ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 83971

Texte de la question

M. Lionel Tardy demande à M. le ministre de la défense 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

Le ministère de la défense accorde la plus grande importance au traitement de la sécurité de l'information. Il participe d'ailleurs aux travaux de la direction générale de la modernisation de l'État, en particulier sur le processus de référencement des produits de sécurité éligibles pour le référentiel général de sécurité (RGS). La multiplication des attaques d'une sophistication et d'une furtivité toujours plus grandes, qui ne se concentrent plus seulement sur les systèmes du ministère mais aussi sur les personnels et les moyens utilisés en situation de mobilité, demande en effet une adaptation continue des mesures de protection. Le ministère de la défense s'emploie donc à établir un dispositif robuste destiné à surveiller et protéger l'ensemble de ses réseaux d'information, à alerter sur leur fragilité, ainsi qu'à sensibiliser en permanence ses utilisateurs. Les attaques virales de l'année 2009 ayant montré la fragilité et l'insuffisance des solutions antivirales classiques, le ministère a renforcé sa doctrine de protection contre les codes malveillants en introduisant des principes de défense en profondeur. Elle s'est traduite par la mise en place d'outils automatiques de contrôle des configurations et de déploiement des correctifs de sécurité. Les passerelles d'interconnexion des réseaux internes avec des réseaux publics, notamment l'Internet, constituent des points d'entrée d'attaques potentielles et des portes de sortie de données numériques sensibles. Ces points font l'objet de mesures particulières de prévention et de protection, tant en matière de doctrine qu'en matière de surveillance des flux. Les utilisateurs sont régulièrement informés des nouveaux risques liés aux usages des technologies de l'information, en particulier des interférences entre les domaines professionnel et privé, chacun exposant l'autre à ses risques spécifiques. Dans ce contexte, un plan de sensibilisation a été établi cette année. Il prévoit la production de supports de communication portant des messages adaptés aux différentes typologies d'utilisateurs, ainsi que l'acquisition en 2011 d'un produit d'e-learning. La direction interarmées des réseaux d'infrastructure et des systèmes d'information du ministère de la défense assure ces missions de protection des informations et de surveillance des réseaux sans recours massif à des prestataires extérieurs. Elle peut toutefois faire appel à des prestations ponctuelles d'assistance ou de réalisation dans le cadre de projets spécifiques. Ce dispositif est renforcé, au plan national, par l'action de l'agence nationale de la sécurité des systèmes d'information (ANSSI), créée par le décret no 2009-834 du 7 juillet 2009, pour permettre à la France de se doter d'une véritable capacité de défense de ses systèmes d'information. Cette vision interministérielle contribuera à déceler des attaques ciblées sur les systèmes gouvernementaux. Le centre opérationnel de 1'ANSSI propose des services de détection précoce d'attaques et d'alerte basés sur des observations continues de l'activité malveillante sur l'Internet. Le ministère de la défense met en place les équipements nécessaires aux endroits les plus exposés de son réseau afin de bénéficier de

cette surveillance. Au niveau international, le ministère de la défense a établi des accords d'échanges bilatéraux, autorisant l'échange d'informations classifiées, avec des partenaires étrangers. Une coopération avec l'Organisation du Traité de l'Atlantique Nord est en cours de formalisation. S'agissant enfin de la mise en oeuvre du référentiel général de sécurité (RGS), qui définit un ensemble de règles de sécurité s'imposant aux autorités administratives dans la sécurisation de leurs systèmes d'information, la Défense y accorde la plus grande attention dans la mesure où un certain nombre de ses procédures internes sont dématérialisées depuis déjà plusieurs années. L'infrastructure de gestion de clés (IGC), chargée de produire les éléments qui apportent la confiance dans les échanges électroniques, déjà opérationnelle, sera mise en conformité avec le RGS. Les applications informatiques migreront progressivement vers les spécifications du RGS en s'appuyant sur la carte d'identité multiservices dont il est prévu de doter les agents du ministère en 2012. En matière d'organisation, le ministère de la défense applique dès à présent les recommandations du RGS pour gérer la sécurité des systèmes d'information et adopte la démarche de prise en compte de la sécurité des systèmes d'information tout au long de leur cycle de vie, de façon systématique pour le traitement des informations classifiées de défense, progressivement pour les applications qui traitent de données sensibles.

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 : 83971
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Défense
Ministère attributaire : Défense

Date(s) clée(s)

Question publiée le : 13 juillet 2010, page 7741
Réponse publiée le : 7 septembre 2010, page 9669