


ACER

 Agency for the Cooperation
of Energy Regulators

Cybersecurity from regulatory point of view *(With an in-depth in the REMIT Domain)*


Stefano Bracco – Stefano.BRACCO@acer.europa.eu

(Security Officer and Knowledge Manager at the Agency for the Cooperation of Energy Regulators)

Essen, 22 May 2019

1. Role of NRAs coordination and input to CSCG;
2. Specific cybersecurity requirements related to REMIT;
3. Learning from EU examples ACER/CEER.

ACER

 Agency for the Cooperation
of Energy Regulators

Cybersecurity from regulatory point of view

Role of NRAs coordination and input to CSCG

(An in-depth in the REMIT Domain)

Stefano Bracco – Stefano.BRACCO@acer.europa.eu

(Security Officer and Knowledge Manager at the Agency for the Cooperation of Energy Regulators)

Essen, 22 May 2019

Technological Advancements

- Industry 4.0
- Digitalisation
- "Smartification"
- 24/7 Connectivity
- Internet of Things
- Big Data, Smart Analytics
- Process & Computing Power
- Automation, Machine 2 Machine
- **Blockchain**
- **Artificial Intelligence**
- **Quantum Computing**
- **Advanced automations**



Increased System Complexity

- Demand/Response
- Competitive Pressure
- Multiple Market Actors
- Real-Time Operations
- Multi-Directional System
- System Balancing / Volatility
- Decentralization / Renewables
- Multiple Standards / Regulations
- **More regulations covering the same markets in a non-coherent manner**
- **Non-coordinated markets Energy Markets (Systems)**



New interdependencies and opportunities, but vulnerabilities as IT (Information Technology) and OT (Operational Technology) continue to converge and interoperate

Reality check on a cyber attack to the grid: Ukraine 2015

23 Dec 2015 h 15:35



**3 DSOs
affected**



225.000



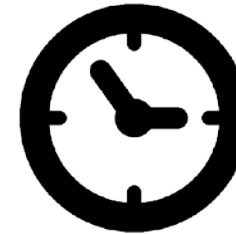
**103
Cities
and
Towns
Affected**



**135 MW
Impact**



**7 x 110 KV
SubStations
23 x 35 KV
SubStations
(up to 50)**



**3.5 to 7
hours
Outage
Duration**



**100s
Damaged**



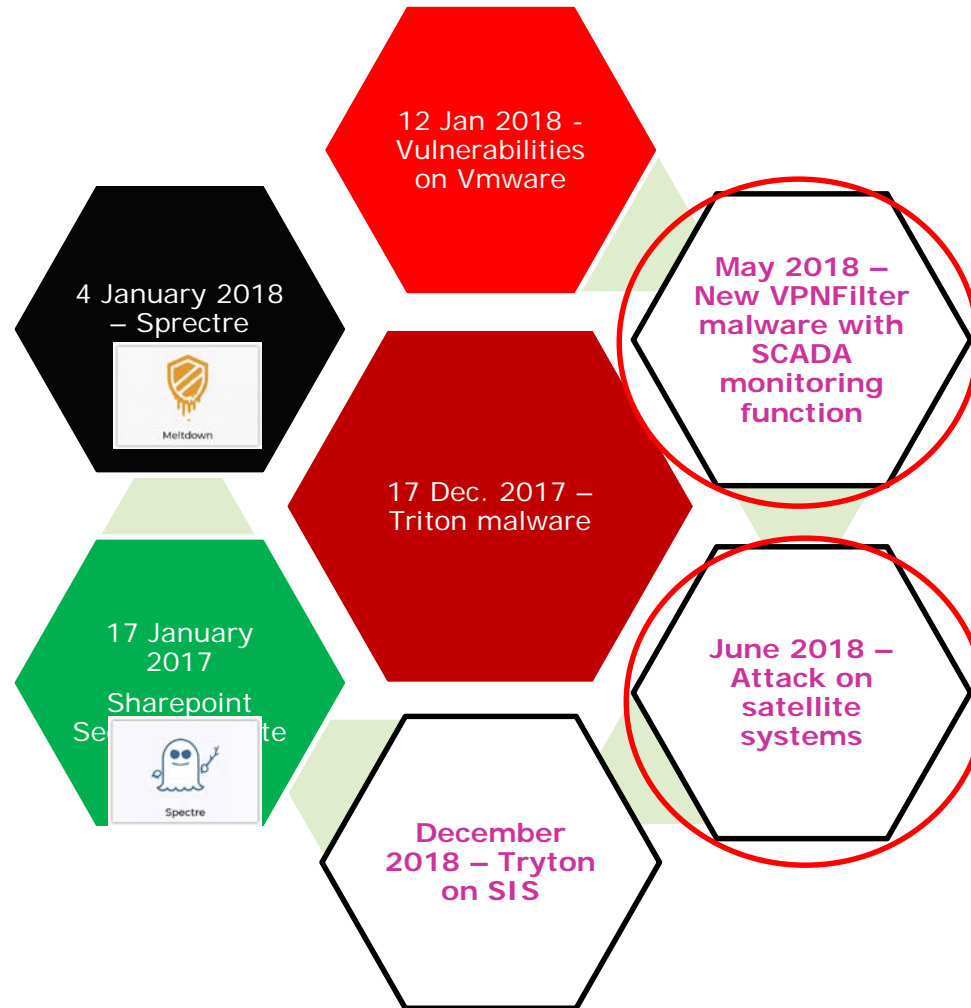
**10s Field
Device
Affectes**



**Outside
Temp.
Between
4 and
-8° Cent.**

(Source: SANS ICS - ICS.SANS.ORG)

Analysing recent threats impacting the energy sector



(23) The Agency should ensure the **operational security and protection of the data** which it receives, prevent **unauthorised access to the information kept by the Agency**, and establish procedures to ensure that the **data it collects are not misused by persons with an authorised access to them**. The Agency should also **ascertain whether those authorities which have access to the data held by the Agency are able to maintain an equally high level of security and are bound by appropriate confidentiality arrangements**. The operational security of the **IT systems** used for processing and transmitting the data therefore also needs to be ensured. For setting up an IT system that ensures the highest possible level of **data confidentiality**, the Agency should be encouraged to work closely with the European Network and Information Security Agency (ENISA). These rules should also **apply to other authorities that are entitled to access to the data for the purpose of this Regulation**.

(25)

Where information is not, or no longer, sensitive from a commercial or security viewpoint, the Agency should be able to make that information available to market participants and the wider public with a view to contributing to enhanced market knowledge. Such transparency will help build confidence in the market and foster the development of knowledge about the functioning of wholesale energy markets. The Agency should establish and make publicly available rules on how it will make that information available in a fair and transparent manner.

Article 12

Operational reliability

1. The Agency shall ensure the **confidentiality, integrity and protection** of the information received pursuant to Article 4(2) and Articles 8 and 10. The Agency shall take all necessary measures to prevent any misuse of, and unauthorised access to, the information maintained in its systems.

National regulatory authorities, competent financial authorities of the Member States, national competition authorities, ESMA and other relevant authorities shall **ensure the confidentiality, integrity and protection of the information** which they receive pursuant to **Articles 4(2), 7(2) or 8(5) or Article 10** and shall take steps to prevent any misuse of such information.

The Agency shall **identify sources of operational risk and minimise them through the development of appropriate systems, controls and procedures.**

2. Subject to Article 17, the Agency may decide to make publicly available parts of the information which it possesses, provided that commercially sensitive information on individual market participants or individual transactions or individual market places are not disclosed and cannot be inferred. The Agency shall make its commercially non-sensitive trade database available for scientific purposes, subject to confidentiality requirements. Information shall be published or made available in the interest of improving transparency of wholesale energy markets and provided it is not likely to create any distortion in competition on those energy markets. The Agency shall disseminate information in a fair manner according to transparent rules which it shall draw up and make publicly available.

NIS Directive

- Raising **resilience** through **baseline CS standards**
- Ensuring EU-wide minimum CS **capabilities** through **audits** and **penalties**
- NIS competent authorities on national and sector level
- Improving **information-sharing** and **collaboration through reporting obligations** Cross-border between the EC and MS, MS and MS, with ENISA
- Nationally between public and private stakeholders

Cybersecurity Act

- New ENISA Mandate
- Cybersecurity Certification Schemes

Clean Energy for All Europeans

- Security of the smart metering systems and their data communication (also AMI – See Norwegian example);
- Use of the best available techniques for ensuring the highest level of cybersecurity protection (especially on SGs);
- EU DSO entity responsible for ensuring data management, cyber security and data protection and participation in the elaboration of network codes;
- Network Codes on cyber security rules and rules concerning regional operational centres;
- Guarantee of security of supply against the risk of an electricity crisis also depending on malicious attacks having regard to some scenarios:
 - Simultaneous
 - Cross Border
 - At Regional Level
 - At National Level
 - All which goes beyond N-1 security criterion

General Data Protection Regulation

- All rights on protection of Customer and Citizens Data are extended to the Cyberspace




European Cyber Landscape

- Different guidelines / standards, often not energy specific, and not converging
- Sometimes unclear governance
- No clear ownership and responsibility of the issue
- **New emerging standards and old known problems (use of NIST, ISO - ISO/IEC 27019:2017 Information technology - Security techniques - Information security controls for the energy utility industry)**



ACER

 Agency for the Cooperation
of Energy Regulators

Cybersecurity from regulatory point of view

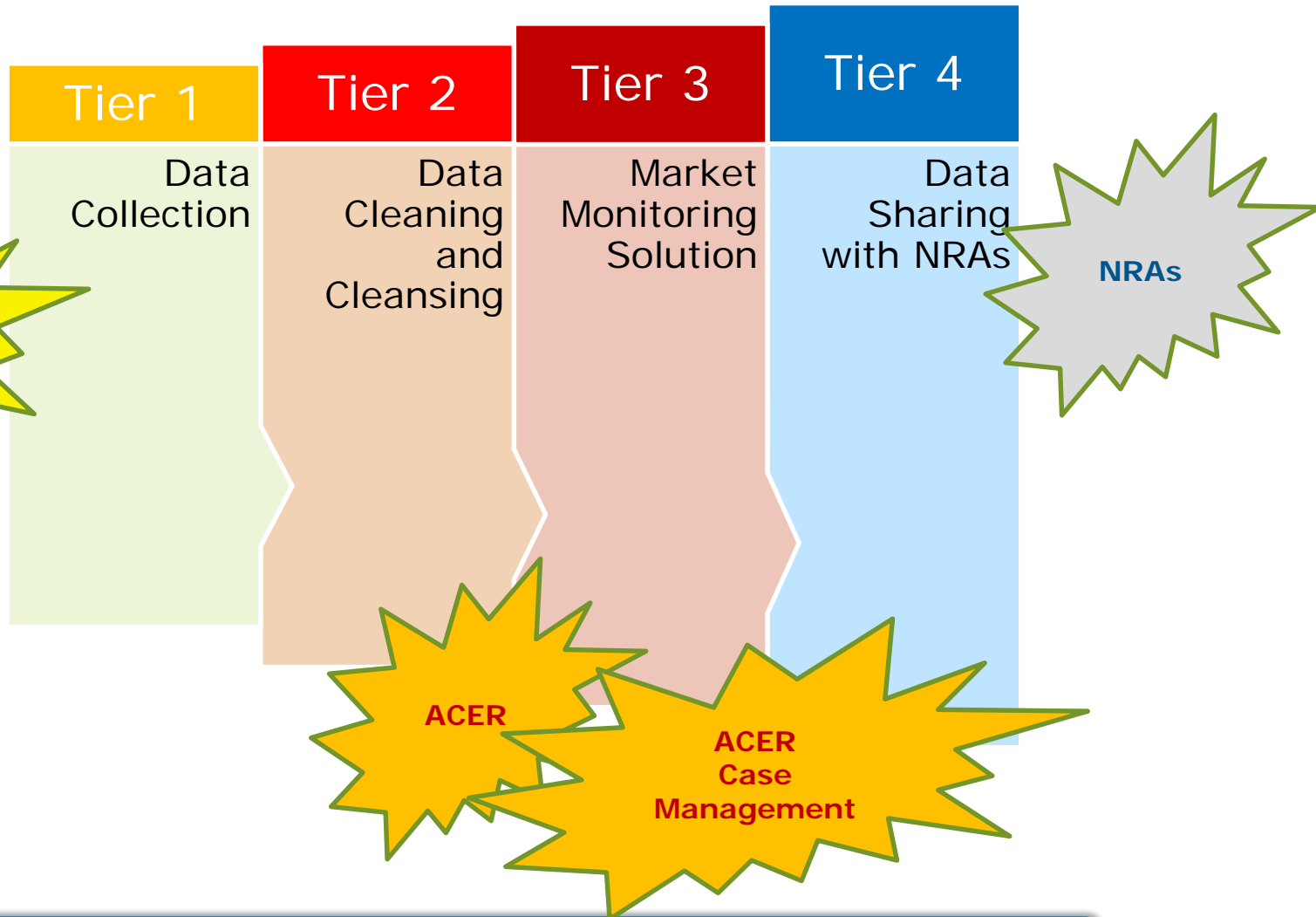
**Specific cybersecurity requirements related to
REMIT**

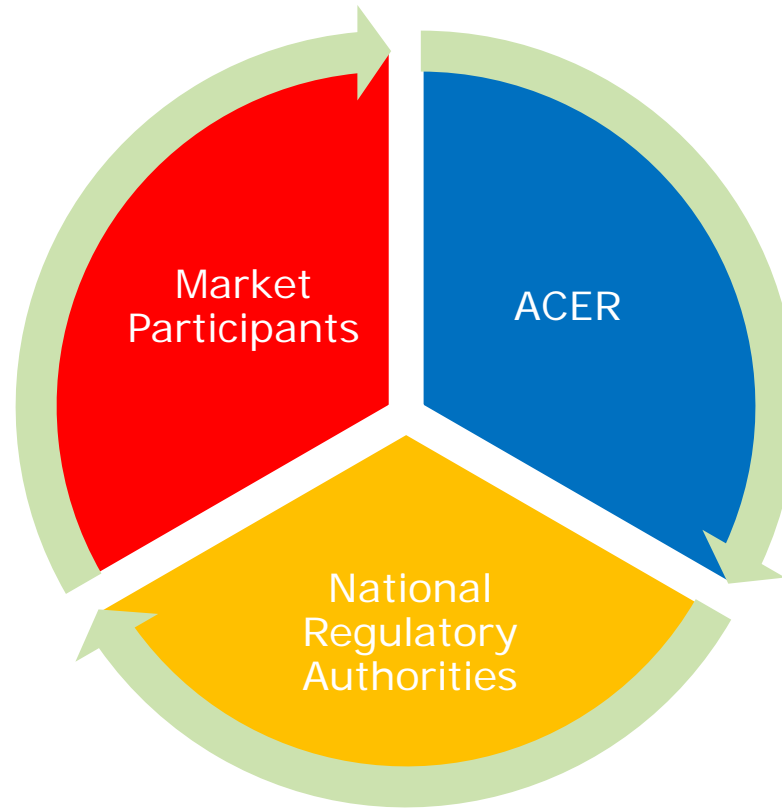
(An in-depth in the REMIT Domain)

Stefano Bracco – Stefano.BRACCO@acer.europa.eu

(Security Officer and Knowledge Manager at the Agency for the Cooperation of Energy Regulators)

Essen, 22 May 2019





Companies
and
companies
structures

Transactions
and their
history

Status of
networks

History of
all data
collection
s

Capacity
transactions

Energy
transactions

Inside
information
reports

Inside
information
reports

Contracts

Enrichment



Strategies

erse
An in-de


int of view

- 28 Member States to agree on a set of requirements
- ACER
- Need to involve ENISA
- Data received from thousands of Market Participants (RRMs or single Market Participants)
- Data received from ENTSO-E and ENTSO-G
- Fundamental, trading data and **Market Participants Registration**
- Data provided to all NRAs, other National Competent Authorities
- Anonymised data provided to Academic institutions

- **Peer review process**
 - **Minimum 5 people**
 - **All requirements documented, adopted and implemented**
 - **Information Security System shall be compliant by design**
 - **The final solution is connected only at the end of the process**
- **Case Management Tool**
 - **Fixed configuration**
 - **84 requirements out of**

- Risk Management
- Incident Management
- Exception Management
- Change Management
- Log Management
- Teleworking
- Asset Management
- Access Management
- Physical Security
- Supporting Procedures
- Service Provider Management
- Software Development Lifecycle
- Information Management
- Business Continuity Management
- Cryptography

ACER

 Agency for the Cooperation
of Energy Regulators

Cybersecurity from regulatory point of view

Learning from EU examples ACER/CEER

(An in-depth in the REMIT Domain)

Stefano Bracco – Stefano.BRACCO@acer.europa.eu

(Security Officer and Knowledge Manager at the Agency for the Cooperation of Energy Regulators)

Essen, 22 May 2019

Audience

- 8 NRAs
- 27.5% did not pass the PR
- 62.5% passed the PR

Time spent to implement REMIT CS Requirements

Average time spent:

- 10.5 months
- Minimum 7 months
- Maximum 18 months

Financial and human efforts for initiating the project

- 1 to max 10 FTEs depending on the size
- The majority had 4 people working on the project
- Spent between 30,000 and 40,000 EUR

Time spent to comply

Average time to comply:

- 19 months
- Minimum 13 months
- Maximum 28 months

Financial and human efforts to comply

- 1 to max 10 FTEs depending on the size
- Majority had 4 people working on the project
- Spent additional 5-6,000 EUR

Difficult areas to consider in regard to the process

- Scarcity of human resources
- CMT is easier to achieve for most of them

Difficult policies when drafting

- Risk Management
- Asset Management
- Change Management
- Access Management
- Exception Management
- Log Management

- Others (e.g. crypto)

Difficult policies when drafting - Reasons

- Outsourced services
- The policies will collide with the existing rules
- Technical difficulties implementing the policies afterwards
- Absence of specific policies and practices in a specific areas (e.g. Change Management)

Difficult policies when implementing

- Asset Management
- Change Management
- Access Management
- Information and information classification policy
- HR Management
- Log Management
- Incident Management

- Others (e.g. crypto)

Difficult policies when implementing - Reasons

- Outsourced services
- The policies will collide with the existing rules
- Technical difficulties implementing requested area
- Consistent reduction in the way data are shared and used within the same NRA

Difficult policies when enforcing

- Risk Management
- Asset Management
- Change Management
- Access Management
- Exception Management
- Log Management
- Cryptography

Difficult policies when enforcing - Reasons

- Restrictions are often difficult to impose and to accept;
- Sometimes there are also technical limitations which would prevent the enforcement.

Improvements suggested

- HR Management Policy
- Assets Management Policy
- We think the requirements in Log Management and Access Management related with segregation of functions need to be reviewed. There could be small organizations in which this can be not an option.
- The arrangement is extensive and it feels like the ISO certification is too in depth sometimes. The parts should all be included, however not as extensive.

Improvements suggested - Reasoning

- HR Management Policy is always according to national legislation and is not directly related to Information Security, as all the other fields.
- Requirement proposed for review: Networks shall be segregated taking into account sensitivity level and risk analysis.
- Reason for review: automatic download and storage in the same network of national collection or public data from secured website of data providers is not possible.
- Proposed change: Need a minimum internet connection through VPN

Question 1. Which information and documentation you find useful before the Peer Review?

- ACER Guidance (More information about ACER technical requirements and examples of architecture compliant with the requirements requested by the ACER.)
- ISO documents
- In general all checklists and breakdown of the ISO certification was greatly appreciated. Maybe send one document with all information needed in it to reduce the risk of missing a part. (Providing best solutions from previously approved peer Reviews with examples on what a accepted solution would be appreciated. It will greatly reduce the time spent "re-inventing" the wheel.)
- ARIS policies
- **Guidelines to submit a compliance Request to the RISIG Peer Review Panel**
- Self-Assessment
- ARIS Guidelines *.DOC + Summary Guidelines *.XLS (REMIT Information Security Policy - NRA guidelines): Measures & Controls Scenarios with Min., Max. and Suggested prescriptions.
- **Additional references/recommendations for information security sectoral minimal/good/best practices or prescriptive guidelines (as sometimes discussed at the Peer Review hearings): literature, case studies, examples of ISO/IEC typical scenarios of control implementation (e.g. excerpts from BSI like Technical Guidelines).**

Fairness of the process

- Fair process 3 out of 5;
- Do not want to answer 1 out of 5;
- **Unfair 1 out of 5.**

What to change

- “Simplified guidelines, expectations and boundaries”

What can we do to help?

- “Compile best solutions and other pre-approved processes.”

How to improve

- “As mentioned, the peer Review process could use simplified guidance and also clearer instructions in regards to what is expected.”

Strengths of the process

- “To set up the way to efficiently and securely work with data.”

Additional suggestions

- “An idea is to have people working within IT-security and such as a part of the peer Review process instead of only NRA-representatives.”
- “At the start of the peer Review process it could have been made clearer that the Peer reviewers should be supportive instead of convictive in their approach to the process.”
- The Peer Review group of NRA representatives + Lead auditor should consist of at least two (if lead auditor is available) or three out of five reviewers with Peer Review/Follow Up experience for higher consistence in the inspection process. The presence of lead auditor is in our view essential to the on-site Peer Review process. Therefore Peer Review Sessions in parallel (due to many applicants) should be rather an exception (and practiced only in case of utmost importance).

Conclusions

- Scenarios are very helpful;
- Fairness of the process and work more on instructions;
- The Peer Review group of NRA representatives + Lead auditor should consist of at least two (if lead auditor is available) or three out of five reviewers with Peer Review/Follow Up experience for higher consistence in the inspection process. The presence of lead auditor is in our view essential to the on-site Peer Review process. Therefore Peer Review Sessions in parallel (due to many applicants) should be rather an exception (and practiced only in case of utmost importance).

- **Revision of the REMIT IS Policies;**
- **Revision of the existing guidelines;**
- **Risk Assessment;**
- **Massive On-Boarding.**

Security, your responsibility

Thank you for your attention!



www.acer.europa.eu