ACER
Agency for the Cooperation of Energy Regulators

Session: Digital security risks to the energy infrastructure: electricity

Starting from the basics: cybersecurity awareness campaigns in the electricity and energy sector

Stefano Bracco – Stefano.BRACCO@acer.europa.eu
(Security Officer and Knowledge Manager at the Agency for the Cooperation of Energy Regulators)

Paris, 15 February 2018

A snapshot from day 1

- A reliable sector proudly closed (as an isolated ecosystem), living in its historical isolation, with a great safety tradition, aware of its core importance for the civil society, living in an age of innovation, with the need (and the obligation) to renovate under market and regulatory pressure;
- The technical angle: a strange fusion of Information Technology and Operational Technology (rarely mixed in their essence), with a clear good understanding of quality concepts;
- Risk perception was altered by the two factors before: isolation gave the feeling that the status of the energy systems could not be altered by minor contaminations;
- The financial dimension: a sector where long term investments and partially the "wild" new innovation, where not really promoted having in mind cybersecurity;
- A market where (at least in EU) a structural change can take several years to become law, and several years to become reality.

Why in energy awareness encountered a new level of complexity

- Awareness in electricity involves a plethora of actors (TSOs, DSOs, Generation, Regulators, Governments, Policy Makers, National Security Agencies, International Organizations working on Cybersecurity Standards, Law enforcement, Intelligence, International institutions an bodies, energy markets, markets operators, other actors from interconnected sectors)
- As a consequence: awareness programs in electricity involves different disciplines and skills to be provided from different angles (Law, economics, technical IT/OT, physics, engineering, diplomacy, regulatory matters, knowledge of law enforcement, forensics, intelligence, national/homeland security)
- Awareness in energy is usually cross-border (The role of ENTSO-E and, in future, of EU-DSO in the EU, cross-border agreements in non EU Member States, the role of the Federal Government in the US together with regulation at State level, and especially the challenge of Security of Supply)
- Awareness has to be omnidirectional: all actors have to make others aware of constraints, limitations, and opportunities, as well as of information (sometimes extremely sensitive or even classified).
- Awareness in electricity goes beyond the sector and involves other sectors (investors, dependencies on Gas, Oil, Nuclear, Water and others)

2 minutes of history – When awareness campaigns started

- In EU awareness campaigns on cybersecurity started as a result of risk assessments in some Member States;
- A number of attacks in other sectors made the governments conscious and aware that the risk on the Energy Sector was real, imminent, and would have materialized soon;
- The real heavy start was linked to a number of legislative actions in the US which involved cybersecurity affecting also the Energy Sector, the EU and others followed;
- The need for further awareness actions became evident after the Ukraine case in 2015, the attack in 2016 worked as a booster;
- It was just the start: Governments, Regulators, International Institutions, the Industry mobilized slowly but immediately and started preparing campaigns at any level possible (Top Management, Middle Management, Tactical, Strategic, Technical levels).
- Research and academy became supportive since the beginning. They predicted the risks and were able to provide new interesting scenarios which then became part of the further considerations.

Topics of the cybersecurity awareness for Electricity

- Cybersecurity Hygiene (then moving to existing best practices and standards – (see PPP of DoE on C2M2);
- Importance of the human factor;
- Coordination, cooperation and solidarity (value of information sharing, response to attacks and incidents in several scenarios in a coordinated manner, boosting recovery actions in the interest of the sector reputation and of the civil society);
- Focused on providing short and medium term macro-objectives, and less on pure technical matters;
- Awareness in energy focused on the few case studies, but mainly focused on making people aware the need to assess risks and make plans to respond to those possible adverse scenarios;
- Awareness in energy will further focus on Situational Awareness (perception and understanding of the topics is still quite low in some of the key stakeholders having a decisional power).

Challenges ahead

- Strengthen cooperation among all actors providing common reachable goals;
- Structuring an inclusive cybersecurity awareness strategy which will allow access to the market also to new actors, and will also promote a further level of digitalisation;
- Define an agreed and acceptable posture which can be implemented at any actor (independently from their size and posture), and provide awareness campaigns on the agreed posture as fast as possible;
- Provide a perspective on how digitilisation may help in decreasing the risks, especially if managed with proper mind set, and with an ordered approach;
- Make all actors aware of the financial implication of cybersecurity and drive them toward prudent cybersecurity investments which must balance among the need for innovation, the expectations of the market operators, of the consumers and the strategic goals of the Governments;
- Create a neutral meeting points where the electricity sector, the IT/OT (and IoT/IIoT) industry and the research can meet and find affordable solutions touching and prioritizing core important cybersecurity issues;
- Awareness helps in keeping a dialogue open, providing unavailable information, and consolidating knowledge, but especially building a solid trust within the sector and a network of people who can make cybersecurity real in a reasonable time frame when keeping risks still under control.

ACER
Agency for the Cooperation of Energy Regulators

Security of Supply

Digital security risks to the energy infrastructure: electricity

ACER
Agency for the Cooperation of Energy Regulators

Thank you!

Security, your responsibility

ACER
Agency for the Cooperation of Energy Regulators

Thank you for your attention!

www.acer.europa.eu