NIS Directive (2013)

Directive concerning measures to ensure a high common level of network and information security across the Union [COM 2013 (48)]

What is it about?

Can be roughly divided in two parts

1. **Measures targeting Member States (MS)**

- Need to adopt a national NIS strategy and national NIS cooperation plan (strategic objectives, policy and regulatory measures)
- Designate a national NIS competent authority with adequate financial and human resources to prevent, handle and respond to NIS risks and incidents
- Create cooperation mechanism among Member States and the Commission to share early warnings on risks and incidents through a secure infrastructure; involvement of ENISA

2. **Measures targeting industry, in particular operators of critical infrastructures**

financial services, transport, energy, health, enablers of information society services and public administrations are required to comply with a range of requirements, ranging from mandatory security incident reporting to implementting security baseline standards;

Why is there a need for it?

According to the Commission (COM), there is a

- **Need for resilience and stability** of network and information systems for the functioning of the **internal market** (cross-border movements of goods, services and people); s**ecurity incidents** (caused by human error, malicious attacks) are increasing
- **Lack of an effective mechanism for cooperation and collaboration** and secure information sharing on incidents and risks

What are the measurers proposed?

- **Member States**: establish competent authorities for NIS / Computer Emergency Response Teams (CERTs), national strategies - some need to catch up and raise their level of national capabilities, come up to speed with regards to cyber security
- **Competent authorities** need to cooperate, exchange information; also through ENISA (European Network and Information Security Agency)
- **Companies in critical sector**s: banking, stock exchange, energy, transport, health, internet services; public administration: need to adopt measures to ensure NIS, that is:
    - Take "appropriate technical and organisational measures to manage the risks" to NIS with the aim to prevent and minimise the impact of incidents on their network and information system and the core services they provide (ensure continuity of service)
    - Notify national authorities of major security incidents that have a substantial impact (this is yet to be defined!) on the security of the core services they provide

    - The competent authority may require them to <u>inform the public</u> (if they don't choose to do it themselves) if they consider the incident of public interest

Controversial issues

- Member States (MS) do not agree upon **<u>mandatory versus voluntary</u>** approach (why legislative?): BE or PL for minimum harmonisation of cybersecurity policies, UK for voluntary; DE and UK for looser cooperation and step by step cooperation (the reason being "trust": i.e. sharing and exchanging is more likely when it's voluntary than when mandatory; law enforcement differs across MS)
- **<u>Scope</u>**: European Parliament (EP) wanted to *exclude* Information Society services and "internet enablers" (domain name registries, internet exchange points, etc.), the Italian presidency wants to revisit the Commission proposal entirely; apparently IE, DE, BE and ES want TLDs to be covered

Why is it relevant for ccTLDs?

- **<u>Scope</u>**: Risk that domain name registries will be explicitly included in the scope of the draft (this has not been the case in the original COM proposal)
    - Should domain name registries be included, there is no clarity on the criteria being used with implications on enforcement: location? Only the officially designated ccTLDs included?
- **<u>Unfair competition</u>**:
    - EU business vs. businesses outside the EU (e.g. EU ccTLDs vs. .com): European businesses will be regulated whereas the scope of the directive will not cover US-based competitors; not taking into account that any top level domain can be operated from anywhere in the world; sometimes a TLD registry outsources the running of the TLD to another country; those located outside the EU will not have the compliance costs
    - Officially designated ccTLDs versus new geographic TLDs (e.g. .wales): ccTLDs would be regulated vs. geoTLDs that would not?
- **<u>Lack of understanding of the European domain name industry</u>**: one-size fits all approach, whereas the industry is very diverse (adverse effects especially on small and medium sized businesses); some are for-profit, others are not; some are in the private sectors, some in the public sector; different levels of commercialisation
- **<u>Effects on the registrars</u>**: if you want to regulate .com within the EU, you would have to go to the registrars; (costly) requirements could lead to market consolidation and few big, powerful registrars
- **Risk that once the domain name system** is included in one piece of legislation, it will be in any that is going to follow

<u>The objective is therefore</u>: Keep ccTLDs out of the scope of the directive (Council list, i.e. Annex 2)

Timing

- COM proposal published in February 2013 (together with European Cybersecurity Strategy)
- EP: from July 2013 till March 2014
- Council: June 2013 till now
    - Working party on telecommunications and information society (to discuss Italian presidency text) 11/09/2014
    - Working party on telecommunications and information society (to discuss NIS directive) 18/09/2014
    - COREPER meeting: First or second week of October 2014 (tbc)
    - ITA presidency will try to reach political agreement before the end of their term and to obtain a mandate to start trialogue (potentially by end Oct/beginning of Nov) without the need to go through

2nd reading at EP first (responsible committee and rapporteur seem to have remained; IMCO/ Schwab)

- Telecommunications Council Meeting: 27/11/2014

What has been done so far?

CENTR position paper on the draft (November 2013)

- Impact especially on SMEs, i.e. requirements (e.g. security auditing) can be too burdensome and disproportionate
- Focus on capacity building and trust

Nominet activities

- Very active vis-à-vis MEPs and Council representatives; good collaboration with national government

What can we still do? How can you help?

Get in touch with your governments and tell the story

- Make sure we remain constructive: we do support the overall objective to increase the level of cyber security within the EU; we do think that it is necessary to raise awareness of cyber security threats and the need to act, especially in MS that have less developed infrastructure

CENTR will try to “put a figure” on the costs of implementation of the directive on ccTLDs (i.e. additional security requirements and incident notification (s.a. Art. 14 of the proposal)

- *Should you have data on the costs of implementation of CERTs or CSIRTs and/or audit requirements (if possible even on the basis of extra cost per domain name), please let us know: it would be very valuable to share this data across the community and present reliable data to the Commission, EP and Council*