La cyber-sécurité des grandes infrastructures. Vivre avec le risque

Jean-Pierre Hauet
Associate Partner
KB Intelligence
Membre Emérite de la SEE

Il devient difficile d'écrire sur la cyber-sécurité : tant de choses ont été dites sur les virus, les vers, les chevaux de Troie, l'homme du milieu, le phishing, le snarfing, le spoofing. Pourtant la menace existe et la cyber-sécurité est plus qu'un beau sujet de conférence : c'est un risque avec lequel il faut désormais apprendre à vivre ; un risque qui n'est pas aujourd'hui contenu : l'article d'Yves Deswarte et Sébastien Gambs constitue une véritable taxinomie de toutes les espèces d'attaques qui sont aujourd'hui recensées et qui deviennent de plus en plus sophistiquées et pernicieuses. Le temps est bien fini où les étudiants passionnés par les travaux d'Adi Shamir s'entraînaient à craquer le chiffrement Wep des premiers Wi-Fi sur le parking des supermarchés. Les attaques ont pris une autre ampleur, elles sont le fait de spécialistes organisés, sponsorisés par des organisations maffieuses ou terroristes, voire par des gouvernements et les références à la Chine, à la Russie, aux USA, à Israël, etc. reviennent souvent dans les coupures de presse.

L'épisode de l'attaque Stuxnet dirigé contre les centrifugeuses de l'usine d'enrichissement d'uranium de Natanz en Iran a montré que les systèmes de contrôle-commande de procédé n'étaient plus à l'abri des attaques et que celles-ci pouvaient atteindre un degré de sophistication inimaginable il y a quelques années.

La contamination par les maliciels peut se faire de façon subreptice, être masquée par de faux certificats, revêtir des périodes d'incubation très longues, se développer sur des cibles choisies mais infectant cependant des dizaines de milliers de porteurs sains.

La comparaison avec les plus redoutables des pandémies se fait chaque jour plus réaliste.

Stuxnet est venu mettre un terme à un mythe qui avait la vie dure : celui de « l'air gap », c'est-à-dire de la protection par l'isolement. Aucun système de traitement de l'information ne peut prétendre être durablement isolé du monde extérieur. Survient toujours un moment où il faut mettre à jour un logiciel, actualiser des paramètres, échanger des informations, changer des mots de passe, admettre de nouveaux opérateurs, etc. Qui plus est, la recherche de la productivité et de l'efficacité passe nécessairement par une intégration toujours plus poussée entre les différents niveaux d'une structure et on connait le succès qu'ont rencontré dans l'industrie les notions de MES (Manufacturing Execution System) et ERP (Enterprise Resource Planning). Les organisations qui affirment s'être mises à l'abri des attaques cyber-sécuritaires par un « air gap », se bercent d'illusion. Elles ont simplement remplacé les réseaux traditionnels par les réseaux furtifs que sont les CD Rom, les clés USB, les smartphones, en attendant mieux, et on sait par expérience qu'un système fondé sur la seule confiance des personnes est tôt ou tard voué à être miné par la négligence ou par la corruption.

Bien entendu le fantastique développement de l'Internet et de la mise en réseau des hommes et des objets, qui est bien loin d'avoir atteint son apogée, ne fait qu'élargir la menace ; « Tous ne mourraient pas, mais tous étaient frappés » pourra-t-on bientôt dire.

L'article de Pierre Caron ouvrira les yeux de tous ceux qui ne voient dans les smartphones et dans les réseaux sociaux que les avantages d'une ouverture toujours plus large sur le monde qui nous entoure. Il ne s'agit pas pour autant d'imaginer que l'on puisse freiner la progression de l'univers numérique. La recherche de la productivité et du confort, l'élargissement du tissu social seront toujours aux avant-postes ; mais il faut apprendre à vivre avec le risque, ce qui implique de connaître les menaces, d'être conscient de ses vulnérabilités et de prendre les décisions raisonnables pour ramener le risque à un niveau acceptable.

Le cas des grandes infrastructures est particulièrement éloquent. On entend par grandes infrastructures celles qui rendent un service essentiel à la nation : la production, le transport et la distribution d'électricité, l'alimentation en eau, la production et la distribution d'hydrocarbures, le système bancaire, les services d'urgence, les transports publics, les

services gouvernementaux régaliens, les télécommunications. Tous utilisent les technologies de l'information pour leur gestion mais aussi pour leur fonctionnement. Ce sont donc des cibles de premier choix pour la cybercriminalité. Tout d'abord parce que l'interruption de leur fonctionnement crée en soi un préjudice notable qui pourrait prendre des proportions vertigineuses : imaginons un instant un centre de contrôle ferroviaire pris en mains par des terroristes et précipitant deux TGV l'un sur l'autre. Egalement parce que, curieusement, leur nombre a tendance à augmenter : on voit par exemple poindre des flottes de véhicules électriques dont le fonctionnement technique et financier pourrait être gravement perturbé par des cyber-attaques. Enfin et surtout parce qu'elles sont de plus en plus interdépendantes les unes des autres. Il y a bien longtemps que le particulier sait que son chauffage central au fuel devient inopérant en cas de coupure d'électricité. Mais cette interdépendance devient la règle générale. Le couplage entre système d'information et système électrique est porté aux nues par les thuriféraires des « smart grids ». Il y a certes des voies de progrès indéniables. Mais un dérèglement grave sur le système électrique lié à un cyber-incident aurait des répercussions immédiates sur tous les autres services. De la même façon, une attaque en déni de service sur les systèmes de communication pourrait rendre les services d'urgence impuissants.

Patrick Pailloux évoque à juste titre le scénario des concours de dominos où des centaines de milliers de dominos s'effondrent sous l'effet d'une simple pichenette. Les attaques terroristes à double détente, où une première vague détourne l'attention cependant qu'une deuxième vague plus meurtrière se prépare, sont particulièrement pernicieuses. Mais tous les scénarios peuvent être envisagés et s'agissant d'attaques délibérées, ils échappent aux calculs de probabilités objectives.

Jean-Pierre Hauet *est ancien élève de l'Ecole Polytechnique et Ingénieur du corps des mines. Il a occupé différentes positions dans l'Administration, en particulier celle de rapporteur général de la Commission de l'Energie du Plan. Il a dirigé le centre de recherches de Marcoussis d'Alcatel avant d'être nommé directeur Produits et Techniques de Cegelec, puis Chief Technology Officer d'ALSTOM. Depuis 2003, il est Associate Partner de KB Intelligence, spécialisé dans les questions d'énergie, d'automatismes industriels et de développement durable. Il préside l'ISA-France, section française de l'ISA (Instrumentation, Systems & Automation Society). Il est membre Emérite de la SEE et membre du comité de rédaction de la REE.*

Le présent dossier n'a pas l'ambition de tout traiter. Il faudra en particulier revenir sur le cas des réseaux électriques et des risques inhérents aux systèmes de comptage communicants. Le risque n'est pas que l'usager rentre dans le compteur évolué des informations pernicieuses. Sans doute ne le pourra-t-il pas. Mais, dès lors que le pouvoir de coupure sera ouvert par ordre distant, que se passera-t-il si une organisation criminelle s'infiltre dans le système, détourne les clés de chiffrement et envoie des ordres fallacieux d'interruption de service à des millions d'usagers sans que la tension puisse être rétablie autrement que par une intervention sur place ? A-t-on également pesé tous les risques de voir les 30 millions de compteurs devenir des zombies d'un gigantesque « botnet » ?

Il faut convenir que la France fait preuve d'une assez grande insouciance face à ces problèmes. La création de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ne date que de juillet 2009, alors qu'il y a belle lurette, et surtout depuis les événements du 11 septembre 2011, que les américains sont sensibilisés au risque terroriste malgré les excès du syndrome Y2K. Plusieurs organisations gouvernementales Nord-américaines – le NIST (National Institute of Standards and Technology), le NERC (North American Electric Reliability Corporation) – ont édicté des règles visant à se prémunir contre le risque cyber-sécuritaire. Mais c'est aujourd'hui l'ISA (International Society of Automation) qui, en liaison étroite avec la CEI, propose le corpus méthodologique le plus complet afin d'évaluer la vulnérabilité des installations industrielles au risque de cyber-attaque et de proposer une démarche rationnelle permettant de se protéger, en profondeur, contre des attaques, en adaptant judicieusement le coût de la protection à celui des risques encourus. ■

LES ARTICLES