enartia
GROUP OF BRANDS

NIS compliance, challenges and problems

Panagiotis Vavilis

GRNOG 9


enartia
GROUP OF BRANDS


papaki
HAPPY.PEOPLE.ONLINE


Top.Host
EXTREME SUPPORT


the core


magic press
by Enartia

What is the NIS?

As part of the EU Cybersecurity strategy the European Commission proposed the EU **N**etwork and **I**nformation **S**ecurity directive. The NIS Directive (see EU 2016/1148) is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU. The NIS directive was adopted in 2016 and subsequently, because it is an EU directive, every EU member state has started to adopt national legislation, which follows or 'transposes' the directive. EU directives give EU countries some level of flexibility to take into account national circumstances, for example to re-use existing organizational structures or to align with existing national legislation. The deadline for national transposition by the EU member states is 9 May 2018.

enartia
GROUP OF BRANDS

The NIS Directive has three parts:

- **National capabilities:** EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.
- **Cross-border collaboration:** Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.
- **National supervision of critical sectors:** EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, and finance sector), ex-post supervision for **critical digital service providers** (internet exchange points, domain name systems, TLD registries).

Critical digital service providers

- Internet exchanges (e.g. GR-IX)
- Domain name systems (e.g. Papaki)
- TLD registries (e.g. .gr)
- Online marketplaces
- Online search engines
- Cloud providers

enartia
GROUP OF BRANDS

Criteria (4577/2018)

- Criticality
- Wide user usage
- Wide area usage
- Wide market share
- Size of company

enartia
GROUP OF BRANDS

Specific criteria (1027/8.10.2019)

- **IXP:** daily average traffic 5G/s **or** the traffic should be the 10% of total traffic in Greece.
- **DNS:** > 1B request/day **or** 50K total registered domains **or** the 10% of the total request/day in Greece.
- **TLDs:** >50M queries/day **or** the 10% of all TLDs

enartia
GROUP OF BRANDS

Requirements

- the security of systems and facilities
- incident handling
- business continuity management
- monitoring, auditing and testing
- compliance with international standards
- CSIRT
- Incidence report

enartia
GROUP OF BRANDS

Human Resources

- DPO
- Security Officer
- Legal
- On call (CSIRT)
- Training
- Audits
- Drills

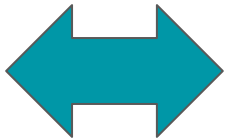
enartia
GROUP OF BRANDS

ΑΔΑΕ-ΑΠΔΠΧ-NIS

enartia
GROUP OF BRANDS

Information Security Management System (ISMS)

- Policies for
  - Accountability
  - Security awareness
  - Risk management
  - Risk treatment
  - Business continuity
  - Incidence management
  - Access control
  - Assets management



ISO 27001:2013

enartia
GROUP OF BRANDS

ELDIM

- eldim is a web server that accepts file uploads from a particular set of hosts, and its job is to encrypt them, and then store them in an OpenStack Swift backend system.
- It has a preconfigured ACL that only allows specific IP Addresses to access the file upload service. After a file is uploaded, it is encrypted with a symmetric key, and then uploaded to a configured Swift provider.

https://github.com/DaKnOb/eldim

enartia
GROUP OF BRANDS

LDAP-SSO

- Centralized user database
  - Connect applications or panels direct to ldap or via SSO
  - Use of multivalue OU attribute in order to give specific access. (e.g. ou=support, ou=vpn, ou=ssh)

enartia
GROUP OF BRANDS

Password manager

- We forced users to
  - use password manager with random long unique passwords for each entry
  - use 2FA

enartia
GROUP OF BRANDS

Bastion - Guacamole

- For the Linux systems
  a. Login to Bastion (ldap, filter attribute ou=foo)
  b. Login to destination server and record all the session
- For the Windows system
  a. Login to guacamole (ldap, filter attribute ou=bar)
  b. RDP to destination server and record all the session

enartia
GROUP OF BRANDS

Subnetting

- Vlans per department
- Intervlan firewalling
- WiFi: WPA enterprise
  a. OpenLDAP, FreeRadius
  b. General SSID dynamic VLAN assignment by Radius
- Wired: IEEE 802.1X

enartia
GROUP OF BRANDS

References

- https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements
- https://www.enisa.europa.eu/topics/nis-directive?tab=details
- https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016L1148&from=EN#d1e1767-1-1
- https://www.lawspot.gr/nomikes-plirofories/nomothesia/ypoyrgiki-apofasi-1027-8102019
- https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4577-2018-phek-199a-3-12-2018.html

enartia
GROUP OF BRANDS

Thanks!