ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 53087

Texte de la question

M. Thierry Lazaro attire l'attention de Mme la ministre de la santé et des sports 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 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 de la défense nationale, au travers de l'agence nationale de sécurité des systèmes d'information (ex-direction centrale de sécurité des systèmes d'information). Elle vise à répondre aux enjeux du ministère de la santé et des sports en la matière dont les principaux sont la continuité de l'action gouvernementale ; la protection sanitaire des populations face aux risques majeurs, aux menaces et leurs évolutions telles que les menaces NRBC ; le maintien, en toutes circonstances, du fonctionnement du système sanitaire, de solidarité et de cohésion sociale. Ce système très décentralisé est pleinement engagé dans la démarche de réforme de l'État, de simplification et dématérialisation des échanges entre l'administration et le citoyen. Ces enjeux sont d'importance car ils concernent les intérêts vitaux de nos concitoyens et les intérêts financiers des régimes sociaux, et ce au quotidien ou en période de crise. Face à ces enjeux, le ministère a identifié un certain nombre de menaces dont fait partie le cyber-terrorisme, conformément aux exigences du Livre blanc sur la défense et sécurité nationale. Afin de satisfaire à ces enjeux et face à ces menaces, un ensemble de moyens organisationnels ou techniques sont mis en oeuvre. A. Les moyens organisationnels : a) 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, de services déconcentrés ou d'agences ; b) 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 de responsables de sécurité des systèmes d'informations, nommés par l'autorité qualifiée dont ils dépendent ; c) 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 ; d) pour garantir la cohérence du dispositif, un schéma directeur « sécurité des systèmes d'information » a été élaboré autour de trois axes : la maîtrise du patrimoine informationnel, qui correspond notamment à son identification, sa classification et ses règles ainsi qu'aux processus de gestion ; le respect de la conformité légale ; 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 ; e) des structures de gouvernance de la sécurité des systèmes d'information ont été déployées au travers de la définition de l'organisation opérationnelle des chaînes SSI, intégrant les nouveaux acteurs, notamment les délégués de zone et les délégués de défense pour les opérateurs, conformément aux préconisations du Livre blanc sur la défense et la sécurité nationale ; la mise en place d'un comité stratégique SSI, qui définit les orientations en matière de SSI et suit les actions menées ; la mise en place 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 ; la formalisation et l'animation des chaînes d'alertes ; f) des actions de sensibilisation sont réalisées avec des intervenants extérieurs (prestataires, DCRI) ou des ressources internes (HFDS/fonctionnaire de sécurité des systèmes d'information) ; par la publication d'une lettre mensuelle d'information ; par des formations adaptées aux différents acteurs, en lien notamment l'agence nationale de sécurité des systèmes d'information ou des prestataires externes ; g) les déclinaisons opérationnelles sont réalisées grâce à des chartes utilisateurs (la charte du ministère est disponible uniquement sur l'intranet http ://www.intranet.sante.gouv.fr/popsid/groups/docs/ @intra/@reinet/@securite/documents/doi/doi_reinet_018930.pdf), des procédures de remontées d'alertes et des tableaux de bord. B. Au plan technique : pour renforcer les moyens déjà mis en oeuvre, trois axes d'études ont été lancés pour pouvoir agir dès l'exercice budgétaire 2010 : la maîtrise des accès logiques ; la protection des systèmes, tant sur le lieu habituel de travail qu'en situation de travail distant (par exemple, par la mise en oeuvre d'un accès par authentification forte - carte à puce - ou le chiffrement des données des postes nomades) ; la mise en place de moyens liés à la mise en oeuvre des plans de continuité. En conclusion, cette stratégie ministérielle permet de disposer d'observatoires et de noyaux durs de coordination de l'action contre la cybercriminalité constatée. Elle a déjà donné des résultats encourageants en situation réelle, notamment dans le cas du ver Confiker.

Données clés

Auteur : M. Thierry Lazaro
Circonscription : Nord (6e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 53087
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Santé et sports
Ministère attributaire : Santé et sports

Date(s) clée(s)

Question publiée le : 23 juin 2009, page 6072
Réponse publiée le : 26 janvier 2010, page 906