Creating NIS Compliant Country in a Non-Regulated Environment

Jurica Čular
(jcular@zsis.hr)

REPUBLIKA HRVATSKA
ZAVOD ZA SIGURNOST INFORMACIJSKIH SUSTAVA

What NIS actually is?

NIS Directive

- NIS – Network Information Security Directive
- EU Cyber Security Policy
- Mandatory for all EU states
- NOT Mandatory for all EU companies
- Focus on essential/critical services

Scope

- Operators of Essential Services - OES
- Digital Service Providers - DSP

OES

- Entity supplies service essential for maintaining critical social and economic activities
- Service supply fully depends on ICT
- Cyber incident would significantly impact service delivery

OES

- Energetics – electricity, oil, gas..
- Transportation – air, railway, roads, mainland
- Banking – credit institutions
- Financial markets infrastructure
- Health
- Water supply
- Digital infrastructure

DSP

- Online marketplace
- Online search engine
- Cloud computing service

Important dates

- August, 2016 – entry
- February, 2017 – CG/CN starts
- May, 2018 – transposition into local legal framework
- November, 2018 – MS to identify and report ES
- 2018 - EC control
- 2020+ - broad scope

Expectations

Member states

- Sectoral authorities
- Single POC
- Cyber strategy
- CERT

Incident reporting

- Incident reporting towards authority with „no delay” – 24-72 h from discovery

Standards

- „State-of-the-art” equipment
- „Guaranteed security level according to risk”

What transposition is?

EU Directive vs EU regulation

- EU Regulation
  - Immediately applicable and enforcable by law in all Member States
  - As good practice, Member States issue national legislation that defines the competent national authorities, inspection and sanctions on the subject matter
- EU Directive
  - Sets certain aims, requirements and concrete results that must be achieved in every Member State
  - Sets a process for it to be implemented by Member States
  - National authorities must create or adopt their legislation to meet these aims by the date specified in each given Directive

Croatia - current state of play

Croatia – current state of play

- Youngest EU member state - July 2013
- (Rather) Young country/democracy/free market
- All NIS sectors covered by law…but
- Sectoral regulation – banking and financial markets
- Water management – NO CI

How we did it?

Process

- Working Group (WG) summer 2017
- Weekly meetings, drafting, polishing
- Final draft – December 2017

Who?

- NSA
- CERT Community
- Sectoral representatives
- Regulators
- MFA

Steps

- Identify current legislation – mostly non-existent
- Develop identification criteria by sector
- Analyze current audit/CERT capacities by sector
- Identify national competent authorities (NCA)
- Develop legislation scheme
- Write the LAW
- …..

Centralized Vs. Sectoral

- Depending on current country set up
- Centralized:
  - Single organization
  - Cyber skilled setup, NCSC
- Sectoral
  - Multiple sectoral authorities
  - Dispersed management

Legislation scheme

- OES and DSP cyber security law
  - Roles
  - Deadlines
  - Criteria
  - Penalties
- Statute on cyber security measures
  - Security measures
  - Reporting procedures
- Guidelines

Criteria - challenges

- What is essential?
- Different views by each sector
- Several types of criteria:
  - Number of users
  - Unique service provider
  - Capacities
  - Market share
  - Geographic dispersity

Croatia custom design

- Sectoral approach
- „Compliance body”
- 2 CERTs
- 8th sector – „Government information infrastructure services”
  - e-Citizen
  - Business services for state budget users

Lessons learned

What could have been done better?

- Develop national regulation/legislation
- Foster (cross)sector cooperation
- Invest in NCA skills and awareness
- Start early
- Communicate
- Test

Predictions

- Scenario 1
  - Not enough power/will to conduct by new law
  - Not enough resources within key role players
  - OES not investing

- Scenario 2
  - Full implementation with deadline flexibility
  - Close cooperation with OES
  - Use of CEF funds
  - Development of strong internal cyber services market

KEEP
CALM
AND
ASK
QUESTIONS