RIPE NCC

RIPE NETWORK COORDINATION CENTRE

Initial Impact Analysis of NIS 2

Marco Hogewoning | 9 March 2020 | RIPE Cooperation WG

Overview of NIS Directive

- The Directive on security of network information systems (NIS) came into force in 2018
    - "The first European cybersecurity law"
- Aims to protect critical infrastructure and the ICTs they rely on
    - The big five: health, energy, finance, transport, telecoms
- The Internet industry is part of the scope
    - In particular, the domain name system (DNS) and Internet exchange points (IXPs)
    - Recognised the potential for cascading effects into other sectors
- Directive means it has to be transposed in national laws

Revising NIS: Problem Space

- Many definitions under NIS are not all that clear
  - What exactly is an “Internet exchange” or “DNS service provider”?
  - Thresholds for criticality are not universal and depend on the market
  - No unified framework for implementation across countries
- Differences in national legislation and implementation
  - Member states had to identify Operators of Essential Services (OES)
  - Based on different requirements and thresholds
  - Implementation and regulatory regime is a national matter
- Many operators and providers operate across borders

NIS 2: Key Changes

- New attempt at definitions
  - Fixed list of operators and services that are in scope
  - Member states no longer required to select OES; already done for them
- Repeals parts of the European Electronic Communications Code
  - EECC only came into force in December 2020
  - Moves the security parts to NIS 2
- Two-tier system between operators and services in scope
  - Essential: extensive *ex-ante* and *ex-post* regulatory regime
  - Important: more lightweight and *ex-post* only regime

NIS 2: Expanded Scope

- Definition and scope of DNS services is much broader
  - All ccTLD and gTLD operators are in scope (not just the main ccTLD)
  - Explicit about inclusion of the DNS root server operators
  - Strong hints that other authoritative DNS servers are in scope
- DNS registration and whois services
  - Collect, maintain and publish accurate and complete registration data (non-PII)
  - Personal data to be made available to competent authorities upon request
- SMEs and microenterprises
  - Defined exemptions under which micro and small enterprises fall within scope (e.g. DNS service providers)

NIS 2: Potential Impact

- Implementation is fairly open
  - Exact requirements and compliance to be defined
- High-level framework, including enforcement:
  - Management is personally liable
  - Management has to be trained in cybersecurity
  - Mandatory notification of security incidents within 24 hours
  - Mandatory reporting (post-mortem) on incidents within one month
  - Requirements could involve the supply-chain (EU cybersecurity toolbox)
- Fines for non-compliance up to 2% of revenue or €10M

Extra-territorial Aspects

- NIS 2 proposal follows the now familiar format:
  - In scope if you deliver services aimed at or within the European Union
  - Regardless of where you are based or are legally established
- Entities from outside the EU who are in scope:
  - Required to designate a legal representative within one of the EU member states
  - Fall under the jurisdiction of the member state where that representative is based

Our View

Perspective of RIPE NCC operations

Our Main Concern

- The definitions of DNS will put us under scope
  - Not surprised
- We have concerns with including the DNS root
  - Majority of our own root servers (K-root) are outside the EU
  - Majority of servers in the EU are operated by non-EU entities
- Could be seen as “reverting parts of the IANA transition”
  - Large impact that could alter global relations regarding the DNS
  - Could bring us into scope of national legislation elsewhere
  - Could damage the multistakeholder model

Impact on RIPE NCC Services

- Scope and implementation of NIS 2 remains unclear
  - Could bring other services into scope
- Have some trust in the original assessment behind NIS
  - Discussions with the Dutch competent authority
- Impact of downtime and disruption at the RIPE NCC is limited
  - In particular, no immediate cascading effects expected
  - Packets don’t flow through our network
  - Routing should be fail safe!
- Trust these previous assessments are still valid

Back to You

What does it mean for your operations?

Do Your Own Assessment

- We highly recommend reading the full text of the proposal
  - Work with your lawyers and compliance colleagues in assessing the scope
  - Pay attention to details such as exceptions or explicit inclusions
- A separate proposal contains the annexes
  - These are the lists of essential and important services and entities
- If something is unclear, ask!
  - Contact the relevant competent authority or your government
  - Better to get clarity on definitions before the text is final
  - Text is very likely to change in negotiations

Keep an Eye Out for EECC Changes

- If your services are defined as an Electronic Communication Service (ECS) or Electronic Communication Network (ECN)
  - But also when you are not defined as ECN or ECS
- All of "telecoms" would fall under one directive (NIS 2)
  - Expect a change in competent authority and compliance framework
  - Depending on national law, could alter the legal basis and framework
- Definitions are slightly different
  - You have to consider again whether you are in scope
  - In particular on the ECS, NIS 2 casts a much wider net

Questions

marcoh@ripe.net