ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 53089

Texte de la question

M. Thierry Lazaro attire l'attention de M. le haut-commissaire aux solidarités actives contre la pauvreté, haut-commissaire à la jeunesse, 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 haut-commissariat 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 lutte contre la cybercriminalité est prise en compte dans le cadre de la politique ministérielle de sécurité des systèmes d'information. Cette politique, qui va au-delà de la lutte contre la cybercriminalité, s'inscrit sans ambiguïté dans le cadre défini par le secrétariat général de la défense et de la sécurité nationale, au travers de l'Agence nationale de la sécurité des systèmes d'information (ex-direction centrale de la sécurité des systèmes d'information). Le ministère, très décentralisé, est pleinement engagé dans la démarche de modernisation de l'État en promouvant largement la simplification et la dématérialisation des échanges entre l'administration, les entreprises et le citoyen (télé déclarations, interfaces multiples avec partenaires tiers, etc.). Dans ce cadre, le ministère a identifié un certain nombre de menaces, conformément aux exigences du livre blanc sur la défense et la sécurité nationale. Afin de satisfaire à ces enjeux et face à ces menaces, un ensemble de moyens organisationnels sont mis en oeuvre : la sécurité des systèmes d'information est pilotée au travers d'une chaîne organisationnelle ayant pour point d'entrée le haut fonctionnaire de défense et de sécurité (HFDS), assisté par le fonctionnaire de sécurité des systèmes d'information. Ce dernier est en relation avec des autorités qualifiées en sécurité des systèmes d'information (AQSSI), nommées par arrêté, qui sont les directeurs d'administration centrale ou de services déconcentrés ; une politique ministérielle de sécurité des systèmes d'information a été définie et diffusée aux AQSSI afin de la décliner dans leur périmètre de responsabilité. La mise en oeuvre opérationnelle de cette politique est effectuée par une chaîne technique composée d'un responsable sécurité des systèmes d'information nationale relayée par des correspondants régionaux (un pour chaque région), nommés par l'autorité qualifiée dont ils dépendent. Un comité trimestriel se tient pour présenter aux intervenants les différentes évolutions de la politique ministérielle ; la sécurité des systèmes d'information est intégrée dans une démarche plus globale de gestion des risques et d'amélioration continue des services rendus. La sécurité des systèmes d'informations est abordée comme une réponse à des risques identifiés : si pour certains documents il existe un risque lié à leur confidentialité, la réponse en matière de sécurité des systèmes d'information peut être la mise en place d'autorisation d'accès à ces documents, la traçabilité des accès, le chiffrement, etc. ; l'amélioration continue des services rendus consiste à suivre la pertinence des mesures au travers d'indicateurs et à les ajuster en tant que de besoin. La direction centrale de la sécurité des systèmes d'information réalise de manière régulière des inspections visant à apprécier le niveau de sécurité du système

d'information, notamment par la recherche de vulnérabilités. Le rapport d'inspection remis est suivi par l'élaboration d'un plan d'actions, suivi annuellement pour la bonne exécution des solutions palliatives présentées ; pour garantir la cohérence du dispositif, un schéma directeur « sécurité des systèmes d'information » (SSI) a été élaboré autour de trois axes : premièrement, la maîtrise du patrimoine informationnel, qui correspond notamment à son identification, sa classification et ses règles ainsi qu'aux processus de gestion ; deuxièmement, le respect de la conformité légale ; et, enfin, troisièmement, la défense en profondeur, qui consiste à prendre des mesures facilitant l'anticipation des événements tels que des outils de pilotage, de surveillance, d'alerte, d'information ou de sensibilisation des personnels et de veille ; des structures de gouvernante de la sécurité des systèmes d'information ont été déployées au travers de la définition de l'organisation opérationnelle des chaînes SSI, conformément aux préconisations du livre blanc sur la défense et la sécurité nationale : tout d'abord par la mise en place d'un comité stratégique SSI, qui définit les orientations en matière de SSI et suit les actions menées intégrant le RSSI national du ministère, puis par la création de comités de pilotage sectoriels qui coordonnent la mise en oeuvre des décisions stratégiques et constituent de véritables réseaux d'échange et de mutualisation d'informations, et enfin grâce à la formalisation et l'animation des chaînes d'alertes ; des actions de sensibilisation sont réalisées avec des intervenants extérieurs (prestataires, la direction centrale du renseignement supérieur) ou des ressources internes (HFDS/fonctionnaire de sécurité des systèmes d'information) : par la publication d'une lettre mensuelle d'information, et par des formations adaptées aux différents acteurs, en lien notamment avec l'Agence nationale de sécurité des systèmes d'information ou des prestataires externes ; les déclinaisons opérationnelles sont réalisées grâce à des chartes utilisateurs, des procédures de remontées d'alertes, des tableaux de bord et des comités SSI trimestriels. Parallèlement, et ce afin de renforcer les dispositifs précités, trois typologies d'actions ont été inscrites au plan budgétaire de 2010 : un renforcement de l'architecture de sécurité ministérielle par une plus grande segmentation de nos règles d'accès, en cohérence avec l'organisation décentralisée du ministère (proxy cache, reverse proxy, anti-spam, pare-feux applicatifs, etc.) ; la mise en oeuvre d'une politique de sécurité des moyens individuels (postes de travail, téléphone mobile, sur le lieu habituel de travail mais aussi à distance) visant à rendre inaccessibles par un tiers les données professionnelles d'un utilisateur du système d'information du ministère ; l'étude de faisabilité d'un plan de continuité visant à garantir le maintien en condition opérationnelle des dispositifs techniques et applicatifs considérés comme critiques et prioritaires par le ministère pour la bonne marche des services de l'État. En conclusion, la politique de sécurité des systèmes d'information fait partie intégrante de la stratégie de mise en oeuvre, d'évolution et de maintenabilité de nos systèmes. Elle prend donc en compte au quotidien les menaces liées à la cybercriminalité en préconisant au travers des différentes instances et moyens énoncés précédemment des directives applicables stricto sensu par l'ensemble des intervenants concernés par la mise en oeuvre et l'utilisation du système d'information.

Données clés

Auteur : M. Thierry Lazaro
Circonscription : Nord (6e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 53089
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Solidarités actives contre la pauvreté et jeunesse
Ministère attributaire : Solidarités et cohésion sociale

Date(s) clée(s)

Question publiée le : 23 juin 2009, page 6079
Réponse publiée le : 20 décembre 2011, page 13381