Approach to the Cybersecurity in the energy sector of the Energy Community and Overview of EU energy related rules, standards and good practice

Blueprint Energy Solutions GmbH

Presenter:
Szabolcs Hallai - CISA, CISM, C|CISO, CITRM, C-DPO

Vienna, 11.04.2019.

About the presenter expert

Szabolcs Hallai

CISA (ISACA) – Certified Information Systems Auditor (from 2004)
CISM (ISACA) – Certified Information Security Manager (from 2005)
CITRM (IIR) – Certified IT Risk Manager (from 2007)
C|CISO (EC-Council) – Certified Chief Information Security Officer (from 2012)
C-DPO (TÜV) – Certified Data Protection Officer (from 2018)

- Chief Information Security Officer of Hungarian Energy Agency (Hungarian NRA) from 2014
- Member of CS WS (Cyber Security WorkStream) in CEER – Council of European Energy Regulators from 2014
- Member of RISIG group (Information Security) in ACER - Agency for the Cooperation of Energy Regulators from 2016
- Participated/participating in more than 25 energy security related projects (TSO/DSO/Exchange/NRA/Cyber authorities/CERT/ISAC/ENISA)

Agenda

1. Year 2018 in EU Cyber Security
2. Threat Landscape of EnC Member States
3. The model and the compliance
4. Standards and Good Practice

Year 2018 in EU Cyber Security

ENISA Threat Report

„2018 was a year that has brought significant changes in the cyberthreat landscape. Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors."

Source: ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends, FINAL VERSION 1.0 ETL 2018, JANUARY 2019

Year 2018 in EU Cyber Security

ENISA Threat Report

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

Source: ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends, FINAL VERSION 1.0 ETL 2018, JANUARY 2019

Threat Landscape of EnC Member States

Worldwide:

CNN politics 45 CONGRESS SUPREME COURT FACTS FIRST

US accuses Russia of cyberattacks on power grid

By Sophie Tatum, CNN

Updated 0257 GMT (1057 HKT) March 18, 2018

Source: CNN

US blames Russia for power grid cyberattacks 02:30

Washington (CNN) — The US government has accused Russia of remotely targeting the US power grid, as part of its newly unveiled sanctions on the country.

15 FEB 2019 INFOSEC

Electricity Grid Hacking Makes US Top Threat List

Danny Bradbury Contributing Writer

Follow @dannybradbury

US intelligence organizations have officially included hacking the electrical grid as one of the most significant threats to US national security in a report.

The *Worldwide Threat Assessment of the US Intelligence Community* is an annual document published by the US Senate Intelligence Committee. The 13th edition highlights China, Russia, Iran and North Korea as specific threats to US national security in cyberspace.

Russia and China are the greatest threats, said the report, citing their ability to disrupt US energy networks. It called out Russia's attack on the Ukrainian electrical grid in 2015 and 2016, adding that it could disrupt electrical distribution networks in the US for "at least a few hours.

"Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage," it added.

It also singled out China's ability to launch cyber-attacks that temporarily take out critical infrastructure, "such as disruption of a natural gas pipeline for days to weeks."

This isn't the first time that intelligence officials have fretted over foreign intrusion into electrical systems, and several reports have claimed that foreign nation states have already successfully compromised the US grid.

In March 2018, the Department of Homeland Security's US-CERT posted a warning about Russia targeting the electrical grid. In July, Jonathan Homer, chief of industrial control system analysis at the DHS, said that the breaches were bad enough that hackers reached utilities' control rooms and could have "thrown switches."

In 2016, Idaho National Laboratory published a damning report into electrical grid security, calling for more cooperation between the government and the energy sector to prevent attacks that could be worse than the ones in Ukraine.

In 2015, a Wall Street Journal report said that Russia, China and other countries had left

Why Not Watch?


30 MAR 2017
Every Business has the Same Security Challenge: Employees


7 APR 2016
The Five Stages of Insider Threat


19 JAN 2017
The Enemy Within: Overcoming a Company's Greatest Security Vulnerability – Its People


9 FEB 2017
Protecting Against Malicious Insiders and Targeted Attacks

Related to This Story

Govt moves to protect electricity grid from hacker

Russian Hackers Haven't Stopped Probing the US Power Grid

IDEAS SCIENCE SECURITY TRAN

LILY HAY NEWMAN SECURITY 11.28.18 02:10 PM

RUSSIAN HACKERS HAVEN'T STOPPED PROBING THE US POWER GRID

WIRED

Threat Landscape of EnC Member States

Highlights:

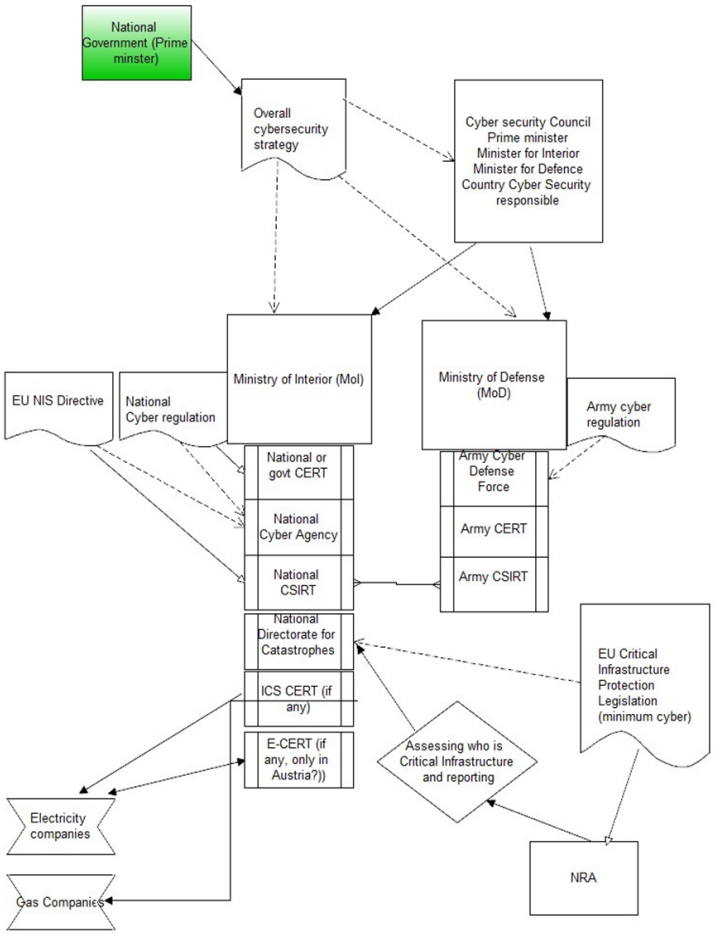
- Hybrid War / State sponsored attacks
- Standard attack patterns through APTs
- Malware/web based attack/web appliation att
- DDOS

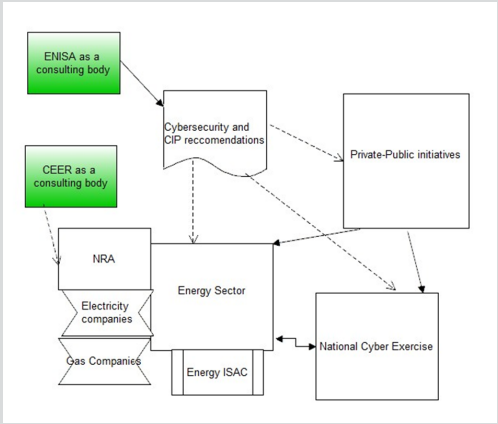
- Structural Underdevelopment
- Legal Fallback
- Territorial Disputes
- Lack of Finance
- Limited Human Resources

- NATO/OSCE Strategic Partnership – Energy Security
  Georgia, Ukraine, BiH, Serbia...

Factsheet: Energy Security, OSCE, 2 May 2017 https://www.osce.org/resources/factsheets/energy-security

The model and the compliance





The model and the compliance

EU DIRECTIVE 2008/114/EC of 8 December 2008 (CIP)

on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

- Identification of Critical Infrastructure Through Assesment
- Continuous Improvement of Protection

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

EU Directive 2016/1148 of 6 July 2016 (NIS)

concerning measures for a high common level of security of network and information systems across the Union

- Identification of Operators of Essential Services
- Country CSIRT, CSIRT Network, ENISA, Incident reporting/information sharing, National Strategy...

https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Standards and Good Practice

ENERGY EXPERT CYBER SECURITY PLATFORM

- Standardisation
- Full coverage of regulatory requirements
- Information sharing (CERT, CSIRT, ISAC)

https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

EU Commission Recommendation on Cybersecurity in Energy

Final Version 3.4.2019.!

Standards and Good Practice

EU Commission Recommendation Features

- Real-time requirements (segregation, authentication, encryption, physical security…)
- Cascading effects (from grid to grid – from country to country)
- Legacy technology combined with network of IoT devices

- Description of some recommended standards (ISO/IEC 27001/27019, IEC62443, IEC62351, ISO/IEC31000)

Questions?

BLUEPRINT energy SOLUTIONS

Thank you!

Blueprint Energy Solutions GmbH

Presenter:
Szabolcs Hallai - CISA, CISM, C|CISO, CITRM, C-DPO

Vienna, 11.04.2019.