PERTES & PROFITS | CYBERSÉCURITÉ

Un virus dans le pipeline

par Philippe Escande

C'est une immense et solide artère qui irrigue une bonne partie de l'Amérique. Le Colonial Pipeline s'étend sur près de 9 000 kilomètres, le long de la côte est des Etats-Unis, de Houston à New York en passant par Washington et Atlanta. A lui seul, il fournit 45 % des besoins de la région en essence, fioul, kérosène et autres carburants raffinés au Texas.

Mais le flot ne coule plus depuis vendredi 7 mai au soir. Une attaque informatique a désorganisé le système d'information de la société exploitante du réseau. Des pirates ont crypté les données et demandent une rançon pour les débloquer. Dans l'incertitude, le gouvernement a décrété l'état d'urgence afin d'autoriser des camions-citernes à sillonner les 17 Etats traversés par le réseau. Des bateaux sont réquisitionnés.

C'est la première fois qu'une attaque informatique touche aussi violemment une infrastructure énergétique essentielle. Mais ce n'est pas la première fois que les professionnels sont prévenus. En 2016, selon le *Wall Street Journal*, le service de cybersécurité du département de la sécurité intérieure des Etats-Unis avait identifié 186 vulnérabilités dans le secteur de l'énergie et, en 2018, une intrusion du même genre avait touché le système de commande d'une unité de compression d'un fournisseur de gaz. La société n'avait aucun plan de réponse à une telle agression.

A l'image de la pandémie, dont la venue avait été annoncée sur tous les tons par de nombreux experts depuis plus de dix ans, les victimes tombent pourtant des nues quand le mal arrive. L'impréparation est totale. Il ne s'agit pourtant plus d'un cygne noir, cet événement très peu probable aux conséquences dévastatrices, mais d'un risque désormais connu et balisé. Qu'ils soient cachés en Russie en Chine ou en Californie, les pirates attaquent désormais des écoles, des hôpitaux et même l'administration. Tantôt pour infecter, voire détruire, tantôt pour prendre en otage des données et programmes essentiels.

Les failles sont souvent les mêmes, au cœur des machines, des matériels anciens, datant d'avant l'Internet, couplés à des systèmes modernes branchés sur le réseau. Les cambrioleurs utilisent l'un pour toucher l'autre. La criminalité numérique s'épanouit dans le basculement du monde vers les réseaux. Il serait bon de s'y préparer sérieusement.