© 360b / Shutterstock.com

© Jstone / Shutterstock.com

en sécurité (l'une dirigée par Neel Mehta, expert en sécurité chez Google, et l'autre de Codenomicon, dont le siège est en Finlande) ne découvrent le bug. Quelques jours plus tard, le magazine *Bloomberg Businessweek* citait des sources anonymes affirmant que la NSA utilisait cette faille depuis des années pour le cyberespionnage.

Nombre d'États puissants ont affecté leurs meilleurs techniciens et des millions d'euros à la découverte et à l'exploitation de vulnérabilités telles que Heartbleed. Les gouvernements achètent aussi des bugs sur le marché libre, contribuant à soutenir l'industrie des failles de sécurité. Un nombre croissant d'entreprises, telles que Vupen Security, à Montpellier, et Exodus Intelligence, à Austin, se spécialisent dans la découverte et la commercialisation de ces précieux bugs. Certains gouvernements dépensent même plus pour la recherche et le développement de capacités offensives que pour la défense contre les cyberattaques. Le Pentagone emploie nombre de chercheurs en vulnérabilités, et le budget de la NSA pour la cyberrecherche offensive est plus du double de celui consacré à la défense.

Cela ne signifie pas que les gouvernements ont des intentions malfaisantes ou qu'ils sont des ennemis de la cybersécurité. Les agences telles que la NSA recueillent des renseignements afin d'empêcher des actes abominables et il est logique qu'elles utilisent tout outil à leur disposition pour y parvenir. Toutefois, une étape importante de la sécurisation du cyberespace consistera à soupeser avec honnêteté les coûts et avantages de l'entretien des vulnérabilités par les agences gouvernementales. Une autre clé de la réussite sera de tirer le plein parti du pouvoir des gouvernements, qui peuvent par exemple obliger des entreprises et autres organismes à partager leurs informations sur les cyberattaques.

Les banques, en particulier, auraient tout intérêt à le faire, car les attaques sur les institutions financières suivent d'ordinaire un schéma prévisible : quand les criminels trouvent un angle d'attaque qui fonctionne avec une banque, ils l'essaient sur une autre, puis une autre… Toutefois, les banques évitent de divulguer des informations sur les attaques subies, car cela soulève des questions sur leur propre sécurité. Elles évitent aussi de communiquer avec leurs concurrentes ; dans certains cas même, les lois antitrust l'interdisent. Les gouvernements, en revanche, peuvent faciliter le partage d'informations entre banques. Ce partage est déjà mis en place aux États-Unis sous la forme du Centre de partage et d'analyse d'informations pour les services financiers (FS-ISAC), qui sert aussi les organismes financiers mondiaux. Et en février, Barack Obama a signé un décret présidentiel qui enjoint d'autres entreprises à partager leurs renseignements entre elles et avec le gouvernement.

DEUX CYBERATTAQUES qui ont marqué les esprits : le 24 novembre 2014, Sony Pictures Entertainment, filiale américaine du groupe japonais Sony, est piratée. De nombreuses données sont détruites, d'autres sont divulguées, notamment des films en postproduction. Quelques mois plus tôt, durant l'été 2014, des pirates ont volé les données personnelles de milliers de clients de la société américaine de portefeuille JP Morgan Chase.

Les pirates à la rescousse

Tant que les hommes écriront des programmes, des vulnérabilités existeront. Sous la pression concurrentielle, les entreprises du secteur des technologies introduisent leurs produits sur le marché plus vite que jamais. Ces entreprises seraient bien avisées d'exploiter l'énorme ressource humaine que constitue la communauté mondiale des hackers. Au cours de l'année passée, catalysées par des événements tels que les révélations d'Edward Snowden sur la NSA, l'industrie technologique et la communauté des hackers ont commencé à accepter l'idée de travailler ensemble. À présent, des centaines d'entreprises voient l'intérêt d'embaucher des hackers en les attirant au moyen de programmes qui récompensent la découverte de bugs ou de vulnérabilités