

OH DEAR - ANOTHER ONE!

- What is NIS? Why?
- What does NIS mean?
- Who's affected and how?
- How the directive is being applied in the UK

DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS

- EU Directive 2016/1148
- Aims to improve cybersecurity across the EU
- Approved in 2016
 - To be enacted in national law by May 2018
 - Identify operators of essential services by Nov 2018

HIGH LEVEL PRINCIPLES

- Define/establish a competent NIS authority or authorities
 - Discrete ones for each sector?
- Provide response teams to share information about risks, early warnings, cooperate on incident handling, etc.
 - Reporting regimes, incident notifications
- Fines for non-compliance and/or serious outages
 - Up to 4% of **global** annual turnover (worst case)

GENERAL APPROACH

- Light-touch and reactive supervision
- Co-operation with law enforcement and other authorities (nationally and across the EU)
 - Facilitated by ENISA and European Cybercrime Centre
- Jurisdiction determined by where providers have their main establishment in the EU

SINGLE POINT OF CONTACT

- The SPOC deals with cross-border cooperation & coordination issues
- National SPOC gets reports from Competent Authorities (e.g. appropriate regulator or CSIRT)
- SPOC might interact with a Cooperation Group which consists of member states, ENISA and the EU Commission

ESSENTIAL SERVICES COVERED BY NIS DIRECTIVE

- The obvious usual suspects:
 - Transport, electricity supply, oil & gas, health care, banking & financial markets, water
- Digital Infrastructure:
 - “Important” IXPs, TLD registries & DNS providers
 - Cloud computing providers, search engines & online marketplaces
- Small and micro enterprises are exempt:
 - Less than 50 staff or a turnover below €10M/year

SIGNIFICANT INCIDENTS FOR DIGITAL INFRASTRUCTURE

- Must be reported to CSIRT and/or Competent Authority:
 - Risk to public safety/security or loss of life
 - Loss of service for 5M+ user-hours
 - Data loss or breach affecting 100,000+ users
 - Damage to at least one user costing €1M or more

UK APPROACH

- Government consultation in 2017
 - Defined thresholds - average query/traffic rates
 - DNS & IXP operators to be overseen by Ofcom, the telecommunications regulator
 - Internet is expressly **not** regulated in the UK
 - Ofcom decides who are Operators of Essential Services
- Information Commissioner's Office to deal with search, cloud computing and online marketplaces

DNS THRESHOLDS

- TLDs that average 2B+ DNS queries/day
- Authoritative DNS providers hosting 250,000+ domains
- Recursive DNS services handling 2M+ queries/day from UK IP addresses
- Ofcom has wiggle room to define other OESes
 - Might need to use that

THRESHOLDS AS METRICS

- Not unreasonable starting point, but...
 - Hard to accurately & independently measure because of cacheing, referrals, anycasting, access to query streams, etc.
 - Lack of qualitative assessment leaves awkward gaps
 - **.scot** or **.london** might be important even though they don't get enough DNS queries
 - BBC only hosts ~100 domains and some of them **really** matter: e.g. **bbc.co.uk**, **bbc.com**

IMPLEMENTATION ISSUES

- Are important overseas TLDs in or out of scope?
- Should anycast DNS providers be included or not?
- Do registrars who park zillions of unused domains matter?
- What about small registrars who handle domains for Fortune500 or Alexa top 100 web sites?
- Independent monitoring or rely on self-reporting?

NIS ELSEWHERE

- Other EU member states following a similar approach but some details might be different
 - Comms regulator probably gets oversight of DNS
 - National cybersecurity organisations get some sort of hands-on or advisory role
- Legislation & consultations still under way or pending in some EU member states

QUESTIONS & COMMENT