Cybersécurité : la quête de législations harmonisées

À quand une législation nationale sur le signalement des incidents de cybersécurité ? Aux États-Unis, la question n'est pas nouvelle. Elle est toutefois revenue dans la lumière avec l'attaque contre Colonial Pipeline. À plus forte raison après l'audition de l'entreprise au Congrès. Elle s'est refusée à évoquer, dans ce cadre, la rançon qu'on la soupçonnait d'avoir payé. Plusieurs parlementaires se sont insurgés, soulignant à quel point une telle information était nécessaire dans la lutte contre la cybercriminalité.

Des représentants du FBI et du département de la Justice ont fait des déclarations de même teneur à l'occasion de la conférence RSA. Et brandi une menace : à défaut de procédure de signalement harmonisée, il faudrait donner au renseignement l'autorisation d'espionner, à des fins préventives, les réseaux de certaines entreprises privées. En particulier les OIV.

Cette législation est l'une des priorités de la Cyberspace Solarium Commission, créée en 2019 pour assister le gouvernement dans ses démarches de cyberdéfense. La mise sur pied d'un « Bureau des statistiques de cybersécurité » en est une autre. Mais pour dresser ces statistiques, il faut des informations…

En l'état, les victimes de cyberattaques font face à un patchwork de textes de loi, axés pour certains uniquement sur les fuites de données personnelles – sans considération de la sécurité du pays. Un seul secteur dispose d'un cadre de portée nationale : la santé, avec le HIPAA (Health Insurance Portability and Accountability Act).

Fais comme FireEye ?

En matière de signalement, les représentants du FBI et du DoJ invitent à prendre pour modèle FireEye. Plus précisément la réaction de l'éditeur après sa découverte de la faille SolarWinds.

Du côté de Colonial Pipeline, on a fini par reconnaître avoir payé une rançon de 4,4 millions de dollars. Mais douze jours après l'incident, alors que la décision semble avoir été prise dans les heures suivant la découverte. Pour sa défense, l'entreprise affirme qu'il s'agissait de « la [meilleure] chose à faire pour le pays ». Tout en admettant avoir eu trop d'incertitude sur l'ampleur des dégâts et donc sur le délai de rétablissement.

Officiellement, le réseau de pipelines a été coupé pour éviter une propagation depuis le SI. Certains soulignent néanmoins qu'au-delà de la sûreté industrielle, un autre élément aurait pu motiver ce choix : l'impossibilité de facturer les clients.

Un autre texte est revenu sur le devant de la scène au Congrès : le Pipeline Security Act. Son objectif : renforcer le rôle des autorités – dont la CISA, homologue de notre ANSSI – dans la cybersécurité des opérateurs de pipelines. Ces derniers font, en parallèle, l'objet d'appels appuyés à la nationalisation.

Photo d'illustration © datacorpltd via Visualhunt.com / CC BY-NC