ASSEMBLÉE NATIONALE

13ème législature

Internet

Question écrite n° 62426

Texte de la question

M. Jean-Paul Dupré attire l'attention de M. le ministre de l'intérieur, de l'outre-mer et des collectivités territoriales sur le développement du piratage sur Internet. Après les clients des banques, il semblerait que ce soit au tour des usagers d'organismes publics d'être la cible des pirates du *web.* Face aux conséquences désastreuses de ces pratiques, il est absolument indispensable de renforcer les moyens de lutte. Il lui demande quelles mesures le Gouvernement entend mettre en oeuvre face à ce phénomène, notamment pour améliorer l'information du public.

Texte de la réponse

Le développement d'Internet offre de nouvelles occasions à une criminalité en constante évolution. Pour y répondre, les forces de sécurité renforcent leurs moyens humains, matériels et juridiques. Un plan d'action de lutte contre la cybercriminalité a été engagé, qui incombe à titre principal à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la direction centrale de la police judiciaire, composé de policiers et de gendarmes. La formation des « cyberenquêteurs » a été améliorée et leur nombre accru, ainsi que celui des « cyberpatrouilleurs ». L'information des internautes, particuliers et professionnels, est un moyen fondamental de lutte contre la piraterie sur Internet. Outre les atteintes aux systèmes de traitements automatisés de données, réprimées par les article 323-1 et suivants du code pénal, les délinquants usent de méthodes qui passent par le vol de données personnelles à l'insu des usagers ou en abusant de leur crédulité. Il peut s'agir d'une pénétration dans leurs ordinateurs ou autres terminaux par le biais d'un « cheval de Troie » ou d'incitations par courriel à se connecter à la réplique d'un site officiel demandant la saisie de leurs identifiants personnels. Dans ce cadre, le ministère de l'intérieur, de l'outre-mer et des collectivités territoriales a développé, dès janvier 2009, une campagne d'information et de sensibilisation par le biais notamment d'affiches et de dépliants. Les dépliants présentent les modes opératoires des délinquants les plus courants et précisent les recommandations essentielles. Ils sont disponibles dans les services de police et de gendarmerie, les préfectures, les mairies et les établissements bancaires. Dans le cadre du plan de lutte contre les escroqueries, une plate-forme de signalement sur Internet (www.internet-signalement.gouv.fr) a été créée pour gérer les informations des fournisseurs d'accès et des internautes concernant les contenus illicites sur Internet. Ce dispositif offre aux citoyens des outils d'information et de prévention concrets contre la cybercriminalité et facilite les investigations des forces de sécurité. Son exploitation est assurée par la plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements, composée de policiers et de gendarmes. Il a également été créé un groupe spécifiquement chargé des escroqueries au sein de l'OCLCTIC. D'autre part, la plate-forme téléphonique « Info escroqueries », rattachée à l'OCLCTIC et composée de gendarmes et de policiers, a pour mission la prévention et l'information du public sur toutes les formes d'escroqueries. Des mesures supplémentaires figureront dans le projet de loi pour la protection des citoyens et la tranquillité nationale, notamment la création d'une nouvelle incrimination pénale d'usurpation d'identité sur Internet. La menace porte également sur les systèmes d'information, publics et privés. Le livre blanc sur la défense et la sécurité nationale l'a pleinement prise en compte et un plan d'action est mis en oeuvre. Une

Agence nationale de la sécurité des systèmes d'information, rattachée au secrétaire général de la défense nationale, a été créée par décret du 7 juillet 2009. Elle a notamment pour mission de contribuer au développement d'une offre de produits et de services de confiance pour les administrations et les acteurs économiques. Chaque zone de défense sera dotée d'un observatoire zonal de la sécurité des systèmes d'information. Plusieurs sont déjà en place et animent un réseau ouvert à l'ensemble des acteurs concernés (services déconcentrés de l'État, collectivités territoriales, organismes chargés d'une mission de service public, entreprises, etc.). S'agissant du ministère de l'intérieur, la surveillance de la sécurité des systèmes d'information y est assurée par la direction de la planification de sécurité nationale, service du haut fonctionnaire de défense.

Données clés

Auteur : M. Jean-Paul Dupré
Circonscription : Aude (3e circonscription) - Socialiste, radical, citoyen et divers gauche
Type de question : Question écrite
Numéro de la question : 62426
Rubrique : Télécommunications
Ministère interrogé : Intérieur, outre-mer et collectivités territoriales
Ministère attributaire : Intérieur, outre-mer et collectivités territoriales

Date(s) clée(s)

Question publiée le : 27 octobre 2009, page 10111
Réponse publiée le : 23 février 2010, page 2119