



European
Commission



Cybersecurity EU developments

Rémi Mayet

Deputy Head of Unit - Security of Supply
EC - DG ENER

General cybersecurity legislation

Cybersecurity Strategy - 2013

NIS Directive - 2016

Cybersecurity Package - 2017

Cybersecurity Act - 2019

Cybersecurity in energy legislation

Regulation of the Security of Gas Supply - 2017

Clean Energy for all Europeans - 2019

Network Code

Risk Preparedness

Real time requirements

Cascading effect

Technology mix

Stakeholder consultations - 2018

Outcome

Information sharing

Guidance on NIS implementation

Guidance beyond NIS

Actions

Events, Workshops, EE - ISAC

Work stream 8 - NIS Cooperation Group

Commission Recommendation C(2019)2400 final

A
D
H
O
C
M
E
A
S
U
R
E
S

Commission Recommendation C(2019)2400 final

Commission Recommendation C(2019) 2400 final on cybersecurity in the energy sector

Identifies actions required to address the particularities of
the energy sector

Real-time requirements

*...simply cannot be
addressed by
standard cyber
security solutions
like authentication or
encryption.*

Cascading effects

*...can trigger black-
outs in other sectors
and countries.*

Technology mix

*...creates risks from
legacy components
designed when cyber
security was not an
issue, and from new
Internet-of-Things
devices not made
with cyber security
in mind.*

Calls Member States to ensure that the relevant stakeholders take the
necessary measures and encourage them to build up **knowledge and
skills** related to cybersecurity in energy



Commission Recommendation C(2019)2400 final

- Addresses: relevant stakeholders, energy network operators and technology suppliers, and in particular operators of essential services **via Member States**
- Monitoring: within 12 months after adoption, and every two years thereafter through the **NIS Cooperation Group**.
- Review: assessment of EC in consultation **with Member States and relevant stakeholders**.

Commission Recommendation: Not only a problem description!

Real-time requirements

- *Use international standards*
- *Apply complementary physical measures*
- *Classify/manage your assets*
- *Consider privately owned communication networks, or consider specific measures*
- *Split system into logical zones*
- *Choose secure communication and authentication*

Cascading effects

- *Evaluate interdependencies*
- *Figure out the impact of the failure of an asset*
- *Ensure communication framework for early warnings and to cooperate in crisis*
- *Ensure level of security for new devices*
- *Consider cyber-physical spill overs*
- *Establish design criteria for a resilient grid*

Technology mix

- *Follow a cybersecurity-oriented approach when connecting devices*
- *Establish monitoring and analysis capabilities*
- *Conduct specific cybersecurity risk analysis for legacy installations*
- *Collaborate with technology providers*
- *Update hard- and software*

Commission Staff working document SWD(2019) 2400 final

Commission Staff working document SWD(2019) 2400 final

- Provides **policy context** on energy, cybersecurity and critical infrastructure
- Provides more **technical details** for C(2019)2400 final
- Describes **relevant standards**, non exhaustive
- Gives an overview of relevant Commission fora, activities and expert groups

Next steps:



- ***Follow the Recommendation***
- *Consider cybersecurity in the plans of the **new EU regulation on risk preparedness***
- *Go ahead with **Network Code** on cybersecurity*
- *Look into certification of energy technologies*



European
Commission



Thank you for your attention!

