JURIDIQUE


DR

Christiane Féral-Schuhl,
avocate à la Cour, associée fondatrice du cabinet Féral-Schuhl/Sainte-Marie, et bâtonnier désigné du Barreau de Paris

Le piratage de Bercy, une illustration de la cybermenace

Le fait : Bercy a confirmé avoir été victime d'une attaque informatique. Une centaine d'ordinateurs ont été infiltrés par un cheval de Troie qui aurait ciblé des documents liés à la présidence française du G20.

Jamais l'Administration n'avait été victime d'une telle opération d'espionnage informatique. Révélée le 7 mars, l'attaque contre le système d'information (SI) du ministère de l'Economie et des Finances a consisté dans l'envoi de courriels contenant une pièce jointe piégée par un code malveillant non encore répertorié par les antivirus mis en place. L'ouverture de cette pièce jointe a ensuite déclenché l'installation d'un cheval de Troie compromettant progressivement d'autres postes informatiques. Cent cinquante ordinateurs auraient été touchés, nécessitant une opération de maintenance qui a conduit à débrancher, puis à réactiver, 10 000 postes.

L'un des risques majeurs

L'importance de la cybermenace dans la sphère publique a été mise en exergue par le livre blanc sur la défense et la sécurité nationale, publié en 2008. Il retenait le risque d'une attaque informatique contre les infrastructures nationales comme l'une des menaces majeures des quinze prochaines années.
L'Anssi (Agence nationale de la sécurité des systèmes d'information) a été créée dans ce contexte, en juillet 2009. Elle assure, depuis le 11 février 2011, la fonction d'autorité nationale de défense des SI et décide des mesures que l'Etat met en œuvre pour répondre aux crises concernant la sécurité des SI des autorités publiques. Le législateur a aussi publié, en mai 2010, la première version du Référentiel général de sécurité (RGS) qui définit un ensemble de règles s'imposant aux autorités administratives dans la sécurisation de leurs SI.

Les voies d'action

Bercy indique avoir déposé plainte contre X. En effet, lorsque les mesures préventives mises en œuvre n'ont pas évité une cyberattaque – pare-feu, antivirus, tests d'intrusion, veille sécuritaire, audits de sécurité, gestion des accès, sécurisation de l'informatique mobile –, la voie judiciaire reste ouverte. Depuis la loi Godfrain de 1988, le code pénal (articles 323-1 à 323-7) réprime l'accès ou le maintien frauduleux dans un système de traitement automatisé de données, l'entrave au fonctionnement du système, l'introduction frauduleuse de données ou encore la falsification ou la suppression frauduleuse de données.

CHRISTIANE FÉRAL-SCHUHL

CE QU'IL FAUT RETENIR

L'attaque dont a été victime le ministère de l'Economie et des Finances rappelle que l'Administration, comme les entreprises privées, sont des cibles potentielles.

NUL N'EST CENSÉ...

Rapport du Sénat sur la création numérique

La Commission de la culture du Sénat a publié un rapport d'information portant sur la création dans le monde numérique. Elle propose quelques pistes que pourrait suivre le gouvernement sur le financement des contenus et la régulation des acteurs d'internet. En ce qui concerne le statut des hébergeurs, il est conseillé de former une alliance entre éditeurs et distributeurs, *« dans l'intérêt de l'ensemble des acteurs concernés »*. Le rapport est à lire sur http://goo.gl/CfK3t.

Google face à ses responsabilités

Une ordonnance du tribunal de grande instance de Montpellier a fait application de la loi informatique et libertés dans un litige mettant en cause le moteur de recherche Google, auquel il était demandé de supprimer des liens renvoyant à une vidéo à caractère pornographique. Le tribunal a considéré, en l'espèce, que Google et la société Google Inc. étaient responsables des traitements informatiques et a fait application des dispositions de compétence territoriale prévues à l'article 5 de la loi de 1978.

La Cnil encadre le recours à la biométrie

La Cnil, à l'occasion d'une condamnation intervenue à l'encontre d'une société ayant fourni une installation biométrique qu'elle avait refusé d'autoriser, a réaffirmé sa politique en la matière. Elle précise qu'elle n'a *« aucune position de principe à l'encontre de la biométrie, dès lors que les dispositifs mis en œuvre sont respectueux des droits et des libertés fondamentales des personnes »*. L'article est disponible sur le site de la Cnil : http://goo.gl/9u0gL.