Cybersecurity regarding HEDNO’s grid

18 January 2022

Dr Dimitrios Michalopoulos
d.michalopoulos@deddie.gr

HEDNO

- **Mission**
  - ✓ Our goal is to substantially contribute to the development of our country as well as the welfare and improvement of the citizens' quality of life in the whole territory with reliable and economically efficient power supply respecting people and environment.

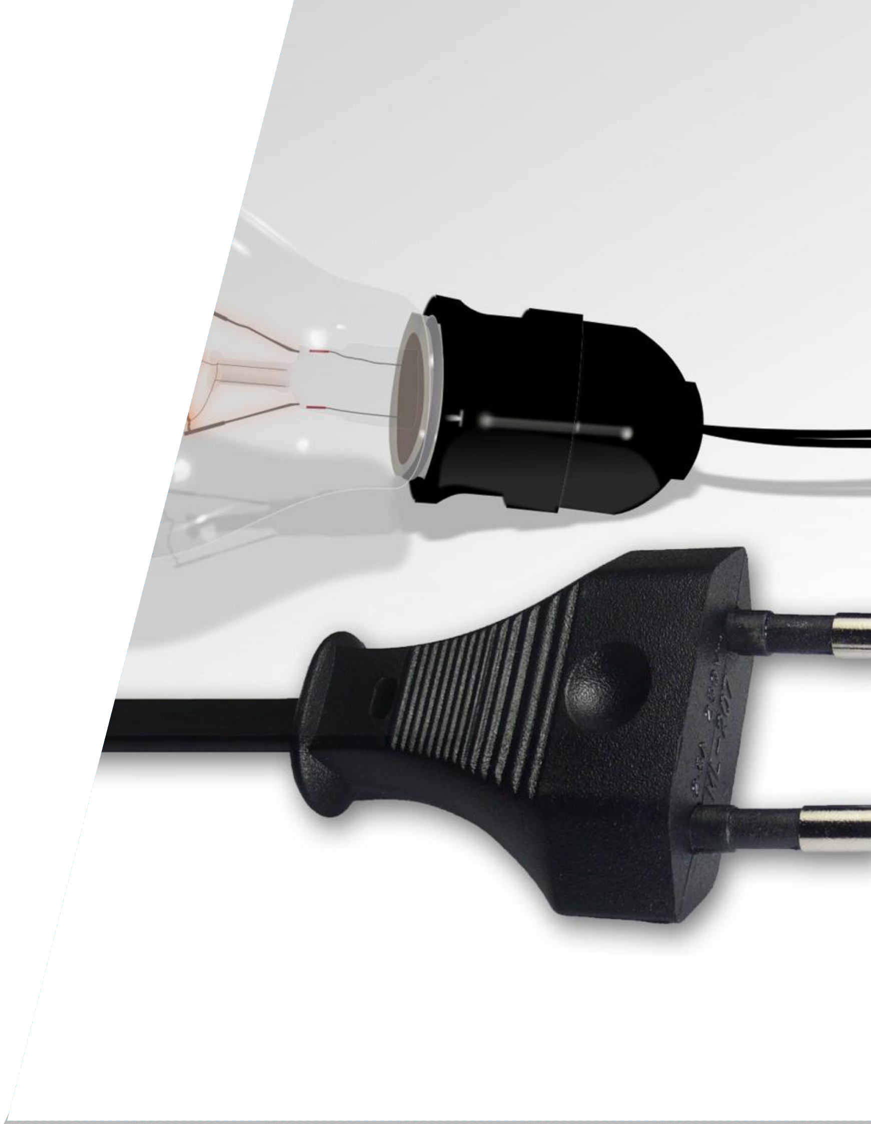
- **Goals:**
  - ✓ Energy Quality
  - ✓ Customer care quality
  - ✓ Reduction of operating costs - modernization
  - ✓ Adjustment to the requirements of the new environment

- **Organizational Structure:**
  - ✓ DATA PROTECTION & INFORMATION SECURITY DEPARTMENT
  - ✓ IT & OT environment

Regulation

- **NIS Directive – v. 4577 2018**
  - ✓ Critical services (Energy, Transportation, Banks, Health, etc)
  - ✓ National CERT
  - ✓ HEDNO (Energy Distribution)

- **National Cybersecurity Strategy**
  - ✓ National Level Risk Assessment
  - ✓ Recording of Existing Institutional Framework
  - ✓ Incident Management - contingency plan
  - ✓ Handbook



Known attacks

✓ 2010 Stuxnet (Iran)

✓ 2012 Shamoon (Saudi Arabia)

✓ 2015 BlackEnergy (Ukraine) first attack

(30 substation – 230.000 consumers – 6 hours)

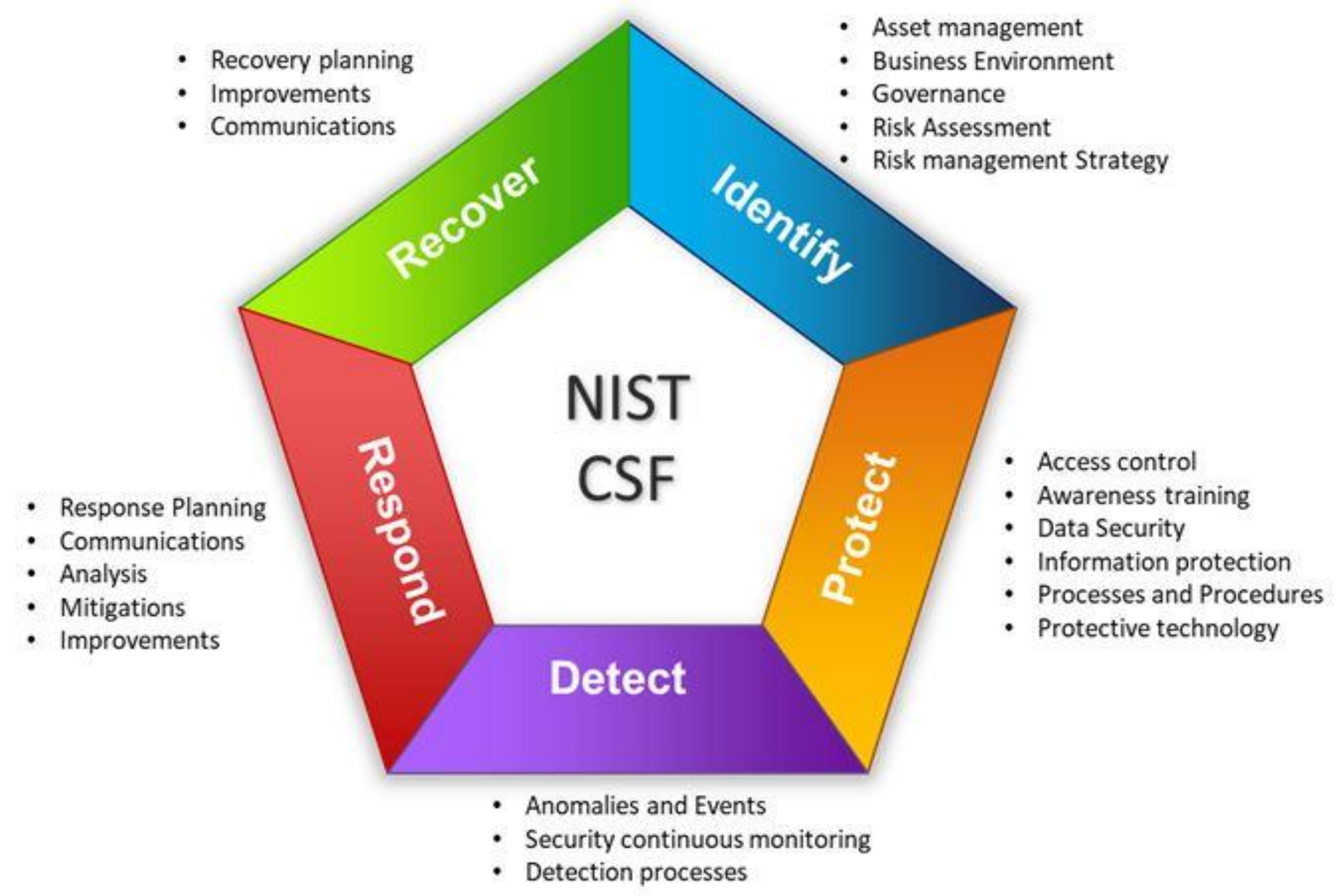
✓ 2016 BlackEnergy2 (Ukraine)

(30 substations 225.000 consumers)

✓ 2018 SamSam (Atlanta, USA)

($51.000 ransom)

Security Model (NIST)



Actions

- ✓ Effective information diffusion models - communication frameworks, internally and / or with respective companies.

- ✓ Incident response teams with clear scenarios and responsibilities. Execution of business exercises, maintaining a high degree of readiness.

Actions

- ✓ Coordination through European institutions - organizations (e.g. E.DSO) joint actions for exchange of know-how and incident management methods and techniques
- ✓ Coordination between similar companies (IPTO, PPC, Hellenic Petroleum)
- ✓ Management model with clear separation of roles and responsibilities

Actions

- ✓ ISO 27001:2013 for IT/OT infrastructure
- ✓ SOC/NOC 24-7
- ✓ Incident detection – As fast as possible
- ✓ Collaboration with relative national institutions (CSIRT) – coordination of actions
- ✓ Backup infrastructure (DR) for critical systems

Actions

- ✓ Risk Management- Risk Treatment plans
- ✓ Integradeted security policies, continuous inspections by internal and external auditors
- ✓ Detailed disaster recovery plan
- ✓ Lessons Learned after each incident

Actions

- ✓ Unified supplier / supply chain management policy
- ✓ Asset Management
- ✓ Impact mitigation actions
- ✓ Tools for monitoring, identifying possible incidents, dealing with-preventing possible incidents
- ✓ Communication person with each organization / partner

Challenges

- ✓ Large scale system integration
- ✓ Experienced and trained personnel
- ✓ ATPs and Zero-day vulnerability handling
- ✓ Digitalization of processes and procedures
- ✓ End user security – awareness
- ✓ Real time threat detection
- ✓ Geographical distribution (systems & employees)

Questions