EU activities on cybersecurity and energy

Cybersecurity Day in the Energy Community, 1 June 2021

Michaela Kollau
Directorate General for Energy
Energy Security & Safety
Policy Context

“A Union that strives for more”

President Ursula von der Leyen

A European Green Deal

An economy that works for people

Protecting our European way of life

A stronger Europe in the world

A Europe fit for the digital age

A new push for European democracy
March 2018…

US accuses Russia of cyber-attack on energy sector and imposes new sanctions

US officials say malware was found in operations of US energy companies and announce sanctions against Russia for interference

Full details on the sanctions

June 2019…

US ramps up attacks on Russian electric grid

by Alana Goodman | June 15, 2019 01:25 PM

The Pentagon is intensifying its attacks on Russian electric grid, which is seen as a part of the cyber war between the U.S. and the Kremlin.

The U.S. has infiltrated Russia’s electric power grid with American malware into the systems in response to the potential to cripple Russia’s electric infrastructure, including efforts to influence the 2018 Russian elections.

The New York Times

Although the Times provided few specifics details of the potential to cripple Russia’s electric infrastructure, its report raised concerns about the potential impact of American malware on Russia’s electric power grid.

The move is intended as a warning to Russia about the potential consequences of cyber attacks against American assets and interests.

The warning strike was authorized by U.S. Cyber Command, which has the power to conduct cyber operations in response to attacks or malicious cyber activity.

May 2021…

European power grid organization says network was hacked

The European Union’s cybersecurity agency said Tuesday that it had detected a major hack of the power grid in Europe, which disrupted electricity supply across the continent.

The hack affected at least six countries, including France, Germany, and the United Kingdom, and was believed to have been carried out by a group of cyber criminals.

The attack was the latest in a series of such incidents in recent years, with some experts warning that the threat of cyber attacks on critical infrastructure is growing.

December 2020…

Colonial Pipeline suffers extensive cyber attack

The attack resulted in the shutdown of Colonial Pipeline’s entire network, leading to fuel shortages in parts of the U.S.

The attack was reportedly carried out by a group of cyber criminals who were able to gain access to Colonial Pipeline’s systems and launch a ransomware attack.

The attack caused widespread disruptions, with some experts warning that it could have potentially been much worse.

March 2020…

European power grid organization says network was hacked

The European Union’s cybersecurity agency said Tuesday that it had detected a major hack of the power grid in Europe, which disrupted electricity supply across the continent.

The hack affected at least six countries, including France, Germany, and the United Kingdom, and was believed to have been carried out by a group of cyber criminals.

The attack was the latest in a series of such incidents in recent years, with some experts warning that the threat of cyber attacks on critical infrastructure is growing.

The attack was reportedly carried out by a group of cyber criminals who were able to gain access to Colonial Pipeline’s systems and launch a ransomware attack.

The attack caused widespread disruptions, with some experts warning that it could have potentially been much worse.
## Horizontal and energy-specific measures to date

<table>
<thead>
<tr>
<th>Year</th>
<th>Measure</th>
</tr>
</thead>
</table>
| 2019 | **Cybersecurity in EU energy**
| | Commission Recommendation (EU) 2019/553 on cybersecurity in the energy sector |
| | Electricity Regulation (EU) 2019/943 |
| | Risk Preparedness Regulation (EU) 2019/941 |
| 2020 | **Cybersecurity new EU legislative proposals**
| | Directive on the Resilience of Critical Entities (proposal) |
| | NIS 2.0* (proposal) |
| | New Cybersecurity Strategy |
| 2021 | **Formal start EU Network Code**
| | Start development Network Code for cybersecurity aspects of cross-border electricity flows |
| | Adoption planned 2022 |
| 2021 | **Review of EU gas legislation**
| | Public Consultation until June 2022 at [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12911-Revision-of-EU-rules-on-Gas](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12911-Revision-of-EU-rules-on-Gas) |
| | Proposal planned in December 2021 |
| 2021 | **Critical energy infrastructure**
| | Thematic Network of Operators of Critical Energy Infrastructure |
| | Round of Technical discussions with Member States |
| | tbc. |

* NIS 2.0: new energy subsectors, including electricity production, nominated electricity market operators, electricity market participants providing aggregation, demand response or energy storage services; district heating and cooling; oil central stockholding entities, hydrogen
Network Code on cybersecurity

• Electricity Regulation (EU) 2019/943, Article 59 (2) empowers the Commission to adopt a delegated acts supplementing this Regulation in accordance with Article 68 concerning the establishment of network codes in respective areas.

• For cybersecurity the Article 59 (2) (e) foresees sector-specific rules for cybersecurity aspects of cross-border electricity flows, on common minimum requirements, planning, monitoring, reporting and crisis management.
Furthermore, Commission Implementing Decision (EU) 2020/1479 establishes a priority list for the development of network codes and guidelines for electricity for the period from 2020 to 2023.

Article 1 of this Decision provides for the development of sector-specific rules for cybersecurity aspects of cross-border electricity flows.

Process in a nutshell:
Thank you

More info on https://ec.europa.eu/energy/topics/energy-security_en