ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 53072

Texte de la question

M. Thierry Lazaro attire l'attention de M. le ministre de l'éducation nationale 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 ». Cette agence se substituera à la direction centrale de la sécurité des systèmes d'information (DCSSI), tout 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 deniers 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'éducation nationale a pris en compte dès le début des années 1990 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'éducation nationale. Les incidents de sécurité sur les systèmes d'information sont de nature à détruire, altérer, 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 à des personnes et notamment à des mineurs, 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 et de structures concernées : environ 12 millions d'élèves et apprentis dont une majorité de mineurs, un million de personnels enseignants et administratifs, 50 000 écoles, « 8 500 EPLE (collèges et lycées), 34 rectorats, 100 inspections académiques, 1 200 circonscriptions de l'éducation nationale, 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, intranet des académies très étendu, 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'éducation nationale. Conformément à la recommandation interministérielle n° 901/DISSI/SCSSI du 2 mars 1994 sur la protection des systèmes d'information traitant des informations sensibles non classifiées de défense, et avec le support de la DCSSI, 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 le service des technologies et des systèmes d'information (STSI) est relayé par un réseau des responsables de la sécurité des systèmes d'information (RSSI) tant au niveau de l'administration centrale que de l'administration déconcentrée où le RSS1 est rattaché fonctionnellement à chaque recteur d'académie en qualité d'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI). Relayés par les CTS (correspondants techniques de sécurité), les RSSI. sont au coeur du dispositif. Leurs missions principales sont les suivantes : constituer et coordonner un réseau interne de correspondants techniques de sécurité dans les rectorats (CATI), Centre académique de traitement de l'information, inspections académiques, les établissements publics locaux d'enseignement (EPLE), les autres composantes académiques) ; 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 ; organiser le référencement des sites dangereux ou illicites au niveau de l'académie et assurer la mise à jour des dispositifs de filtrage ; contrôler régulièrement le niveau de sécurité du système d'information par l'évaluation des risques résiduels et le déclenchement réguliers d'audits de sécurité ; informer et sensibiliser les utilisateurs du système d'information aux problématiques de la sécurité : mise en place de dispositifs de sensibilisations à tous les niveaux des personnels (décideurs académiques, encadrement, chefs d'EPLE, informaticiens) ; 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. La sensibilisation et la formation de tous les acteurs de l'organisation des systèmes d'information est une des conditions essentielles du bon niveau de sécurité et de confiance : le Brevet informatique Internet (B2L) constitue une sensibilisation de premier niveau des élèves (école, collège, lycée) à la notion de sécurité des systèmes d'information ; il est obligatoire pour le brevet des collèges depuis 2008 ; des chartes destinées à sensibiliser les élèves et les personnels du ministère de l'éducation nationale, rappellent 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 et des chefs d'établissements permet de les informer sur leurs responsabilité 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 services académiques 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. Les solutions techniques de sécurisation des systèmes d'information du ministère sont architecturées au niveau national au travers du réseau RACINE, vaste réseau privé virtuel (RPV ou VPN) reliant l'ensemble des implantations de façon hautement sécurisée (protocole IPSec), opéré par le ministère. Le ministère dispose également d'une infrastructure de protection à la fois périmétrique (firewall) à plusieurs niveaux sur l'ensemble des points de contact avec internet. Il dispose également de sondes IDS (intrusion detection system) et IPS (intrusion preventive system) lui permettant de superviser et de détecter toute attaque sur ses systèmes d'informations. Le ministère de l'éducation nationale autorité de certification de confiance. Le ministère de l'éducation nationale a rejoint officiellement le cercle des autorités de certification dites de confiance le 20 novembre 2008, au cours d'une cérémonie de signature de ses certificats électroniques par la direction centrale de la sécurité des systèmes d'information (DCSSI), l'autorité de certification de l'État (IGC A). Un certificat électronique est une carte d'identité numérique qui identifie de façon certaine un équipement, un télé service, une personne. Son utilisation permet de contribuer avec un très haut niveau de confiance à la sécurisation des échanges de données avec l'usager et d'autres ministères ou administrations. Cette confiance est rendue possible par une infrastructure à gestion de clés cryptographiques et un chiffrement qui garantissent l'intégrité et la confidentialité des traitements et des données. Le ministère a développé sa propre infrastructure à gestion de clé (IGC ou PKI) permettant notamment de s'affranchir autant que faire se peut, des certificats électroniques d'opérateurs commerciaux pour la plupart anglo-saxons (ces certificats sont nécessaires au cryptage SSL des échanges et à la gestion d'identité des personnes et des matériels). De multiples applications informatiques dites N-tiers sont déjà sécurisées, comme la gestion de la scolarité de l'élève (1er et second degré) ou les inscriptions aux examens et concours mais également tous les sites WEB des EPLE lorsqu'ils le souhaitent. Pole de compétences national en sécurité des systèmes d'information : au regard de la complexité des systèmes d'informations mis en oeuvre, des populations adressées, de la nécessité d'ouvrir les systèmes sur internet, des nouvelles modalités de travail, de la nature des menaces pouvant peser sur ses infrastructures et systèmes d'information, le STSI du ministère a été amené à créer un pôle de compétences national dédié à la sécurité des systèmes d'information. Pilotée par le niveau national, cette structure mutualisée a vocation à la fois, à assister les académies notamment les RSSI et les chefs de centre informatiques sur toutes les problématiques techniques de sécurité, d'audit fonctionnels ou techniques et d'assistance (notamment juridique) pour garantir aux services une sécurité optimale.

Données clés

Auteur : M. Thierry Lazaro
Circonscription : Nord (6e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 53072
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Éducation nationale
Ministère attributaire : Éducation nationale

Date(s) clée(s)

Question publiée le : 23 juin 2009, page 6038
Réponse publiée le : 15 septembre 2009, page 8826