ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 53080

Texte de la question

M. Thierry Lazaro attire l'attention de Mme la garde des sceaux, ministre de la justice, sur la multiplication des virus informatiques dont la conception relève de plus en plus du domaine de la cybercriminalité. De nombreux pays se sont déjà penchés sur les conséquences dramatiques qui pourraient résulter d'une attaque menée par des cyberterroristes contre les systèmes informatiques de leurs administrations. Aussi, il lui demande de bien vouloir lui faire part des réflexions menées au sein de son ministère ainsi que des services et administrations qui en dépendent, et de le rassurer sur l'efficacité des parades mises en oeuvre en la matière, de façon à éviter que les systèmes informatiques concernés ne puissent être détruits, ou que des données confidentielles ne puissent être transmises à ces cyberterroristes.

Texte de la réponse

La question de l'intrusion dans les systèmes de données est en effet très préoccupante et menace notamment les systèmes d'information tant publics que privés. La législation pénale permet aujourd'hui de poursuivre et de réprimer les agissements visant à porter atteinte aux systèmes informatiques. Ainsi, le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 EUR d'amende. Les peines sont portées à cinq ans et 75 000 EUR lorsque le fonctionnement du système est entravé ou faussé. Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement des données est puni des mêmes peines. Le Livre blanc sur la défense et la sécurité nationale publié le 17 juin 2008 a pleinement pris en compte la protection des systèmes d'information : les attaques informatiques ont été retenues parmi les menaces principales pesant sur le territoire national ; en conséquence, la prévention et la réaction face à ces attaques sont devenues une priorité majeure des dispositifs de sécurité nationale. Le Livre blanc a ainsi fixé un plan d'action, dont la mise en oeuvre est en cours. Pour renforcer la cohérence et la capacité propre des moyens de l'État en matière de sécurité des systèmes d'information, à l'instar des principaux partenaires de la France, le Livre blanc prévoit la création d'une agence nationale de la sécurité des systèmes d'information (ANSSI), relevant du Premier ministre par l'intermédiaire du secrétaire général de la défense nationale (SGDN). Cette agence a été créée par le décret n° 2009-834 du 7 juillet 2009. Elle se substitue à la direction centrale de la sécurité des systèmes d'information (DCSSI), tout en en renforçant les compétences, les effectifs et les moyens. L'Agence nationale de la sécurité des systèmes d'information a notamment pour missions de détecter les attaques informatiques, de prévenir la menace, de jouer un rôle permanent de conseil et de soutien aux administrations et aux opérateurs d'importance vitale, d'informer régulièrement les entreprises et le grand public sur les menaces et les moyens de s'en protéger, et d'entretenir des liens étroits avec ses homologues étrangers. Pour décliner sur l'ensemble du territoire national les mesures prises pour améliorer la sécurité des systèmes d'information, le Livre blanc prévoit également de doter chaque zone de défense d'un observatoire zonal de la sécurité des systèmes d'information (OZSSI), placé sous l'autorité du préfet de zone. Ces observatoires ont été créés au printemps 2009. En ce qui concerne plus précisément les activités judiciaires, l'analyse de risque menée par le haut fonctionnaire de défense et de sécurité (HFDS) dans le cadre du décret n° 2006-212 du

23 février 2006 relatif à la sécurité des activités d'importance vitale, a clairement démontré que les systèmes d'information constituaient des éléments primordiaux pour assurer les missions judiciaires et qu'il était nécessaire de renforcer leur protection. La directive nationale de sécurité du SAIV « Activités judiciaires » (DNS), signée par le Premier ministre en janvier 2008, met en place pour les systèmes d'information du ministère de la justice et des libertés, un ensemble de principes et de règles à la fois organisationnelles et techniques, propres à améliorer progressivement leur sécurité. Chacun des opérateurs d'importance vitale a intégré la menace informatique dans l'analyse conduite préalablement à la rédaction du plan de sécurité opérateur (PSO). En particulier, la sous-direction de l'informatique et de télécommunications (SDIT), service du secrétariat général notamment en charge des infrastructures techniques du ministère a formalisé les mesures à prendre, notamment pour pallier la défaillance de composants d'infrastructures majeurs (incendie dans un centre informatique par exemple) ou de la survenue de crises virales (épisode Conficker au printemps 2009 par exemple). Sans être exhaustif, et dans le strict respect des déclarations CNIL correspondantes, ces mesures comprennent notamment la surveillance renforcée (exclusions d'adresses sur liste noire, contrôle antiviral, détection d'attaques par déni de service) des points d'interconnexion entre le réseau national interne du ministère et les réseaux publics (en particulier internet), la mise en oeuvre d'une défense en profondeur sur ce même réseau interne, une protection - tant logique que physique - renforcée des centres informatiques du ministère, la mise en place de plans de continuité d'activité, la généralisation progressive d'architectures techniques permettant un déplacement rapide de l'exploitation des systèmes critiques, la mise en oeuvre d'une infrastructure destinée à la diffusion automatisée des correctifs de sécurité pour les postes de travail et les serveurs bureautiques, la généralisation au plan national sur les postes de travail d'un anti-virus. À plusieurs reprises, ces mesures se sont avérées pertinentes et efficaces, et les attaques détectées - rares et limitées - ont pu être mises sous contrôle très rapidement. L'ordonnance 2005-1516 sur les échanges électroniques entre les usagers et les autorités administratives et entre autorités administratives, qui annonce la dématérialisation des procédures, oblige à se poser de manière systématique la question sur la disponibilité, la confidentialité et l'intégrité de l'information numérisée. La mise en place d'une infrastructure à clés publiques qui offrirait ces garanties est une des priorités du ministère de la justice et des libertés, en partenariat avec la direction de projet interministériel contrôle automatisé (DPICA) et L'Agence nationale du titre sécurisé (ANTS). Enfin, le système de management de la sécurité porté par les services du HFDS et de la SDIT vise à contrôler, réexaminer, tenir à jour et améliorer la sécurité des systèmes d'information du ministère de la justice et des libertés. Ces objectifs de sécurité passent, conformément aux dispositions de la DNS, par la réalisation quasi systématique d'études de sécurité (selon la méthode EBIOS préconisée par l'ANSSI) pour tout nouveau système d'information ou pour tout système d'information sur lequel une importante évolution est envisagée. Ils passent également par des audits de sécurité de façon à mesurer et corriger la vulnérabilité aux attaques des systèmes.

Données clés

Auteur : M. Thierry Lazaro
Circonscription : Nord (6e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 53080
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Justice
Ministère attributaire : Justice et libertés (garde des sceaux)

Date(s) clée(s)

Question publiée le : 23 juin 2009, page 6059
Réponse publiée le : 20 avril 2010, page 4536