ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 83975

Texte de la question

M. Lionel Tardy demande à Mme la ministre de l'enseignement supérieur et de la recherche 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

I. Les mesures de sécurité. Les solutions de protection des systèmes d'information mises en place au sein du ministère de l'enseignement supérieur et de la recherche reposent sur le concept de défense en profondeur. Le principe repose sur l'établissement de plusieurs barrières indépendantes. La défense en profondeur vise à maîtriser l'information et le système qui la supporte par l'équilibre et la coordination de lignes de défense dynamiques ou statiques dans toute la profondeur du système d'information. 1. L'organisation de cette défense repose sur une chaîne fonctionnelle dont le point d'entrée est le haut fonctionnaire de défense et de sécurité (HFDS) commun aux ministères de l'éducation nationale et de l'enseignement supérieur et de la recherche, assisté d'un fonctionnaire de sécurité des systèmes d'information (FSSI). Celui-ci est relayé par un réseau des responsables de la sécurité des systèmes d'information (RSSI) avec le support de la cellule réseau des universités (CRU) et du CERT-RENATER (Réseau national de télécommunications pour la technologie, l'enseignement et la recherche, celui-ci fédère depuis les années 90 les infrastructures de télécommunication pour la recherche et l'éducation sous l'impulsion des membres du GIP RENATER, ses membres sont les grands organismes de recherche, le ministère de l'enseignement supérieur et de la recherche et le ministère de l'éducation nationale). Le réseau des RSSI est déployé tant au niveau de l'administration centrale que des établissements et organismes de recherche pourvus chacun d'un RSSI rattaché fonctionnellement au président d'université, au directeur d'établissement d'enseignement et de recherche, ou au directeur général d'organisme de recherche. Ces derniers ont qualité d'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI). Les missions principales des RSSI sont les suivantes : constituer et coordonner un réseau interne de correspondants de sécurité dans les différentes composantes de leur établissement ; 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 ; contrôler régulièrement le niveau de sécurité du système d'information par l'évaluation des risques résiduels ; informer et sensibiliser les utilisateurs du système d'information aux problématiques de la sécurité ; 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 concernés. 2. Pour la mise en oeuvre opérationnelle, le service des technologies et des systèmes d'information (STSI) participe à l'élaboration des grandes orientations en matière de systèmes d'information pour les ministères de l'éducation nationale et l'enseignement supérieur et de la recherche et leurs établissements associés. Le STSI conduit la mise en oeuvre opérationnelle du schéma stratégique des systèmes d'information et des télécommunications (S3IT) et du schéma directeur de la sécurité des systèmes

d'information (SDSSI). Les établissements d'enseignement supérieur et de recherche ainsi que les organismes de recherche sont libres de leur politique en matière d'exploitation de leurs systèmes d'information et réseaux ainsi qu'en matière de déploiement d'applications. Toutefois, ils peuvent bénéficier des services de l'AMUE (agence de mutualisation des universités et établissements) qui contribue à l'élaboration du système d'information des établissements et permet à ses adhérents de disposer d'une offre logicielle plurielle répondant à leur besoin. L'AMUE met à disposition de ses adhérents un cadre de cohérence technique qui récapitule les normes techniques et les recommandations de nature à faciliter l'interopérabilité et la sécurisation des applications et des services numériques. 3. La technologie mise en oeuvre. À l'administration centrale, sont mis en place plusieurs dispositifs de filtrage visant à protéger les sites web contre les attaques ciblées par exploitation de vulnérabilités tant dans les bases de données que dans les scripts des portails. Cette défense en profondeur est réalisée par l'ajout de passerelles de filtrage de type reverse proxy pare-feu applicatif (WAF - Web Application Firewall pour les personnes du domaine) en plus d'une couche dereverse proxy liée à l'authentification SSO. À l'usage, cette protection s'avère efficace, et elle fait naturellement l'objet d'amélioration constante pour renforcer cette brique fonctionnelle et en étendre le périmètre à un plus grand nombre d'applications spécifiques. Les établissements et organismes de recherche relevant du MESR sont libres de leur politique d'achat. Toutefois, ils bénéficient d'une structure dite « Groupe logiciel » en interne qui négocie globalement les prix, la distribution, l'assistance des solutions matérielles, logicielles, prestations en matière de système d'information et de leur sécurité. 4. Les contrôles La politique de sécurité et sa mise en oeuvre sont contrôlées. Le ministère a fait l'objet d'inspections dans le cadre du programme mené par le secrétariat général de la défense et de la sécurité nationale (SGDSN) à la demande du Premier ministre. Les premières inspections ont eu lieu en 2008, de nouvelles sont en cours sur 2010-2011. Elles portent sur des entités choisies pour leur caractère névralgique (cabinet ministériel, centre hébergeur de serveurs, application sensible, établissement à caractère scientifique et technologique, opérateur d'importance vitale) et donnent lieu à un rapport adressé au cabinet ministériel concerné. II. La sous-traitance. L'administration centrale commune au ministère de l'éducation nationale (MEN) et au ministère de l'enseignement supérieur et de la recherche (MESR) a mis en place un accord cadre permettant de commander des audits de sécurité pour les applications nationales et infrastructures sensibles. Des audits de sécurité ont été conduits par des sociétés spécialisées en 2009 : le budget annuel consacré est de l'ordre de 50 kEUR. Concernant l'administration centrale, il est fait appel à des prestataires uniquement pour la supervision et la maintenance des équipements de sécurité. La configuration fine est confiée aux équipes internes. III. Le règlement général de sécurité. La prise en compte de la sécurité dans les projets sensibles telle que préconisée par le règlement général de sécurité (RGS) avec étude de risques et audit de sécurité est déjà effective au sein de l'administration centrale commune aux MEN et MESR. Une infrastructure de gestion de clés (IGC Éducation), certifiée par l'ANSSI en 2008, permet de générer des certificats électroniques, véritables cartes d'identité des téléservices mis à disposition par le ministère, à destination de ses usagers ou d'autres administrations. Un accord-cadre de prestations d'études de risques, de procédures de contrôles et de réalisations d'audits techniques a été élaboré par le service des technologies et des systèmes d'information commun au MEN et MESR en 2009. Il constitue un outil d'accompagnement à la mise en oeuvre du référentiel général de sécurité (RGS) qui prévoit une procédure d'homologation de sécurité par une autorité administrative désignée par l'AQSSI au sein de chaque organisme. L'homologation consistera à attester formellement auprès des utilisateurs d'un nouveau système d'information qu'il est protégé conformément aux objectifs de sécurité fixés. Le centre de formation à la sécurité des systèmes d'information du SGDSN (CFSSI) propose un module, destiné à toutes les maîtrises d'ouvrage et maîtrises d'oeuvre ministérielles, leur permettant d'intégrer les enjeux stratégiques, juridiques et technologiques du RGS dont le décret d'application a été publié en mai 2010.

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 : 83975
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Enseignement supérieur et recherche

Version web : https://www.assemblee-nationale.fr/dyn/13/questions/QANR5L13QE83975

Ministère attributaire : Enseignement supérieur et recherche

Date(s) clée(s)

Question publiée le : 13 juillet 2010, page 7775
Réponse publiée le : 5 octobre 2010, page 10905