ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 83969

Texte de la question

M. Lionel Tardy demande à M. le ministre du budget, des comptes publics et de la réforme de l'État 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

Dans les ministères économique et financier, le haut fonctionnaire de défense et de sécurité « anime la politique de sécurité des systèmes d'information (SSI) et en contrôle l'application ». Cette politique est mise en oeuvre par la délégation aux systèmes d'information du secrétaire général, chargée de coordonner l'action des directions en matière de systèmes d'information et qui mène également des actions transversales cohérentes et structurantes et par les directions des ministères, responsables de la sécurité de leurs systèmes d'information (SI). Pour la SSI, et conformément à la réglementation, chaque directeur est assisté d'une « autorité qualifiée pour la SSI (AQSSI) ». Les AQSSI veillent à ce que : un réseau de personnes de confiance et compétentes en SSI soit déployé dans sa direction pour conseiller les autorités hiérarchiques (administration centrale et services déconcentrés) ; soient tenues à jour les listes des informations et des applications sensibles et que pour chacune soit désigné un « acteur responsable » chargé d'en déterminer la sensibilité, les niveaux de risque acceptables, les personnes (ou les fonctions) y ayant accès et avec quels droits. En outre, les AQSSI élaborent et font approuver par leur hiérarchie la politique de SSI (PSSI) de leur direction, déclinaison de la PSSI ministérielle ; elles se prononcent sur les mesures de sécurité, non techniques et techniques, proposées par les maîtrises d'ouvrages des applications pour protéger les informations sensibles et sur les risques résiduels qu'elles laissent subsister ; elles organisent l'homologation des systèmes, qu'ils entrent ou non dans le champ du référentiel général de sécurité (RGS). Enfin elles organisent la sensibilisation des personnels de leur direction. En tout état de cause, et comme le prescrivent aussi bien la réglementation et la PSSI ministérielle qui en découle, la SSI des ministères économique et financier est une préoccupation prise en compte dans les actions menées par les directions dans la construction et l'exploitation de leurs systèmes d'information. Toutefois, le renforcement de la SSI de l'ensemble de nos ministères exige également des actions transversales cohérentes et structurantes afin qu'il n'y ait pas entre les directions des niveaux de sécurité trop hétérogènes. En outre, la mutualisation de certaines mesures permet d'obtenir des économies d'échelle non négligeables. Pour atteindre ces objectifs et pour assurer l'efficacité de la démarche prévue par l'Agence nationale pour le SSI (ANSSI), les axes de travail porteront sur ces principaux chantiers : la mise en oeuvre d'une procédure adaptée aux environnements des ministères économique et financier pour l'homologation des SI ; la mise en conformité des infrastructures de gestion de clés mise en oeuvre au sein de nos ministères. Les mesures techniques de sécurité appliquées par les directions des ministères économique et financier sont à l'état de l'art : défense périmétrique (pare-feux et dispositifs de filtrage de contenu et de décontamination de la messagerie et

des accès Internet), surveillance active des tentatives d'intrusion ; surveillance des interconnexions et des flux circulant sur les réseaux internes ; défense en profondeur, notamment sur les postes de travail (antivirus ...) sécurisation des applications (études amont et audits de sécurité, tests de vulnérabilité ...), les points d'attention portant notamment sur le niveau de sensibilité des données, le contrôle d'accès aux données, la sécurisation des accès logiques et la sécurisation des accès physiques ; sensibilisation et formation des personnels (à l'aide, notamment, de modules d'autoformation en ligne). Le comportement de la plupart des agents est prudent et, comme le leur demande la PSSI, ils signalent assez spontanément, en général, les incidents qu'ils constatent. Des difficultés subsistent cependant, qui ne sont d'ailleurs pas propres aux ministères économique et financier, quand certaines catégories de personnels doivent être équipées de matériels ou de logiciels dont il n'a pas été possible de vérifier l'innocuité. Ce constat n'a pas échappé à l'ANSSI lors de l'inspection de la SSI des ministères qu'elle a conduite il y a quelques années, inspection dont les recommandations ont été appliquées. Le montant du recours aux prestataires spécialisés en SSI peut être évalué s'agissant du ministère du budget, des comptes publics et de la réforme de l'État à 7,5 MEUR environ en 2009, ces prestations portant tant sur des études et audits de sécurité que sur la conception et la réalisation des infrastructures de sécurité du ministère. Le référentiel général de sécurité (RGS) fixe les règles pour suivre une démarche globale de sécurisation de ces SI pour assurer la cohérence d'ensemble du dispositif de sécurité. Cette démarche rend obligatoires les bonnes pratiques et recommandations publiées de longue date par l'ANSSI et largement reprises dans la PSSI ministérielle ; elle prévoit : d'identifier les risques et de déterminer les besoins de SSI ; d'adapter la SSI selon les enjeux et les besoins de sécurité des ministères économique et financier afin d'y consacrer les moyens financiers et humains adaptés ; d'élaborer une politique de sécurité au niveau ministériel pour partager la vision stratégique de la SSI et la décliner pour une mise en oeuvre opérationnelle au niveau directionnel ; d'utiliser les produits et prestataires labellisés par l'ANSSI, attestant ainsi du respect des exigences du RGS ; viser une amélioration continue de la SSI permettant d'assurer l'efficacité du système de sécurité face à l'évolution des menaces. La mise en place d'un processus d'homologation est rendue obligatoire par décret et précisé dans l'arrêté RGS pour l'ensemble des SI présents au sein de l'administration. L'organisation et la mise en oeuvre de ce processus reste limitée au niveau de l'autorité administrative. Pour apporter les éclaircissements nécessaires et ainsi favoriser l'application de ces exigences dans les délais prévus par le RGS, soit le 6 mai 2011 pour les nouveaux systèmes et le 6 mai 2013 pour les systèmes existants, une réflexion est en cours pour définir une procédure d'homologation générique qui puisse s'adapter aux étapes et acteurs de l'essentiel des projets réalisés au sein des ministères économique et financier, certains systèmes exceptionnels par leur taille et leur complexité, existants, déjà partiellement en service ou encore en développement nécessiteront probablement des réflexions spécifiques. En tout état de cause, l'homologation sera systématiquement effectuée pour les nouveaux projets, à compter du 6 mai 2011. Pour le stock existant d'échanges électroniques entre administrations et avec les usagers, elle sera effectuée progressivement en respectant les contraintes calendaires fixées par le RGS pour obtenir une mise en conformité au plus tard pour le début du mois de mai 2013. La direction des SI (DSI) a mis en place dès 2001 une infrastructure de gestion de clés qui permet à toutes les directions des ministères économique et financier de pouvoir coexister dans un espace commun de confiance sans devoir définir des mesures de protection à l'égard les unes des autres. Dès aujourd'hui tous les serveurs de télé-procédures des ministères, indépendamment de leur appartenance directionnelle sont dotés de certificats qui les identifient sur Internet et qui assurent la confidentialité des transactions. L'informatique de gestion et de communication (IGC) ministérielle organise en outre un service de filialisation proposé aux directions des ministères économique et financier qui souhaitent mettre en place l'IGC pour leurs propres besoins. Les règles fixées par le RGS relatives à la mise en oeuvre des infrastructures de gestion de clés doivent permettre, pour l'essentiel : l'établissement d'un ou plusieurs niveaux de sécurité des certificats électroniques adapté aux besoins des applications utilisatrices ; l'utilisation de produits de sécurité référencés pour l'authentification des agents dans les SI mis en oeuvre ; la validation des certificats par l'État. La mise en oeuvre de la politique de référencement des produits de sécurité est d'ores et déjà engagée par la direction générale de la modernisation de l'État (DGME) en liaison avec les ministères les plus concernés, dont les ministères économique et financier, et en coordination avec l'ANSSI en charge des phases amont de qualification des produits de sécurité. Afin de répondre à l'exigence de validation des certificats par l'État, qui vise à garantir l'authenticité d'un certificat électronique issu de l'administration, l'IGC ministérielle a conduit, par anticipation, en 2008 une démarche vis-à-vis de l'IGC de l'administration (IGC-A) gérée par l'ANSSI afin d'être reconnue dans la chaîne de confiance de l'administration française, chaîne dont l'IGC-A est le point d'entrée.

Néanmoins, la validation des certificats par l'État reste partielle pour l'existant des ministères économique et financier. Certaines IGC directionnelles restant à filialiser pour être reconnues dans la chaîne de confiance de l'administration française. En amont de cette étape, et pour répondre à l'obligation de mise en oeuvre du RGS, d'autres travaux viseront à : valider les mises à jour, auprès des directions utilisatrices des certificats émis, des politiques de l'IGC ministérielle de façon à en limiter les impacts sur les applications ; programmer les évolutions des systèmes ; anticiper la qualification des IGC et le référencement des certificats d'authentification qu'elles émettent. Ces différentes tâches se poursuivront au cours des trois prochaines années.

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 : 83969
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Budget, comptes publics et réforme de l'État
Ministère attributaire : Budget, comptes publics et réforme de l'État

Date(s) clée(s)

Question publiée le : 13 juillet 2010, page 7730
Réponse publiée le : 12 octobre 2010, page 11142