ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 53074

Texte de la question

M. Thierry Lazaro attire l'attention de Mme la ministre de l'enseignement supérieur et de la recherche 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 en effet très préoccupante et menace notamment les systèmes d'information tant publics que privés. Ce constat a été souligné dans plusieurs rapports adressés au Gouvernement, notamment ceux du député Pierre Lasbordes et du sénateur Roger Romani. Le Livre blanc sur la défense et la sécurité nationale : depuis, le Livre blanc sur la défense et la sécurité nationale publié le 17 juin 2008 l'a pleinement pris en compte : les attaques informatiques ont été retenues parmi les menaces principales pesant sur le territoire national ; en conséquence, la prévention et la réaction face à ces attaques sont devenues une priorité majeure des dispositifs de sécurité nationale. Le Livre blanc a ainsi fixé un plan d'action, dont la mise en oeuvre est en cours. La création d'une agence nationale : pour renforcer la cohérence et la capacité propre des moyens de l'État en matière de sécurité des systèmes d'information, à l'instar des principaux partenaires de la France, le Livre blanc prévoit la création d'une Agence nationale de la sécurité des systèmes d'information (ANSSI), relevant du Premier ministre par l'intermédiaire du secrétaire général de la défense nationale (SGDN). Le décret n° 2009-834 du 7 juillet 2009 porte création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». Elle se substitue à la direction centrale de la sécurité des systèmes d'information (DCSSI), tout en en renforçant les compétences, les effectifs et les moyens. L'Agence nationale de la sécurité des systèmes d'information a notamment pour missions : 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. La création d'observatoires zonaux de la sécurité des systèmes d'information : pour décliner sur l'ensemble du territoire national les mesures prises pour améliorer la sécurité des systèmes d'information, le Livre blanc prévoit de doter

chaque zone de défense d'un observatoire zonal de la sécurité des systèmes d'information (OZSSI), placé sous l'autorité du préfet de zone. 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 : échelons déconcentrés de l'État, collectivités territoriales, organismes ayant une mission de service public, entreprises et opérateurs privés, etc. Au-delà de la menace liée à la cybercriminalité, le ministère de l'enseignement supérieur et de la recherche a pris en compte dès le début des années 90 diverses menaces dont les sources peuvent être environnementales (météo, incendie, etc.), intrinsèques (conception, technologies, etc.), mais aussi humaines (externes, internes, délibérées, par erreur ou par négligence). À ce titre, le ministère a mis en place des mesures à la hauteur des enjeux. Les enjeux du ministère de l'enseignement supérieur et de la recherche : les incidents de sécurité sur les systèmes d'information sont de nature à détruire, altérer ou prendre connaissance des informations sensibles. Leurs impacts peuvent aller de la simple difficulté de fonctionnement d'un service durant quelques heures au vol de données à caractère personnel, à la dégradation de l'image de l'institution et de la confiance en ses télé-services, à l'atteinte au patrimoine scientifique et technique jusqu'à l'impossibilité d'assurer certaines missions essentielles. La circulation et le stockage des informations électroniques doivent être protégées pour garantir la continuité de l'activité du ministère. Les enjeux sont importants en raison : du nombre de personnes concernées : plus 2 millions d'étudiants dont plus de 10 % sont de nationalité étrangère, des salariés et individuels en formation continue, plus de 500 000 personnels enseignants, chercheurs, administratifs et techniques, travaillant dans le cadre des universités, instituts universitaires de formations des maître (IUFM), instituts nationaux, grands établissements, établissements autonomes, organismes de recherche, des fournisseurs et partenaires, des collectivités territoriales ; du partage d'infrastructures communes rendant le système de liaison complexe (réseaux haut débit nationaux, métropolitains ou régionaux, usages nomades via les environnements numériques de travail). Les solutions de protection des systèmes d'information mises en place au sein du ministère de l'enseignement supérieur et de la recherche : pour assurer la sécurité des systèmes d'information du ministère, une chaîne fonctionnelle de sécurité a été mise en place avec pour point d'entrée le haut fonctionnaire de défense et de sécurité (HFDS) du ministère, assisté d'un fonctionnaire de sécurité des systèmes d'information (FSSI). Celui-ci en lien avec la cellule réseau des universités (CRU) est relayé par un réseau des responsables de la sécurité des systèmes d'information (RSSI) tant au niveau de l'administration centrale que des établissements et organismes où le RSSI est rattaché fonctionnellement à chaque président ou directeur en qualité d'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI). Les RSSI sont au coeur du dispositif. Leurs missions principales sont les suivantes : constituer et coordonner un réseau interne de correspondants de sécurité dans les différentes composantes de leur établissement ; mettre en place les plans de sécurité adaptés aux établissements et aux services, en cohérence avec le schéma directeur de la sécurité des systèmes d'information (SDSSI) du ministère ; contrôler régulièrement le niveau de sécurité du système d'information par l'évaluation des risques résiduels ; informer et sensibiliser les utilisateurs du système d'information aux problématiques de la sécurité ; améliorer la sécurité des systèmes d'information, par une veille technologique active ainsi que par une participation aux groupes de réflexion ad hoc ; assurer la coordination avec les différents organismes concernés. La sensibilisation et la formation de tous les acteurs de l'organisation des systèmes d'information est une des conditions essentielles au bon niveau de sécurité et de confiance : le certificat informatique Internet (CII) constitue une sensibilisation de premier niveau des étudiants (licence, master, IUFM) à la notion de sécurité des systèmes d'information ; des chartes destinées à sensibiliser les étudiants et les personnels, rappelant les droits et devoirs des usagers internes et externes à l'institution ; des séminaires de sensibilisation de l'encadrement de l'administration centrale, des décideurs académiques du supérieur permet de les informer sur leurs responsabilités en matière de systèmes d'information et sur les solutions proposées pour les sécuriser tant au niveau juridique et technique qu'organisationnel ; le ministère participe aux exercices interministériels de crise afin de tester l'organisation de la protection de ses systèmes d'information, en l'occurrence dans le cadre d'un scénario d'attaque majeure sur les systèmes d'information de l'État ou d'importance pour la nation, en application du plan gouvernemental PIRANET ; dans le cadre de la récente création des observatoires zonaux de la sécurité des systèmes d'information (OZSSI), le ministère a veillé à ce que les établissements d'enseignement supérieur et de recherche et les organismes de recherche y soient représentés et apportent leur contribution, sous forme de présentations d'experts en fonction des sujets, d'échanges, de retours d'expérience, et de coopérations avec les différentes entités. Le réseau RENATER et le CERT-RENATER : RENATER, le Réseau national de télécommunications pour la technologie, l'enseignement

et la recherche, fédère depuis les années 90 les infrastructures de télécommunication pour la recherche et l'éducation sous l'impulsion des membres du GIP RENATER (grands organismes de recherche, ministère de l'enseignement supérieur et de la recherche et ministère de l'éducation nationale). Plus de 1 000 sites sont raccordés via les réseaux de collectes régionaux au réseau national RENATER qui fournit une connectivité nationale et internationale ainsi qu'un service de réponse aux incidents de sécurité : le CERT-RENATER (Computer Emergency Response Team). Ce service est essentiel pour l'ensemble de la communauté éducation et recherche à qui il fournit des informations de type bulletins de vulnérabilités, alertes, statistiques. Il est le point de contact centralisateur du traitement des incidents, son expertise apporte une aide en profondeur ainsi que la mise au point d'outils de sécurité. Son adhésion au FIRST (Forum of Incident Response and Security Team), regroupant plus de 100 CERT du monde entier, depuis les années 1990, lui permet d'avoir une visibilité et un partage d'information du niveau international.

Données clés

Auteur : M. Thierry Lazaro
Circonscription : Nord (6e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 53074
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Enseignement supérieur et recherche
Ministère attributaire : Enseignement supérieur et recherche

Date(s) clée(s)

Question publiée le : 23 juin 2009, page 6043
Réponse publiée le : 11 août 2009, page 7906