ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 83981

Texte de la question

M. Lionel Tardy demande à M. le ministre du travail, de la solidarité et de la fonction publique 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 ministre du travail, de l'emploi et de la santé a pris connaissance avec intérêt de la question relative aux indications sur les mesures de sécurité informatique prises dans son ministère, afin d'éviter les intrusions extérieures et les vols de données numériques. La lutte contre les intrusions extérieures, le vol de données numériques, et plus largement contre la cybercriminalité, est prise en compte dans le cadre de la politique ministérielle de sécurité des systèmes d'information (SSI). Cette politique, qui va au-delà de la lutte contre la cybercriminalité, s'inscrit sans ambiguïté dans le cadre défini par le secrétariat général de la défense nationale, au travers de l'Agence nationale de sécurité des systèmes d'information. S'agissant du secteur santé, un plan d'action stratégique a été établi début 2009 établissant les objectifs et actions nécessaires à la maîtrise de la SSI. Ce plan fait l'objet d'une actualisation périodique, en liaison avec toutes les structures des ministères sociaux. Dans le cadre des règles de sécurité du référentiel général de sécurité du 6 mai 2010 qui servent de référence à l'action des services, le ministère chargé de la santé a ainsi réalisé des travaux de certification électronique, et engagé son rattachement à l'infrastructure de gestion de clé gouvernementale (IGC-A). La mise en oeuvre de la SSI ministérielle, assurée en interne, s'appuie sur des prestations extérieures pour la fourniture des solutions matérielles et logicielles (130 kEUR environ). Les secteurs travail et emploi sont très décentralisés et pleinement engagés dans la démarche de modernisation de l'État en promouvant largement la simplification et la dématérialisation des échanges entre l'administration, les entreprises et le citoyen (télédéclarations, interfaces multiples avec partenaires tiers, etc.). Dans ce cadre, le ministère chargé du travail, de l'emploi et de la santé a identifié un certain nombre de menaces dont font parties les intrusions extérieures et le vol de données numériques, conformément aux exigences du livre blanc sur la défense et la sécurité nationale. Afin de satisfaire à ces enjeux et face à ces menaces, un ensemble de moyens organisationnels ou techniques sont mis en oeuvre notamment afin de mettre en place les règles énoncées dans le référentiel général de sécurité précité. Au niveau de l'organisation : la SSI est pilotée au travers d'une chaîne organisationnelle ayant pour point d'entrée le haut fonctionnaire de défense et de sécurité (HFDS), assisté par le fonctionnaire de sécurité des systèmes d'information (FSSI). Ce dernier est en relation avec des autorités qualifiées en sécurité des systèmes d'information (AQSSI), nommées par arrêté, qui sont les directeurs d'administration centrale ou de services déconcentrés ; une politique ministérielle de SSI a été définie et diffusée aux AQSSI afin de la décliner dans leur périmètre de responsabilité. La mise en oeuvre opérationnelle de cette politique est effectuée par une chaîne technique composée d'un responsable national de sécurité des systèmes d'information (RSSI) relayé par des correspondants régionaux (1 pour chaque région), nommés par l'autorité qualifiée dont ils dépendent. Un comité

trimestriel se tient pour présenter aux intervenants les différentes évolutions de la politique ministérielle ; la SSI est intégrée dans une démarche plus globale de gestion des risques et d'amélioration continue des services rendus. Elle est abordée comme une réponse à des risques identifiés : si pour certains documents, il existe un risque lié à leur confidentialité, la réponse en matière de sécurité des systèmes d'information peut être la mise en place d'autorisation d'accès à ces documents, la traçabilité des accès, le chiffrement, etc. ; l'amélioration continue des services rendus consiste à suivre la pertinence des mesures au travers d'indicateurs et à les ajuster en tant que de besoin. La direction centrale de la sécurité des systèmes d'information (DCSSI) réalise de manière régulière des inspections visant à apprécier le niveau de sécurité du système d'information, notamment par la recherche de vulnérabilités. Le rapport d'inspection remis est suivi par l'élaboration d'un plan d'action, suivi annuellement pour la bonne exécution des solutions palliatives présentées ; afin de garantir la cohérence du dispositif, un schéma directeur « SSI » a été élaboré autour de trois axes : la maîtrise du patrimoine informationnel, qui correspond notamment à son identification, sa classification et ses règles ainsi qu'aux processus de gestion, le respect de la conformité légale, la défense en profondeur qui consiste à prendre des mesures facilitant l'anticipation des événements tels que des outils de pilotage, de surveillance, d'alerte, d'information ou de sensibilisation des personnels et de veille ; des structures de gouvernance de la SSI ont été déployées au travers de la définition de l'organisation opérationnelle des chaînes SSI, conformément aux préconisations du livre blanc sur la défense et la sécurité nationale précité : la mise en place d'un comité stratégique SSI, qui définit les orientations en matière de SSI et suit les actions menées intégrant le RSSI national du ministère, la mise en place de comités de pilotage sectoriels qui coordonnent la mise en oeuvre des décisions stratégiques et constituent de véritables réseaux d'échange et de mutualisation d'informations, la formalisation et l'animation des chaînes d'alertes ; des actions de sensibilisation sont réalisées, avec des intervenants extérieurs (prestataires, direction centrale du renseignement intérieur) ou des ressources internes (HFDS/FSSI) : par la publication d'une lettre mensuelle d'information, par des formations adaptées aux différents acteurs, en lien notamment avec l'Agence nationale de sécurité des systèmes d'information ou des prestataires externes (ANSSI) ; les déclinaisons opérationnelles sont réalisées grâce à des chartes utilisateurs, des procédures de remontées d'alertes, des tableaux de bord et des comités SSI trimestriels. Sur le plan technique, trois typologies d'actions destinées à renforcer les moyens déjà mis en oeuvre ont été inscrites au plan budgétaire de 2010 : un renforcement de l'architecture de sécurité par une plus grande segmentation des règles d'accès, en cohérence avec l'organisation décentralisée du ministère (proxy cache, reverse proxy, antispam, pare-feux applicatifs, etc.) ; la mise en oeuvre d'une politique de sécurité des moyens individuels (postes de travail, téléphone mobile, sur le lieu habituel de travail mais aussi à distance) visant à rendre inaccessibles par un tiers les données professionnelles d'un utilisateur du système d'information du ministère ; l'étude de faisabilité d'un plan de continuité visant à garantir le maintien en condition opérationnelle des dispositifs techniques et applicatifs considérés comme critiques et prioritaires par le ministère pour la bonne marche des services de l'État. Afin de réaliser ses missions, le ministère du travail, de l'emploi et de la santé est accompagné par une société titulaire du marché d'infogérance de son centre d'exploitation national. Ponctuellement, d'autres sociétés spécialisées peuvent intervenir lors de la mise en place de projets spécifiques. Le ministère du travail, de l'emploi et de la santé fait appel, pour ces missions, à des prestataires extérieurs pilotés par la sous-direction des systèmes d'information et plus précisément le responsable sécurité de cette dernière. Pour l'année 2009, les montants des commandes et des factures de ces prestations (achats des matériels, des logiciels et maintenance) ont été respectivement de 659 000 et 365 000 EUR. En conclusion, la prise en compte des préconisations du référentiel général de sécurité fait partie intégrante de la stratégie de mise en oeuvre, d'évolution et de maintenabilité des systèmes. Elle prend donc en compte au quotidien les menaces liées à la cybercriminalité en préconisant, au travers des différentes instances et moyens énoncés précédemment, des directives applicables stricto sensu par l'ensemble des intervenants concernés par la mise en oeuvre et l'utilisation du système 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 : 83981

Version web : https://www.assemblee-nationale.fr/dyn/13/questions/QANR5L13QE83981

Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Travail, solidarité et fonction publique
Ministère attributaire : Travail, emploi et santé

Date(s) clée(s)

Question publiée le : 13 juillet 2010, page 7820
Réponse publiée le : 1er mars 2011, page 2083