Une cyber-attaque d'envergure simulée aux Etats-Unis

- Défense - International -

Date de mise en ligne : mercredi 27 septembre 2006

Spyworld Actu

Des sociétés et organismes publics américains ont participé à « Cyber Storm ». Objectif : tester leur réaction face à une attaque informatique. Ce type d'opération est aussi mené en France.

Les Américains ont joué à se faire peur. Une simulation d'attaque informatique d'envergure a eu lieu du 6 au 10 février dernier, baptisée « Cyber Storm ». En soi, elle ne constitue pas une première. Mais elle vient de faire l'objet d'une communication publique, ce qui est inédit.

Cyber Storm consistait à reproduire une attaque informatique de grande ampleur touchant les systèmes bancaires, les infrastructures de communication, les transports en commun, etc. Pour être le plus réaliste possible, cette opération a mobilisé quelque 300 personnes, réparties dans cinq pays (Etats-Unis, Canada, Royaume-Uni, Australie et Nouvelle-Zélande) et aurait coûté plus de 3 millions de dollars.

La simulation a été orchestrée par le Department of Homeland Security, une branche du National Cyber Security (1). Différents objectifs étaient poursuivis, comme la coordination entre les agences gouvernementales ou la corrélation entre des incidents provenant du secteur public et privé, etc. Il y avait aussi un volet technique très concret avec des hackers censés pénétrer un système. Mais les autorités sont restées assez discrètes sur ce point. Cette simulation technique n'a pas été jusqu'à s'attaquer réellement aux réseaux sensibles.

L'ambition de l'exercice consistait à tester les défenses et les mises en oeuvre des procédures d'alerte et de réponse. Dans un rapport disponible en ligne, les autorités ont relevé les points à améliorer. Y figure l'amélioration de la coordination des opérations entre les différentes parties (armée, secteur privé, et médias notamment).

Ce type de simulation n'est pas propre aux Etats-Unis. L'Otan en fait aussi avec son exercice annuel baptisé « Digital Storm ». Quant à la France, elle organise sa propre opération, « Plan Piranet ». Ce plan de réaction « en cas d'attaque informatique terroriste d'ampleur » contre l'Etat a été développé, comme dans d'autres pays, à la suite des attentats du 11 septembre 2001 aux Etats-Unis. Le premier Piranet remonte à 2003. Le dernier a été réalisé fin 2005. Le prochain est « secret défense ».

« Acquérir des réflexes »

Piranet ne vise pas à éprouver la résistance d'un système ou d'infecter un réseau avec un code malveillant, ce genre de tests étant réalisé régulièrement par les services compétents. « L'important avec Piranet est d'acquérir des réflexes » précise Patrick Pailloux, directeur central de la sécurité des systèmes d'information (DCSSI) au Secrétariat général de la défense nationale (SGDN) (2).

« La dimension technique n'est pas la partie la plus importante. L'essentiel se situe au niveau de la procédure, de l'intendance, de la communication. Bref, il s'agit plutôt d'un exercice de gestion d'une crise : comment communique-t-on lorsqu'on ne dispose plus de moyens de communication, comment fait-on pour obtenir une vision synthétique de l'opération afin de faire un briefing précis aux plus hautes autorités de l'Etat, etc. Le plus compliqué est de créer une simulation qui soit proche de la réalité », précise le responsable de la DCSSI.

(1) Il s'agit d'un partenariat public-privé dédié à l'amélioration de la protection de l'infrastructure informatique clé. S'y trouvent aussi des agences de renseignement. Symantec et Microsoft sont des membres majeurs.

(2) Le service dépend directement du Premier ministre.

Post-scriptum :

http://www.01net.com/article/327620.html