Commission Commission de l'Intérieur, des Affaires générales et de la Fonction publique du Mardi 18 décembre 2012 Matin

06 Question de Mme Valérie Warzée-Caverenne au secrétaire d'État à la Fonction publique et à la Modernisation des Services publics, adjoint au ministre des Finances et du Développement durable, chargé de la Fonction publique, sur "la sécurité des systèmes informatiques des services publics fédéraux" (n° 14742)

06.01 **Valérie Warzée-Caverenne** (MR): Monsieur le président, monsieur le secrétaire d'État, cette question complètera celle posée par M. Doomst.

J'ai déjà eu l'occasion de vous interroger en commission de l'Intérieur le 3 juillet 2012 sur le virus *DNS Changer* et la politique de communication mise en place par le *Computer Emergency Response Team* (CERT) vis-à-vis du grand public, d'une part, mais aussi des services publics, d'autre part.

J'ai pris bonne note de la campagne de presse lancée à deux reprises concernant le site DNS permettant de vérifier si un ordinateur n'est pas contaminé. Cette information a été relayée par des articles auprès du grand public et, par ailleurs, on peut se réjouir que les informations nécessaires pour traiter les ordinateurs infectés par le virus restent disponibles sur le site du CERT au-delà de la date fatidique du 9 juillet 2012.

Néanmoins, je dois vous avouer que la réponse fournie en ce qui concerne les services publics fédéraux n'a pas eu le don de me rassurer sur la sécurité de leurs systèmes informatiques, loin de là!

Je vous cite: "Les SPF doivent suivre les recommandations générales de protection valables en matière de protection de leur infrastructure informatique". Sachant qu'il s'agit d'une question de sécurité, ne devrait-on pas parler de mesures à prendre et à faire appliquer plutôt que de recommandations?

En effet, j'imagine que tous les domaines couverts par vos différents départements ont leurs données sensibles et cela me rassurerait de savoir que celles-ci sont cadastrées mais aussi qu'un plan de sécurisation est décidé, mis en place et enfin évalué.

J'aurais donc aimé connaître la nature exacte de ces recommandations ou de ces mesures de sécurité. Quelles sont-elles en termes de piratage (accès à distance) ou d'accès physique (intrusion dans la salle des machines) non autorisé? Sont-elles communes à tous les SPF ou sont-elles laissées à la libre exécution des différents services ICT des différents départements?

Avez-vous la capacité d'être assuré à tout instant que tous les ordinateurs des SPF remplissent bien les conditions de sécurité de base telles que:

- anti-virus mis à jour et non désactivable,
- contrôle régulier des licences et listes de détection,
- monitoring des équipements de transmission data (routeurs, bridges)
- politique de contrôle d'accès aux données sensibles, traçage des opérations et alerte en cas de détection d'opération suspecte.

Enfin, en ce qui concerne le virus *DNS Changer* en particulier, je vous cite encore: "CERT.be enverra prochainement un courrier électronique aux responsables ICT des SPF pour les sensibiliser une fois encore à la problématique du *DNS Changer* et pour leur recommander, s'ils ne l'ont pas déjà fait, de procéder aux vérifications recommandées et, le cas échéant, au

traitement des ordinateurs infectés".

Cette réponse me donne l'impression qu'il n'y avait, avant cette question parlementaire, encore eu aucune démarche spécifique vis-à-vis des institutions gérées par Belnet et son CERT vis-à-vis de ses clients (les universités, écoles supérieures, centres de recherche et services publics belges), alors que ce risque est connu depuis longtemps.

Je voudrais savoir à quel moment les SPF ont été informés de ce danger spécifique, à quelle fréquence et par quels moyens.

06.02 **Hendrik Bogaert**, secrétaire d'État: Monsieur le président, chère collègue, il n'existe pas de mesures générales de sécurité pour la protection des systèmes d'information de l'administration fédérale. Compte tenu de l'autonomie de chaque institution et de l'hétérogénéité des systèmes informatiques au sein de l'administration, chaque organisme public fédéral est responsable de sa propre gestion ICT.

Des concertations entre les responsables des différents départements sont régulièrement organisées sur base volontaire, par exemple via un *information security management forum,* facilité par Fedict. Ce forum a rédigé un projet de règlement général sur la sécurité de l'information dans l'administration. CERT.be publie aussi des conseils en matière de piratage ou de sécurisation d'accès mais ses publications n'ont pas de caractère contraignant.

Ni Fedict ni CERT.be ne disposent d'informations leur permettant d'apprécier si les conditions de sécurité de base sont remplies pour les ordinateurs de tous les SPF. Notre pays manque d'une structure opérationnelle chargée de coordonner l'ensemble de cette problématique. C'est la raison pour laquelle une proposition de stratégie en matière de *cyber security* est actuellement en discussion au gouvernement. Je fais ici référence à la réponse que je viens de donner à un de vos collègues.

En ce qui concerne votre question sur le virus *DNS Changer* et la communication de ce danger aux SPF, je rappelle que CERT.be s'adresse tant au grand public et aux entreprises privées qu'aux clients de Belnet. CERT.be a communiqué régulièrement dès janvier lorsqu'il a été officiellement averti de l'existence de *DNS Changer* et des mesures prises par les autorités américaines. À partir de février, un outil spécifique développé par CERT.be et des mesures de monitoring du réseau Belnet ont permis de détecter les ordinateurs infectés parmi les clients de Belnet (SPF, université, etc.). Lorsqu'un ordinateur infecté était identifié, CERT.be prenait contact avec les organisations concernées en vue de leur donner des recommandations pour l'éradication du virus. Sur base des monitorings en place pour les clients de Belnet, plus aucun ordinateur infecté n'a été détecté et CERT.be a clos cet incident à la mi-juillet.

06.03 **Valérie Warzée-Caverenne** (MR): Monsieur le président, monsieur le secrétaire d'État, merci pour votre réponse. De la même façon, je vous répondrai en deux fois quant à ce virus DNS Changer. D'un côté, je suis rassurée par les mesures prises avant que je ne pose la question; d'ailleurs, il me semblait logique d'agir avant qu'une question n'intervienne.

En revanche, d'après votre réponse, formulée de manière identique à mon collègue, "sur base volontaire, conseil non contraignant": cela me fait peur. En effet, ne pourrait-on pas imposer des mesures de sécurité? La sécurité informatique touche à la sécurité nationale. Certaines informations n'ont pas à tomber entre les mains de n'importe qui.

C'est pourquoi je suggère que, dans la phase de mise en place d'une structure chargée d'assurer la sécurité informatique, vous accentuiez la protection et alliez plus loin dans des mesures contraignantes pour l'ensemble des SPF afin de leur assurer la sécurité.

06.04 **Hendrik Bogaert**, secrétaire d'État: Je vous remercie pour vos remarques. Je partage vos convictions. L'administration publique agit beaucoup sur base volontaire: on compte sur le fait qu'on prend la responsabilité de réaliser certaines activités. Dans ce cas-ci, il s'agira de mesures beaucoup plus contraignantes: il faudra obliger les départements à collaborer et à prendre leurs responsabilités.

Je transférerai votre suggestion au groupe de travail chargé actuellement de formuler les recommandations sur cette problématique.

06.05 **Valérie Warzée-Caverenne** (MR): Monsieur le président, je remercie le secrétaire d'État. Je crois que nous avons pu avancer un peu dans ce domaine de la sécurité: c'était un peu le but de mon intervention.

L'incident est clos.