Datum / Date: 13/06/2016
Uur / Heure: 11:47
Vraag / Question: n° 12374

Question orale de la Députée Kattrin JADIN
à Monsieur Alexander DE CROO, Ministre de l'Agenda numérique, des Télécommunications et de la Poste,
concernant la vulnérabilité de la Belgique aux attaques informatiques
- déposée le 13 juin 2016 -

Monsieur le Ministre,

Selon une récente étude publiée par un grand groupe international de sécurité informatique, spécialisé dans la sécurisation des données sur internet et l'analyse de protection des réseaux informatiques, la Belgique serait ni plus ni moins le pays le plus vulnérable du monde aux attaques informatiques.

En effet, grâce à un outil spécifiquement développé qui lui permet de scanner en quelques heures l'ensemble des adresses IP visibles sur un réseau ainsi que le type de services offerts par ces adresses, l'entreprise a pu établir un classement des États les plus vulnérable aux cyberattaques. Et il ressort de cette étude que la Belgique dispose du réseau le plus exposé au monde. Parmi les faiblesses pointées du doigt sont visées le trop grand nombre de protocoles employés, le manque de sécurisation et de l'obsolescence de ceux-ci ou encore une quantité trop élevée de nos bases de données directement accessibles en ligne.

Monsieur le Ministre, mes questions à ce sujet sont les suivantes :

- Confirmez-vous les faiblesses pointées par l'étude en matière de sécurisation et modernité dans nos protocoles et réseaux informatiques utilisés en Belgique ?

- Dans l'affirmative, des mesures sont-elles actuellement à l'étude au sein de votre département afin de corriger cette préoccupante situation et assurer une sécurisation de optimales de nos réseaux informatiques ? Si oui, lesquelles sont-elles ?

- Disposez-vous de statistiques plus détaillées sur le nombre d'attaques et d'intrusions auxquelles les réseaux informatiques de l'État belge ont dû faire face en 2015 et 2016, la proportion d'entre elles exploitant effectivement une faille de protocole, ainsi que leurs éventuelles conséquences ?

Je vous remercie, Monsieur le Ministre, pour les réponses que vous voudrez bien m'apporter.

Kattrin JADIN

Réponse:

Question 1

Les ports que l'étude a testé ne doivent pas être ouverts chez un utilisateur final au trafic car ils ne correspondent pas à une utilisation standard d'Internet par un utilisateur final. Mais un port ouvert, comme précisé par l'étude, n'est pas synonyme d'une machine infectée.

Par contre, il est vrai que chaque port ouvert augmente la surface d'attaque possible de la machine qui l'héberge. Une bonne pratique est alors de limiter les ports ouverts à ceux strictement nécessaires, généralement à ceux liés aux services utilisés par l'utilisateur de la machine.

Quelques remarques concernant l'étude :

- Le scan n'était pas limité aux utilisateurs finaux mais on a également scanné des équipements professionnels où il serait cohérent d'avoir autant de ports ouverts.
- L'étude n'a testé que les adresses IP v4 alors que la Belgique est en pointe pour les adresses IP v6. Les statistiques auraient été plus favorables en testant l'ensemble des adresses IP

Au stade actuel de l'étude, il me semble prématuré de tirer des conclusions tant que des précisions n'auront pas été apportées et que les résultats n'auront pas été mis en perspective avec d'autres facteurs, tel que le déploiement des réseaux ou l'offre des services applicatifs des pays concernés.

Question 2

Le Centre pour la Cyber-Sécurité Belgique (CCB) a lancé avec Microsoft une initiative contre les botnets à laquelle l'IBPT apporte son support pour combattre pour l'exploiter avec les opérateurs télécoms et les fournisseurs d'Internet.

Cette initiative combattrait préventivement les risques liés à trop de ports ouverts sur les machines belges puisque c'est par un port scan que commence une intrusion dans une machine pour la transformer en zombie (membre d'un botnet).

Question 3

CERT.be n'a aucun accès aux données des systèmes informatiques des différents services fédéraux