ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 83979

Texte de la question

M. Lionel Tardy demande à Mme la ministre d'État, garde des sceaux, ministre de la justice et des libertés, de lui donner des indications sur les mesures de sécurité informatique prises dans son ministère, afin d'éviter les intrusions extérieures et les vols de données numériques. Il souhaite savoir s'il fait appel, pour ces missions, à des prestataires extérieurs, ainsi que le coût de ces prestations en 2009. Il souhaite enfin connaître les mesures qu'il entend prendre pour mettre en oeuvre les règles de sécurité du référentiel général de sécurité du 6 mai 2010.

Texte de la réponse

La question de l'intrusion dans les systèmes de données est en effet très préoccupante et menace aujourd'hui tous les systèmes d'information, tant publics que privés. S'agissant plus particulièrement de l'État, le Livre blanc sur la défense et la sécurité nationale publié le 17 juin 2008 a pleinement pris en compte la protection des systèmes d'information, puisque les attaques informatiques ont été retenues parmi les menaces principales pesant sur le territoire français. En conséquence, la prévention et la réaction face à ces attaques sont devenues une priorité majeure des dispositifs de sécurité nationale. Pour renforcer la cohérence et la capacité propre des moyens de l'État en matière de sécurité des systèmes d'information, le Livre blanc a prévu 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 et de la sécurité nationale (SGDSN). Cette agence, créée en juillet 2009, a notamment pour missions de détecter les attaques informatiques, de prévenir la menace, de jouer un rôle permanent de conseil et de soutien aux administrations et aux opérateurs d'importance vitale, et de procéder régulièrement à des inspections de sécurité. En ce qui concerne plus particulièrement les activités judiciaires, l'analyse de risque menée par les services du ministre de la justice et des libertés, ministre coordonnateur du secteur d'activités d'importance vitale (SAIV) des activités judiciaires, a clairement démontré que les systèmes d'information constituaient des éléments primordiaux pour assurer les missions d'importance vitale et qu'il était dès lors nécessaire de renforcer leur protection. Les menaces identifiées concernent les intrusions extérieures et des vols de données numériques, ainsi que les atteintes à la disponibilité des réseaux et des systèmes. La directive nationale de sécurité (DNS) qui a découlé de cette analyse, approuvée par le Premier ministre en janvier 2008, a par conséquent édicté un ensemble de principes et de règles à la fois organisationnels et techniques, propres à améliorer progressivement la sécurité des systèmes d'information. En particulier, les opérateurs d'importance vitale sont invités à intégrer la menace informatique dans l'analyse de risques conduite préalablement à la rédaction du plan de sécurité opérateur (PSO), et à désigner un responsable de la sécurité des systèmes d'information (RSSI). La DNS « activités judiciaires » a également consacré la création d'un système de management de la politique de défense et de sécurité des activités judiciaires, animé et coordonné par le haut fonctionnaire de défense et de sécurité (HFDS) en liaison avec l'ensemble des opérateurs ; dans ce cadre, un comité de suivi de la sécurité des systèmes d'information piloté par le HFDS et la sous-direction de l'informatique et des télécommunications (SDIT) effectue un examen mensuel de l'état d'avancement de l'ensemble des questions relatives à la sécurité des systèmes d'information.

Les objectifs de sécurité fixés par la DNS nécessitent, par ailleurs, la réalisation systématique d'analyses de risque (selon la méthode EBIOS, préconisée par l'ANSSI) pour tout nouveau système d'information ou pour tout système d'information existant sur lequel une importante évolution est envisagée. Ils passent également par des audits de sécurité, de façon à mesurer et corriger la vulnérabilité aux attaques des systèmes. Pour ces missions d'analyse de risque et d'audits de sécurité, le ministère de la justice et des libertés fait régulièrement appel à des prestataires extérieurs, qui font si nécessaire l'objet d'une procédure d'habilitation en fonction de la sensibilité des données auxquelles ils doivent pouvoir accéder. Afin de simplifier la passation de ces marchés sensibles et d'en contrôler la qualité, le secrétariat général du ministère a décidé en 2008 de procéder à la passation d'un accord-cadre multiattributaires, ouvert à l'ensemble des opérateurs d'importance vitale du SAIV « activités judiciaires ». Depuis sa notification, quatre prestations d'analyse de risque et deux prestations d'audit de sécurité ont ainsi été menées par l'intermédiaire de cet accord cadre, représentant un total cumulé de dépenses de 229 320 EUR (116 000 EUR payés en 2009). En complément de ces prestations externalisées, le SAIV « activités judiciaires » a aussi fait l'objet en 2009 d'une inspection par les services de l'ANSSI, qui a permis de procéder à un audit général et à six audits locaux sans coût direct pour le ministère. De plus, afin de limiter l'impact d'éventuelles intrusions extérieures, la DNS « activités judiciaires » développe également le concept de défense en profondeur au sein des systèmes d'information. Celui-ci se concrétise notamment par la mise en place d'outils de protection des postes de travail, ainsi que par le cloisonnement des infrastructures réseau, ce qui a amené le ministère à investir entre 2008 et 2010 environ 430 000 EUR pour l'achat de matériels et de logiciels directement liés à la sécurité informatique et pour les prestations d'installation associées. Ces investissements seront complétés dans les trois prochaines années par environ 1 500 000 EUR supplémentaires pour poursuivre ces travaux sur les réseaux et 2 000 000 EUR sur les postes de travail. En ce qui concerne l'application des règles introduites par le référentiel général de sécurité (RGS) du 6 mai 2010, il convient de souligner que les travaux concernant l'élaboration de ce référentiel avaient été suivis très attentivement par les services du ministère de la justice et des libertés, et que la plupart de ces règles ont donc déjà été inscrites par anticipation au sein de la DNS « activités judiciaires » et des plans de sécurité des opérateurs d'importance vitale. Il s'agit notamment des six grands principes de gestion de la sécurité des systèmes d'information, énoncés dans le RGS, et que l'on retrouve dans le système de management de la sécurité du ministère : l'adoption d'une démarche globale, l'adaptation de la SSI aux enjeux, la gestion des risques SSI, l'élaboration d'une politique de sécurité, l'utilisation de produits et de prestataires labellisés et la recherche d'une amélioration continue de la sécurité. C'est ainsi que diverses prestations concourant à la sécurisation du système d'information ont été commandées dans le cadre de marchés plus globaux, non dédiés spécifiquement à cette problématique : tierce maintenance applicative, infogérance, interconnexion de réseaux, assistance à la maîtrise d'oeuvre, etc. Il n'est cependant pas possible d'individualiser simplement parmi ces prestations les coûts associés au seul volet relatif à la sécurité, car ils ne font pas l'objet d'un décompte spécifique par les services du ministère. Enfin, il convient de signaler que le ministère de la justice et des libertés procède actuellement à la mise en place d'une infrastructure de gestion de clés (IGC) réalisée en partenariat avec la direction du projet interministériel « contrôle automatisé » (DPICA) et l'Agence nationale des titres sécurisés (ANTS), dont les certificats électroniques, qui seront émis à partir de l'automne 2010, respecteront les exigences correspondant au niveau de sécurité le plus élevé décrit dans le RGS, soit « *** » et offriront des garanties élevées sur les fonctions de sécurité au sein des systèmes d'information.

Données clés

Auteur : M. Lionel Tardy
Circonscription : Haute-Savoie (2e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 83979
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Justice et libertés (garde des sceaux)
Ministère attributaire : Justice et libertés (garde des sceaux)

Date(s) clée(s)

Question publiée le : 13 juillet 2010, page 7795

Version web : https://www.assemblee-nationale.fr/dyn/13/questions/QANR5L13QE83979

Réponse publiée le : 14 septembre 2010, page 10081