Question orale en Commission de l'Intérieur du mardi 3 juillet 2012, transformée en question écrite de Madame la Députée Valérie WARZEE-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 relative au CERT et le virus informatique de type « Cheval de Troie »

Il semblerait que 4 millions d'ordinateurs au sein de plus de 100 pays ont été infectés par un virus de type « Cheval de Troie ». Le virus "DNS Changer" qui est l'oeuvre de pirates informatique estoniens, redirigeait les utilisateurs vers des copies de sites web afin de voler leurs données et de leur envoyer des publicités.

Les serveurs provisoires sur lesquels les ordinateurs infectés par le virus "DNS Changer" sont redirigés seront maintenus en activité jusqu'au 9 juillet 2012 suite à une décision d'un tribunal américain, a-t-on appris via le site du CERT (Computer Emergency Response Team). Date après laquelle les ordinateurs infectés seraient privés d'accès au net.

Compte tenu des très nombreux utilisateurs belges privés d'une part mais aussi des multiples disfonctionnements et paralysies qu'un tel virus pourrait entraîner dans nos administrations publiques d'autre part, j'aurais aimé savoir ce qui suit :

- votre département ou le CERT a-t-il mis en place un plan de communication afin de faire connaître au plus grand nombre de personne le site www.dns-ok.be permettant de vérifier si leur ordinateur n'est pas contaminé ?
- on apprend par ailleurs que ce site restera en activité jusqu'à la nouvelle date limite, qu'en est-il après celle-ci ?
- des mesures spécifiques de précautions sont-elles prévues pour les services publics ?
    - dans l'affirmative, lesquelles ?

Staatssecretaris bevoegd voor ambtenarenzaken en modernisering	

		Adviseur:
Q 11263 Warzee-Caverenne	**Kamer / Mondelinge vragen**	

1) Cert.be a organisé une campagne de presse à deux reprises afin de sensibiliser tant les particuliers que les entreprises à la problématique du virus

« DNS Changer ». Suite à ces campagnes, divers articles sont également parus dans la presse. Cert.be est également en contact avec les fournisseurs internet afin d'organiser une communication de ceux-ci vers leurs clients.

2) Au-delà de la date limite, l'outil développé pour le site www.dns-ok.be ne pourra plus détecter les PC's infectés, cette reconnaissance s'appuyant sur les informations de redirection fournies par le site contrôlé actuellement par le FBI. Les informations nécessaires pour traiter les PCs infectés resteront toutefois disponibles sur le site de cert.be (https://www.cert.be).
3) Les services publics doivent suivre les recommandations générales de protection valables en matière de protection de leur infrastructure informatiques. Cert.be enverra prochainement un courrier électronique aux responsables ICT des services publics fédéraux pour les sensibiliser une fois encore à la problématique de « 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 PCs infectés.