12 juillet 2016

Le secteur énergétique exposé à la cyber-menace

Gabrielle DESARNAUD

Depuis plus de deux décennies, les métiers de l'industrie énergétique sont révolutionnés par la digitalisation. Celle-ci a non seulement pénétré les services commerciaux, administratifs et financiers des entreprises, mais aussi leurs systèmes industriels : de l'optimisation de nos réseaux électriques à la précision des forages pétroliers, les technologies de l'information et de la communication (TIC) sont désormais indispensables à toutes les étapes de la production, du transport et de la distribution d'énergie. La numérisation de ce secteur ne cessera de se développer avec les réseaux intelligents et les compteurs communicants.

L'analyse et le traitement des données sont peu à peu considérés comme le nouvel « or noir » du secteur énergétique et créent de nouvelles activités à l'image de l'équipementier General Electric, qui propose à l'industrie énergétique une plateforme d'analyse des données récupérées par les capteurs présents dans les équipements industriels[1].

Cette révolution silencieuse offre d'innombrables opportunités économiques et ouvre la voie vers une meilleure allocation des ressources. Elle rend aussi les infrastructures physiques vulnérables à la cybercriminalité, un risque que l'industrie énergétique n'est pas complètement préparée à affronter.

Une menace en expansion

Le 23 décembre 2015 en Ukraine, une cyber-attaque sur plusieurs opérateurs électriques régionaux a privé d'électricité plus de 200 000 résidents durant quelques heures et forcé les opérateurs à gérer les postes électriques manuellement jusqu'à plusieurs semaines après l'attaque. L'utilisation de méthodes classiques de piratage informatique telles que le hameçonnage[2], combinée à une connaissance très précise des Systèmes de Contrôle Industriels (SCI)[3] gérant la distribution d'électricité, ont permis aux attaquants d'actionner à distance les

Gabrielle Desarnaud est chercheur au Centre Énergie de l'Ifri.

ISBN : 978-2-36567-597-0

Comment citer cette publication :

Gabrielle Desarnaud, « Le secteur énergétique exposé à la cyber-menace », *Édito Énergie*, 12 juillet 2016.

Ifri
27 rue de la Procession
75740 Paris Cedex 15
Tél. : +33 (0)1 40 61 60 00
Email : accueil@ifri.org

Site internet :
www.ifri.org

disjoncteurs d'une trentaine de postes électriques et couper le courant[4].

C'est la première fois qu'une cyber-attaque visant spécifiquement un réseau électrique parvenait à ses fins. Peu sont susceptibles de provoquer des dégâts d'une telle ampleur. Tous les experts s'accordent à dire que le degré de préparation, de coordination, de connaissance des systèmes industriels visés, ainsi que les moyens financiers probablement engagés dans cette opération ne sont pas à la portée de tous les groupes criminels, ni même de tous les États. Une investigation menée sur le terrain par plusieurs agences américaines a de plus déduit que les SCI des opérateurs ukrainiens étaient particulièrement bien protégés[5].

La Russie a rapidement été montrée du doigt par les autorités ukrainiennes[6]. S'il y a peu de preuves sur le rôle réel joué par Moscou, le facteur géopolitique ne peut être écarté. La seule autre cyber-attaque ayant eu des répercussions sérieuses sur une infrastructure énergétique[7] remonte au ver informatique Stuxnet découvert en 2010, configuré pour ralentir le programme nucléaire iranien, et à l'origine de dégâts matériels conséquents. Un millier de centrifugeuses d'enrichissement d'uranium ont été endommagées par ce *malware*, passé inaperçu durant plus d'un an[8]. Là encore des intérêts géopolitiques et le soutien présumé de deux États-nations (États-Unis et Israël[9]) rendent cette attaque exceptionnelle.

Les entreprises énergétiques seraient de plus en plus visées par ce genre de menaces[10] et la structure de leurs activités (à la fois commerciales et industrielles) les rend particulièrement vulnérables pour plusieurs raisons :

- culturelles : les secteurs industriels sont traditionnellement protégés physiquement. Il s'agit d'un monde d'automaticiens où la sécurité des personnes et la continuité du service sont les maîtres-mots, mais où les pré-requis informatiques sont encore nouveaux.

- historiques : les SCI qui ont permis d'automatiser et d'optimiser les processus industriels étaient à l'origine fondés sur des logiciels propriétaires développés pour des activités spécifiques, ce qui rendait complexe une connaissance fine de chaque système par des personnes extérieures. Des systèmes d'exploitation clef en main

(Windows, Linux…) ont finalement pénétré les entités commerciales et industrielles des énergéticiens.

- organisationnelles : différentes entités d'une entreprise peuvent être infiltrées et servir de point d'accès aux SCI. Une campagne de hameçonnage bien ciblée peut inciter un utilisateur à cliquer sur un document corrompu (dans le cas ukrainien des emails frauduleux laissaient penser qu'ils étaient envoyés par le Parlement). Les canaux de communication entre différentes entités d'une même entreprise (sites de production, transformation, transport, business, etc.) peuvent être protégés mais restent vulnérables. Autoriser l'accès à distance pour gérer les processus industriels peut permettre à des personnes externes d'en prendre le contrôle en cas de protection insuffisante (absence de systèmes d'authentification superposés). Par ailleurs, assurer la continuité des opérations industrielles rend la mise à jour des systèmes d'exploitation complexe, alors qu'exploiter leurs vulnérabilités est aujourd'hui à la portée d'un grand nombre d'individus.

Une cyber-attaque sur des infrastructures énergétiques aurait des répercussions conséquentes sur toute une économie. En 2015, la compagnie d'assurance Lloyd's simulait les coûts d'une cyber-attaque sur plusieurs générateurs d'électricité aux États-Unis. La mise hors service du réseau dans 15 États engendrerait un coût total pour l'économie américaine entre 243 milliards et un trillion de dollars[11]. En Europe, l'interconnexion des réseaux électriques pourrait également conduire à un écroulement du réseau en cas d'attaque, comme ce fut le cas en novembre 2006 lorsque la déconnexion d'une ligne haute tension en Allemagne a entraîné des faillites en cascade dans six pays, touchant 15 millions d'utilisateurs[12].

Construire une cyber-sécurité à l'européenne ?

Les autorités européennes sont conscientes que la cybercriminalité n'a pas de frontières : en 2013, le logiciel Dragonfly élaboré pour espionner des industries de défense américaines a été retrouvé dans les systèmes informatiques de plusieurs entreprises énergétiques aux États-Unis et en Europe[13]. Si celui-ci n'était a priori destiné qu'à la collecte de données, il disposait en revanche de fonctionnalités capables de causer des dégâts matériels substantiels. Les logiciels malveillants circulent facilement entre les entreprises de différents

secteurs, les SCI étant souvent communs à différents types d'activités industrielles.

Les moyens d'action pour se prémunir contre ce type de menace au niveau européen restent aujourd'hui limités. Dans un espace où les infrastructures énergétiques sont de plus en plus interconnectées, la mise en place de certaines normes communes et d'une coopération renforcée entre les Etats membres peut éviter la propagation de logiciels malveillants à travers toute la chaîne logistique énergétique. A l'heure actuelle, l'Agence européenne pour la sécurité des réseaux et de l'information (ENISA)[14] n'est pas en mesure de faire appliquer des normes communes en matière de sécurité des systèmes d'information. Cette dimension préventive de la cyber-sécurité au niveau européen est encore peu opérationnelle, alors que le traitement ex-post des crises de cyber-sécurité est bien coordonné par Europol. La Commission européenne se rapproche tout de même des États-Unis où des standards sont imposés au niveau fédéral dans le secteur de l'électricité [15], afin d'étudier l'intérêt d'une harmonisation avec l'Europe. Cependant, si certains Etats comme la France, appliquent des normes strictes notamment à leurs sites nucléaires[16], celles-ci ne sont pas forcément transposables au reste de l'Union européenne.

En 2013, la Commission européenne a présenté une stratégie de cyber-sécurité[17] pour l'Europe, accompagnée d'un projet de directive[18] sur la sécurité des réseaux et de l'information (SRI). La proposition a été approuvée par le Conseil européen en mai 2016, et adoptée par le Parlement européen le 6 juillet dernier. Attendue pour une entrée en vigueur en août 2016[19], la directive SRI pose les premiers jalons d'une politique de sécurité commune en matière de protection du cyberespace européen. Ce texte législatif impose aux Etats membres de se doter d'une stratégie de cyber-sécurité, de désigner une autorité nationale dotée des ressources appropriées pour gérer les incidents SRI et d'établir une liste d'opérateurs fournissant des services essentiels (transports, énergie…). Ces derniers devront adopter des pratiques de gestion des risques informatiques et rapporter tous les incidents à l'autorité nationale compétente. Un mécanisme de coopération entre États membres et la Commission permettra également de diffuser des alertes et échanger des informations.

La Commission européenne entend donc construire une culture commune de la cyber-sécurité, sans empiéter pour autant sur les

fonctions régaliennes des États membres. Des programmes de recherche et des exercices de simulation viennent renforcer cette approche, avec un intérêt croissant de la part des hauts dirigeants et des entreprises. Cette stratégie se heurte toutefois à trois obstacles. Les questions de sécurité et de défense restent la prérogative des États, et ceux-ci sont peu enclins à partager les informations dans ce domaine. Les entreprises sont également réticentes à communiquer sur ces questions pour préserver leur réputation. Enfin, l'industrie énergétique a l'habitude de gérer des incidents physiques, alors qu'évaluer la probabilité, l'étendue, les conséquences physiques et financières d'une cyber-attaque demeure complexe. Une cyber-attaque reste une menace intangible et les systèmes de protection avancés sont perçus comme onéreux et invasifs.

La cyber-menace est aujourd'hui une réalité. Et dans le cas où l'industrie énergétique aurait affaire à une « menace persistante avancée[20]», aucune protection, si développée soit-elle, n'est infaillible. Construire un cadre préventif qui prend en compte les interdépendances du système énergétique européen, fondé sur un socle de standards communs et un partage de l'information systématique permettrait cependant de singulièrement réduire les risques.

1. Predix « http://gereports.fr ».

2. Attaque informatique basée sur l'usurpation d'identité, par email par exemple, afin d'inciter le récepteur à donner des informations confidentielles, ou avoir un comportement qu'il ne sait pas être dangereux pour son entreprise (installer un programme, cliquer sur un lien corrompu…).

3. Les SCI sont des systèmes informatiques servant à contrôler et automatiser de nombreux processus industriels.

4. *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Electricity Information Sharing and Analysis Center and SANS Institute, mars 2016.

5 . « Cyber-Attack Against Ukrainian Critical Infrastructure », U.S. Department of Homeland Security, ICS-CERT, février 2016.

6. Le 28 décembre 2015, le Service de sécurité d'Ukraine met en garde contre des cyber-attaques russes sur les infrastructures énergétiques ukrainiennes. Le principal élément menant à cette conclusion vient d'une attaque en déni de service sur les centres d'appel d'urgence des opérateurs attaqués, les empêchant de recevoir les plaintes de leurs clients. La vague d'appels visant à saturer le réseau semble provenir de la région de Moscou « www.sbu.gov.ua». La société de sécurité informatique ESET a communiqué sur la possibilité d'une intervention sous un « faux drapeau ».

7. Le 15 Août 2012 Saudi Aramco subissait une cyber-attaque détruisant les disques durs de 35000 ordinateurs de la firme, cependant les infrastructures énergétiques n'ont pas été touchées et la production est restée stable.

8. K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital*

Weapon, Crown Publisher, novembre 2014.

9. « Obama Order Sped Up Wave of Cyberattacks Against Iran », *The New York Times*, 1er juin 2012.

10. « https://ics-cert.us-cert.gov».

11. *Emerging Risk Report 2015*, *Business Blackout – The Insurance Implications of a Cyber-attack on the US Power Grid*, Lloyds and University of Cambridge, 2015.

12. Union for the Coordination of Transmission of Electricity UCTE, *Final Report*, System Disturbance on 4 November 2006

13. N. Nelson, « The Impact of Dragonfly Malware on Industrial Control Systems », SANS Institute, janvier 2016.

14. European Union Agency for Network and Information Security.

15. www.nerc.com

16. www.power-eng.com

17. https://ec.europa.eu/digital-single-market

18.http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52013PC0048

19 Pour tout le processus législatif voir www.europarl.europa.eu/ et http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm

20. « Advanced Persistant Threat », désigne un type d'attaque informatique ayant une cible spécifique, le plus souvent pour des motifs d'affaires ou politiques. Elle est « avancée » car elle met en œuvre des moyens techniques et financiers conséquents, et « persistante » car l'opération peut durer plusieurs années de façon dissimulée.