Éditoriaux de l'Ifri

Édito Énergie

12 July 2016

Cyber Attacks: A New Threat to the Energy Industry

Gabrielle DESARNAUD

In about two decades, the energy industry has been deeply transformed by the digital revolution, which penetrated companies' commercial, administrative and financial branches, but also their industrial systems. From the optimization of electric grids to the precision of oil drilling, information and communication technologies (ICT) are now essential to every stage of energy production, transport and distribution processes. Data mining and analysis are increasingly considered as the energy sector's new "black gold", and generate new activities just like the platform Predix designed by General Electric to help energy companies (among others) collect and analyze industrial data[1].

This silent revolution offers countless economic opportunities and paves the way for a better resource distribution and use. But it also puts physical energy infrastructures at risk.

An Expanding Threat

The 23 December 2015 in Ukraine, a cyber-attack on several regional grid operators deprived more than 200 000 people of electricity for a few hours, and constrained operators to physically intervene at the substations to restore power. Since substations could no longer be remotely controlled, on-site interventions had to be maintained during several weeks after the event in order to ensure the electricity delivery. The use of common hacking methods such as phishing[2], combined with a very precise knowledge of Industrial Control Systems (ICS) [3] dealing with electricity distribution, allowed attackers to remotely activate breakers in about 30 electric substations and cut the power off[4].

This was the first time a cyber-attack targeting the grid had physical consequences. Few attacks are likely to have such implications. All experts agree on the fact that the level of preparation and coordination, the degree of knowledge of ICS targeted and probable financial means invested in this operation are not within reach of any criminal group, or State. Moreover, an on-field study conducted by several Federal US

Gabrielle Desarnaud is a researcher at the Center of Energy of Ifri.

The opinions expressed in this text are the responsibility of the author alone.

ISBN: 978-2-36567-598-7

How to quote this publication:

Gabrielle Desarnaud, « Cyber Attacks: A New Threat to the Energy Industry", *Édito Énergie*, 12 July 2016.

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

Website:
www.ifri.org

agencies found that the Ukrainian operators' ICS were particularly well protected[5].

Ukrainian authorities have been quick to point at Russia after the event[6], and even if very few elements can lead to the conclusion that Moscow was involved in the attack, this event might well have a geopolitical background[7]. The only other known cyber-attack with serious consequences on an energy infrastructure goes back to the Stuxnet worm discovered in 2010, designed to slow the progression of the Iranian nuclear program. A thousand uranium enrichment centrifuges were damaged by this malware, which went unnoticed for more than a year[8]. Here again, strategic interests and the presumed support of two nation-States (the USA and Israel) make this attack remarkable[9].

Energy companies are more and more targeted by this kind of threats[10], and the structure of their activity makes them particularly vulnerable, for several reasons:

- Cultural reasons: industrial sectors are traditionally protected physically. Automation engineers pay a particular attention to safety and service availability, while they are less prepared for IT systems' protection.

- Historical: the ICS that helped automate and optimize numerous industrial processes were at first proprietary software developed for specific activities. It would have been difficult for people not involved in their conception and operation to know them in detail and exploit their vulnerabilities. Ultimately, off-the-shelf software (Windows, Linux…) were adopted in business and industrial entities of energy companies.

- Organisational: different company units can be used as a backdoor to ICS. A phishing campaign can persuade an employee to open a corrupted document (in the Ukrainian case, the malwares involved in the attack had spread to the operators' computers thanks to fraudulent emails, to all appearances sent by the Parliament). Communication channels between different company entities (business unit, production site, transportation system…) can be protected (by a firewall, for instance) but remain vulnerable. Remote control of some industrial processes can be used by hackers in case of low protection level (lack of strong authentication measures). Besides, ensuring industrial operations continuity makes software updates difficult, while taking advantage of their vulnerabilities is now within reach of lots of individuals.

A cyber-attack on energy infrastructures would have significant economic implications. In 2015, the insurance company Lloyd's calculated the potential costs of a cyber-attack targeting several electricity generators in the US. The subsequent grid failure in 15 States would cost 243 billion to one trillion dollars to the US economy[11]. The cascading failures hypothesis used by Lloyd's might happen in Europe as well, like in 2006 when the disconnection of a high voltage line in Germany caused a blackout in six countries, depriving 15 million people of electricity[12].

Building a European cyber security framework?

Cyber criminality has no frontiers: in 2013 for instance the malware Dragonfly designed to spy US defence industries has been discovered in computer systems of several energy companies across Europe and the US[13]. Even though the main purpose of this malware was data collection, other functionalities could have caused substantial material damages. Because same ICS are used in very different industrial processes, malwares can disseminate easily between companies and sectors having very few connections between them.

Means of action at a European level to guard against these kinds of risk remain very limited. On a territory where energy infrastructures are set to be more and more interconnected, creating an entity able to react quickly and coordinate the actions of the Member States might avoid the propagation of malwares to multiple critical operators across Europe. For now, the European Union Agency for Network and Information Security (ENISA)[14] is not in a position to apply common standards in terms of information networks security. This preventive aspect of cyber security remains little operational in Europe, while the ex-post treatment of crisis can be well coordinated by Europol. The European Commission is discussing with the US (where cyber security standards are already implemented at the federal level to the electricity sector[15]) in order to study potential cooperation areas in the field of cyber security norms. However, some Member States like France apply, for instance, very strict standards in their nuclear power plants[16], which might not be applicable to the rest of the EU.

This is why in 2013 the European Commission released a cyber-security strategy for Europe[17], along with a proposal for a new directive entitled Network and Information Security directive (NIS)[18]. After an approval by the European Council in May 2016, the directive was approved on July 6th by the European Parliament. Expected to enter into force in August 2016[19], the NIS directive prepares the ground for a common security policy in the European cyber space. This legislative text requires from Member States to designate a national authority and a Computer Security Incident Response Team (CSIRT) provided with appropriate resources to deal with NIS incidents, adopt a national strategy, and establish a list of critical operators (transports, energy…). The companies and institutions identified as critical will have to adopt a cyber security management strategy and report all incidents to the national authority. A cooperation mechanism between member States and the EU Commission will also allow alerts diffusion and information exchanges.

The European Commission is aiming to build a common cyber security culture without overlapping with sovereign powers of Member States, through research programs and simulation exercises, with a growing interest from States and companies’ top management. But this strategy faces three main obstacles. First, questions of security and defence remain the prerogative of the States, which are not prone to share information in this matter. Then, companies are also reluctant to communicate on their vulnerabilities in order to preserve their reputation. Finally, the energy industry has a long experience in dealing with physical incidents and disruptions, while assessing the probability, the scope, and the material consequences of a cyber-attack remains complex. A cyber-attack is an intangible threat, while advanced protection systems are still perceived as expensive and invasive.

The cyber threat is a reality, and in case an “advanced persistent threat”[20] would target the energy industry, no protection, as efficient as it might be, would be infallible. Building a preventive framework taking into account interdependencies between European energy systems, based on a set of common standards and procedures and systematic information sharing practices, would instead significantly reduce the risks.

[1] Predix “ http://gereports.fr”

[2] “Phishing” is a kind of cyber attack relying on social engineering. It refers to the attempt

to acquire sensitive information (usernames, passwords) by masquerading as a trustworthy entity in an electronic communication.

3. "Industrial Control System" or "ICS" is a general term that encompasses several types of electronic systems used to control industrial processes. They include Supervisory Control and Data Acquisition systems (SCADA), often targeted by cyber-attacks on industries.

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

5. US. Department of Homeland Security, Industrial Control Systems Computer Emergency Response Team, Cyber-Attack Against Ukrainian Critical Infrastructure, February 2016.

6. In December 2015, the Ukraine Security Service warned against cyber attacks orchestrated by Russian authorities on Ukrainian energy infrastructures.

7. The main element leading to this conclusion is a denial of service (DoS) attack simultaneous to the cyber attack on grid operators, and preventing victims of electricity blackouts to call operator's emergency call centers. This DoS attack seems to come from the region of Moscow. "www.sbu.gov.ua". The internet security company ESET warned on the fact that this attack could have been done under a "false flag".

8. K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown Publisher, November 2014.

9. "Obama Order Sped Up Wave of Cyberattacks Against Iran", *New York Times*, June 1st, 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, January 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. For all the legislative process see: www.europarl.europa.eu/ and
http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm

20. "Advanced Persistent Threat" or APT refers to a cyber attack targeted at a specific entity for specific motives. It is "advanced" because it implies significant financial and technical means of action and "persistent" because it can last several years before being discovered.