NIS - Italian National Cyberspace Security Plan

Fondazione Don Carlo Gnocchi Onlus

NIS - Italian National Cyberspace Security Plan

- Milestones and Timeline
- Security Organization Model and Incident Reporting Platform
- Some open issues

National Cyberspace Security Plan - milestones and roadmap:

A defined perimeter: list of sensitive national structures:

- **OSE** (Core&Essential Service Operators)
- **FSD** (Digital Service Providers)

National institutions supporting IT security:

- Coordination of principal Ministries (Health, Economy, Environment, etc.)
- Department of Information Security (DIS)
- Agency for Digital Italy (AGID)
- Incident and Compromise Detection Centers (CERTs)

National Legislation revised:

- Adoption of international standards for safety management ISO 27001/31000
- Three-year plan related to public administration normative (AGID)
- Information flows to the European Community (list of structures and incidents)

National action plan and 11 operational guidelines:

- Models and security in the PA (empowerment defence/capacity, IT compliance/law, operations/resilience, comunication/education)
- Three-year IT Roadmap National and Regional development plan

NIS adoption Plan Timeline

Timeline

- **2014-2017: Italian National Cyberspace Security Plan**
  - 6 strategic milestones
  - 11 operational guidelines
- **2016: UE 2016/1148 (NIS Directive)**
- **2018: NIS adoption by law**
  - DL n.65 18/05/2018
  - Joint of national CERT: CSIRT (CERT-N (priv.) + CERT-PA (pa))
  - CSIRT under DIS Dipartment of Intelligence
- **Europen collaboration data exchange:**
  - GCoop: 9/08/2018 + 2Y
  - OSE list 9/11/2018 + 1Y
  - FSD entro 9/11/2018 + 1Y
- **30 luglio 2020 further documentation (DPCM N.131)**
  - GDPR checklist and control armonization
- **5/2020:** Started **CSIRT** exchange IOC CTI platform

Healthcare structures are «OSE» must adopt the plan, under Regional Law:

- **SECURITY ORGANIZATION** (processes, risk analysis, assets):
  - Information security organizational model
  - Information security management system
  - Continuous process of Risk Analysis Evaluation / Assessment

- **INCIDENTS REPORTING on the CERT Platform:**
  - Change IT systems to communicate relevant events in machine-to-machine mode
  - Alternative use of IOC messaging systems by client notification

Role of AGID: (former actor of the IT security coordination group)

- Defines national development IT guidelines and IT standards adoption
- Certifies the national suppliers providing essential services
- Offer support through risk tools and training course (free for PA)

Some **actual issues**:

- **SECURITY ORGANIZATION:**
  - Lack of regional asset management tools (risk, CMDB)
  - Problems in regional/National procurements guidelines to intercept needs
  - Regional CERT organization vs. CSIRT (national) processes and tasks are not already completed
  - Differences and sinergies beetween public and private guidelines
  - CSIRT (Computer Security Incident Response Team) under intelligence: creation of a national Cyber Agency

Thank you

Matteo Montesi mmontesi@dongnocchi.it

Fondazione Don Carlo Gnocchi Onlus