de la SSI, en renforçant ses compétences, ses effectifs et ses moyens ; elle a notamment pour missions : de mettre au point, en concertation avec les ministères, la réglementation et les méthodes à appliquer en sécurité des systèmes d'information ; de détecter les attaques informatiques et de réagir au plus tôt, grâce à un centre opérationnel renforcé de cyberdéfense, actif 24 heures sur 24, 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 : l'agence contribuera 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. Le Livre blanc prévoit que cette agence soit relayée, sur l'ensemble du territoire national, par des observatoires zonaux de la sécurité des systèmes d'information (OZSSI), placés sous l'autorité du préfet de zone et travaillant au profit des échelons déconcentrés de l'État (en étroite liaison avec les ministères concernés), les collectivités territoriales, les organismes ayant une mission de service public, les entreprises et opérateurs privés, etc. Cinq observatoires zonaux ont été créés avant l'été 2009, les deux derniers étant prévus à l'automne. Ils ont déjà commencé à animer un réseau largement ouvert à l'ensemble des acteurs concernés. Le décret n° 2007-207 du 19 février 2007 charge le haut fonctionnaire de défense et de sécurité « d'animer la politique de sécurité des systèmes d'information et de

contrôler l'application de celle-ci ». Il fait appel pour cela aux compétences de l'ANSSI en tant que de besoin et s'appuiera sur un réseau de correspondants dans chacune des directions du ministère, dont il assure la coordination et à qui il apporte ses conseils et son appui pour la déclinaison de la politique de sécurité ministérielle, l'application des méthodes de l'ANSSI, la prise en compte de la sécurité dans l'architecture des systèmes, le choix des produits de sécurité (dans le respect du code des marchés publics), la sensibilisation des personnels, les audits, les enseignements des incidents éventuels, les exercices etc. Cette organisation fonctionne correctement depuis plus de neuf ans. Le niveau de sécurité des systèmes d'information du ministère apparaît donc adapté aux enjeux que constituent ces systèmes et aux menaces qui pèsent sur eux. Il est naturellement imparfait, et est donc continuellement renforcé, ne serait-ce qu'en fonction de l'évolution des menaces, sans préjudice des adaptations indispensables aux évolutions tant des systèmes eux-mêmes et des technologies utilisées que des modes de travail des agents, comme le nomadisme, qui permet par ailleurs un accroissement de leur productivité. Enfin les modifications de l'organisation, comme la création de la direction générale des finances publiques ainsi que le rattachement récent de la direction générale de l'administration et de la fonction publique, exigent également que soient repensés et adaptés l'organisation, les moyens techniques de la sécurité. Lors de la dernière attaque virale majeure, le virus Confiker qui a infecté 9 millions d'ordinateurs de par le monde début 2009, quelques dizaines d'ordinateurs du ministère seulement ont dû être décontaminés.

Données clés

Auteur : M. Thierry Lazaro
Circonscription : Nord (6e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 53061
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Budget, comptes publics et fonction publique
Ministère attributaire : Budget, comptes publics, fonction publique et réforme de l'Etat

Date(s) clée(s)

Question publiée le : 23 juin 2009, page 6006
Réponse publiée le : 15 septembre 2009, page 8763