ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 83972

Texte de la question

M. Lionel Tardy demande à M. le ministre d'État, ministre de l'écologie, de l'énergie, du développement durable et de la mer, en charge des technologies vertes et des négociations sur le climat, 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

L'actualité montre régulièrement que les réseaux informatiques sont utilisés illégalement pour tirer des profits, déstabiliser des entreprises, voire des autorités publiques. Le pillage d'informations industrielles, de recherche et de développement est aussi en augmentation depuis l'ouverture accrue des systèmes d'information vers l'extérieur. Le ministère de l'écologie, du développement durable, des transports et du logement (MEDDTL), et plusieurs des opérateurs relevant de son domaine sont donc à protéger. S'agissant des structures, au sein du secrétariat général, le service des politiques support et des systèmes d'information est chargé de toutes les actions opérationnelles en matière d'informatique. Le bureau chargé de la sécurité des systèmes d'information, le pôle national d'expertise en sécurité et le pôle de supervision de l'infrastructure informatique nationale concourent spécifiquement à la protection des systèmes d'information de plus, au sein du service de défense, de sécurité et d'intelligence économique (SDSIE), service du haut-fonctionnaire de défense et de sécurité, la mission de la sécurité des systèmes d'information est dirigée par le fonctionnaire de sécurité des systèmes d'information (FSSI). Le MEDDTL a ainsi renforcé les moyens humains, techniques et financiers consacrés à la protection de l'information et des systèmes d'information vitaux. S'agissant d'organisation, le ministère s'est doté en 2010 d'une politique générale de la sécurité des systèmes d'information (PGSSI). Pour son pilotage, a été créé le comité de sécurité des systèmes d'information. La PGSSI rend obligatoire pour les autorités qualifiées des systèmes d'information (AQSSI) et pour les responsables de sécurité des systèmes d'information (RSSI) : la tenue à jour dans chaque direction de l'inventaire des systèmes d'information faisant ressortir les besoins de sécurité attendus et les impacts sur les activités en cas de dysfonctionnement ; la réalisation systématique d'analyse de risque pour toute nouvelle application stratégique. L'intrusion et le vol d'information font partie intégrante de l'analyse ; la mise en oeuvre de moyens d'authentification forte (usage de certificats électroniques) et de chiffrement des données dès que l'exigence de confidentialité, d'intégrité et de traçabilité devient forte ; le traitement de toutes les alertes et situations d'urgence ; le renforcement des mesures de contrôle tant sur le plan local que national. S'agissant de l'infrastructure opérationnelle, les systèmes d'information majeurs sont hébergés sur trois sites situés à Bordeaux, Paris et Saint-Malo. Les audits réguliers établis tous les trois ans montrent le bon niveau de protection de ces centres et le professionnalisme reconnu de leurs agents. Le contrat d'hébergement du portail du MEDDTL prend en compte les résultats de l'analyse de risque et les recommandations du référentiel de l'hébergement. Enfin, s'agissant de l'information classifiée de défense, son traitement respecte les exigences des instructions générales interministérielles (IGI) spécifiques. Sur un plan

pratique, le portail sécurisé ISIS et la messagerie sécurisée MAGDA sont présents au SDSIE, au cabinet du ministre, dans les zones de défense, et équipent les principaux opérateurs (nucléaire, RATP, SNCF). L'appréciation de la menace relève de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Dès lors qu'une menace de haut niveau est mise en évidence, le FSSI diffuse l'information à l'ensemble des AQSSI et des RSSI du ministère et des opérateurs et organismes de son domaine et organise un suivi. Le MEDDTL participe aussi aux exercices annuels PIRANET organisés par le Secrétariat général de la défense et de la sécurité nationale (SGDSN). Le ministère fait appel à des prestataires extérieurs pour quatre missions : les études de risque en amont, les audits, l'infrastructure de gestion de clé (IGC) et les antivirus. S'agissant des prestataires extérieurs, depuis deux années, après un appel d'offres commun avec le ministère en charge de l'agriculture, deux sociétés ont été retenues afin d'aider les services en matière de sécurité. L'appel à leurs prestations s'effectue dans le cadre d'un marché à bons de commande. La société Solucom intervient pour toute étude en amont, notamment pour le développement de systèmes d'information. Le montant total de prestations en 2009 s'est monté à 700 000 EUR. S'agissant de protection antivirus, le produit Kaspersky couvrira l'ensemble du ministère en 2011. Les 80 000 postes du ministère sont équipés d'antivirus pour un coût de l'ordre de 100 000 EUR. Enfin, l'infrastructure de gestion de clés initiée en 2007 couvre tous les champs du ministère, la société Bull héberge le dispositif. Le montant de la prestation en 2009 s'est monté à 250 000 EUR. Le référentiel général de sécurité (RGS), créé par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, a été publié par arrêté le 6 mai 2010. Le MEDDTL s'est impliqué fortement dans le groupe de travail animé par la direction générale de la modernisation de l'État et l'ANSSI qui a préparé le RGS. Celui-ci a été diffusé aux diverses directions générales du ministère en charge des télé-procédures, ainsi qu'aux maîtrises d'oeuvre internes. Toute nouvelle télé-procédure, tout produit répondant à ces exigences seront réalisés en conformité immédiate. Les applications antérieures à la parution de cet arrêté ont trois ans pour se mettre en conformité. Les politiques de certification et les déclarations des pratiques de certification de l'infrastructure de gestion de clés du ministère ont pris en compte les versions provisoires du RGS. L'infrastructure de gestion de clés du ministère sera mise en conformité vis-à-vis de ces exigences avant le terme de trois ans.

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 : 83972
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Écologie, énergie, développement durable et mer
Ministère attributaire : Écologie, développement durable, transports et logement

Date(s) clée(s)

Question publiée le : 13 juillet 2010, page 7750
Réponse publiée le : 11 janvier 2011, page 217