Report

EUTC Cybersecurity Workshop 13 November 2019

9:00-18:00, Brussels

EUTC held a Cybersecurity workshop in Paris on 13 November 2019. Modernised grids bring many benefits but may struggle to adequately protect legacy devices with useful remaining service life. The goal of this Workshop was indeed to answer several questions: *How do legacy devices survive in a cyber-threat world that did not exist when they were deployed? How do utilities retain visibility to devices of all levels of sophistication?*

This one-day workshop included discussions on compliance with the European Union's Network and Information Security (NIS) Directive, supply chain risk, case studies of utility cybersecurity deployments, and how to match the appropriate level of security to different asset types. Utilities and technology providers that need to optimize smart grid cybersecurity will especially benefit from this workshop.

Experts from following organisations actively participated to the workshop: *AS Latvenergo, ESB, Chronos, Power Networks Demonstration Center, Stratchlyde University, Virtual Access, Satellite Insight, Alliander, Wireless Innovation, Secarma, MMX, Communications Services Limited, RAD, SIEMENS, Kore Wireless, Satellite Insight, GE Industrial Communications, EDF*

All participants agreed that EUTC should continue to make efforts to ensure that the utility sector is well equipped to counter the increasing cyber threats.

On our Twitter page, you can see some updates of our day: https://twitter.com/eutcnow

Detailed report

Introduction

The increasing attack surface created by a significant increase in the number of connected devices on the grid represents a significant challenge for smart grids. Potential for significant disruption to critical national infrastructure exists if adequate consideration is not given to protection of these systems against disruptive actors. Whilst smart grids will play a crucial role in decarbonisation of the energy sector, it is imperative that we do not inadvertently reduce reliability and availability through increased vulnerability. The recognition that security in OT and IT have subtly different requirements and hence different approaches is important. The EUTC cyber security workshop explored a wide range of different topics including many which do not normally receive a great deal of attention at larger more mainstream cyber security events.

Presentations

- **Vincent Audebert & Youssef Laarouchi** *(EDF)* **–** EDF welcomed all participants to their Campus. Moreover, Mr Laarouchi gave a short overview of how EDF is dealing with cybersecurity, and why it is key important for the utility sector.
- **Tania Wallis** *(Glasgow University)* **–** Ms Wallis briefly outlined some cyber incidents including some incidents in Ukraine. Moreover, explanation on implementing the NIS Directive including efforts by OES to manage supply chains in different sectors, was given.
- **Erez Koren** *(RAD)* – Mr Koren introduced the edge computing. Automation and monitoring of sensors and systems is enabled through the IoT revolution like never before. Traditional utilities and industry verticals are affected by enabling new and advanced applications. Mr Koren explained that edge Computing-enabled platforms allows higher security for new infrastructures, at the same time seamlessly bridging such gaps.
- **Marco Bijvelds** *(Kore Wireless)* – Mr Bijvelds gave an overview of the e-sim technology. Traditional cellular connectivity solutions have inherent disadvantages that increase the cost related to connectivity significantly over the lifetime of an IoT device. eSIM addresses these concerns through remote provisioning of the SIM. Secure transfer of both data and SIM profiles is imperative to make this new technology viable for mission critical IoT applications.
- **Holly Grace Williams** *(Secarma Ltd)* – Ms Grace Williams gave an overview of Secarma's expertise and experience of dealing with cyber security protection, best practise and associated trends.
- **Kinan Ghanem** *(Power Networks Demonstration Centre)* – The cybersecurity requirements of smart grids place increasingly significant requirements for data throughput in all levels of the network. In this session, Kinan Ghanem presented current progress in a research project that examines how to handle this 'order-of-magnitude' increase in security communications throughput.
- **Patrick Conway** (*Virtual Access*) – Patrick explained how to secure legacy devices in modern networks. Even with the latest core technology and sophisticated detection capabilities, there remains a significant deployed asset base of older heavy electrical plant and RTUs that present a challenging vulnerability.
- **Maciej Goraj** *(Siemens)* – Mr Goraj gave a vision on cybersecurity from the industrial technology provider's viewpoint. Proper cybersecurity approach shall start at the equipment and software vendor itself. "Security by design" measures include end-to-end approach in vulnerability handling and disclosure process. IEC 62443 certification process guarantees own "Secure Product Development Lifecycle". To ensure

comprehensive protection of industrial plants and electrical substations from internal and external cyber-attacks, all levels must be protected simultaneously – ranging from the plant management level to the field level and from access control to copy protection. The "defense in depth" concept according to standards such as ISA99 or IEC 62443 is a cybersecurity framework that includes cyber risk assessment, implementation, management and maintenance phases.

- **Christian Farrow** *(Chronos)* – This session explored the criticality of synchronisation and solutions to ensure a trusted source is always available. The increasing importance of reliable, highly accurate time synchronisation in smart grids requires uninterruptable access to reliable time signals even in the event of failure or spoofing of one or more reference sources. Modern grids require reliable time services to operate.
- **Kay Barber** *(Satellite Insight)* – Kay Barber talked about satellite connectivity. Can satellite connectivity provider a similar level of cybersecurity to terrestrial systems? Satellite communications provide an increasingly attractive option for connectivity. Indeed, the introduction of low earth orbit constellations may be an option for low-latency services such as teleprotection.