Digital Security Authority (DSA): The way forward to a dynamic Cyber security for Cyprus

George Michaelides
Commissioner of Electronic Communications & Postal Regulation
http://www.ocenepr.org.cy
...dynamic Cyber security for Cyprus
Our Vision - Building our future

Security for all

Secure: Critical Information Infrastructures, Government, SMEs, CITIZENS

Security is a TEAM sport

Cooperation at a national level, with other CSIRTs, national authorities and academia

Approach

- Think Big
- Start Small
- Scale Fast

Fortification of critical elements of our economy such as shipping, financial services etc
Strong Cybersecurity Ecosystem

1. **Build on our expertise**
   Shipping: in merchant fleet we are 3rd in E.U and 11th world wide

2. **Engage academia**

3. **Engage private sector**

4. **Attract technology companies**

5. **With the support from the public sector**
Digital Security Authority -
International Maritime Ecosystem for Cybersecurity (IMEC)
Vision of the National Cybersecurity Strategy

“The protection of all critical information infrastructures of the state and the operation of information and communication technologies with the necessary levels of security, for the benefit of every citizen, the economy and the country”

Education – Training – Awareness – Cooperation – Trust
Revising the Strategy

- ENISA Good Practice Guides
- EU Cybersecurity Package
- Lessons Learned (from current strategy)
- CMM Evaluation Results
- National Cybersecurity Strategy 2
- Current threat / risk landscape
1. Council of Ministers decisions on the Commissioner, DSA, CSIRT-CY and critical info. infrastructures
   - Digital Security Authority, including the National CSIRT – under the supervision of the Commissioner
3. Commissioner’s Decisions on the designation of critical information infrastructures
4. Regulations on the Security of Network and Information Systems (Fees) of 2018
5. Secondary legislation on security measures will follow
6. Secondary legislation on incident notifications will follow
New Organisational Structure

Commissioner and Deputy Commissioner of Communications

- OCECPR (Regulator)
  - Electronic Communications
  - Postal Services
- Digital Security Authority (Cybersecurity)
Digital Security Authority

Operators of Essential Services (~50)

Digital Service Providers (<10)
Cloud Computing Services, Online Marketplaces, Search Engines
National CSIRT (Computer Security Incident Response Team)

“A CSIRT with national responsibility (or "National CSIRT") is a CSIRT that has been designated by a country or economy to have specific responsibilities in cyber protection for the country or economy. A National CSIRT can be inside or outside of government, but must be specifically recognized by the government as having responsibility in the country or economy.”

Source: www.cert.org
National CSIRT – Areas of activities

- Incident Monitoring
- Incident Response
- Incident Analysis
- EC awareness on incident handling process etc.

- Communication
  - Early warning, alerts, announcements, etc.
  - General awareness regarding incidents (public/media) etc.

- Incident Management
  - Cooperation with NIS Authority
  - Mutual assistance with other national CSIRTs
  - Exchange non-classified information
  - Participation in exercises etc.

- Advanced Services
  - Remote incident response and support
  - On site Incident Response/support
  - Artefact forensic analysis

- Cooperation

Office of the Commissioner of Electronic Communications & Postal Regulation
Thank you for your attention