RIPE NCC
RIPE NETWORK COORDINATION CENTRE

The EU Cyber Resilience Act

Feedback provided by the RIPE NCC

Bastiaan Goslings | 26 January 2023 | Roundtable Meeting

The Cyber Resilience Act proposal

- Initial aim to cover connected “Internet of Things” devices > scope broadened significantly
- Mandatory cybersecurity requirements for “products with digital elements” throughout their lifecycle
- Increases the responsibility of *manufacturers*
  - Provide security support and software updates to address identified vulnerabilities
  - Provide *consumers* with information about the security of the products they use

https://t.ly/JjdY

Feedback requested by EC

- RIPE NCC submitted a response:
  - What does this mean, in terms of scope, definitions, necessity & proportionality?
  - How does it affect RIPE NCC services and infrastructure?
  - What are the concerns within the RIPE community at large?

https://t.ly/upBI

Good intentions

- Improve cybersecurity in the EU
- Harmonisation and legal clarity for manufactures when placing products on the EU market
- Risk-based approach
- Security-by-design principle
- Clear information for users

Scope creep

- “Products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network”
  - What does this mean?
  - “Software as a service” is explicitly out of scope, covered by NIS2 > but what about e.g. a customer portal?
  - If any software available and to be used online is covered, that massively expands the scope…

Impact on the RIPE NCC

- RIPE Atlas probes and anchors appear to be in scope > but not in the critical classes (Annex III)
- The compliance requirements from Annex I seem reasonable, based on industry best practices, but…

Clarity needed

- Products already on the market before the CRA only in scope (besides reporting obligation) when subject to *substantial modifications*
  - What exactly does that mean?
- The “software bill of materials” a manufacturer is mandated to draw up covers “at the very least the top-level dependencies of the product”
  - Need further clarity on how far manufacturers are expected to go
  - The Commission “may specify the format and elements” (art. 10.15)

Incident and vulnerability reporting

- Article 11 sets out reporting requirements for manufacturers to notify to ENISA
  - Any vulnerability that is actively exploited
  - Any incident having impact on the security of the product
  - Within 24 hours
- We think the required response and response time should be proportional to the risk/impact

Source code publishing

- We publish source code for several of our products like RIPE Atlas and Resource Public Key Infrastructure (RPKI)
  - For transparency and research/review purposes, to increase trust
  - Not made available for distribution or use as an independent product
- Further clarity needed on “the course of a commercial activity”
  - How does this relate to the RIPE NCC’s reasons, as a not-for-profit organisation providing services for the good of the Internet, to publish source code?

Questions ?

bgoslings@ripe.net

RIPE Community Feedback on the CRA Proposal

Difficult for small entities

- Small organisations will have difficulties to get certified
- This might drive them out of the (EU) market
- Favours large companies and centralisation
- Often open-source SW developers are not even an SME or even a legal entity
- Might reduce availability of open-source SW in Europe

What is “commercial activity”?

- Community welcomes exception for open-source SW
- But is unsure about the meaning of: “developed outside the course of commercial activities”
- Often open-source SW developers don’t charge for SW, but for support
- Internet relies heavily on open-source SW, small and large

Collaboration

- RIPE community is a great source of expertise
  - large, small, commercial, not-for profit
  - all aspects of Internet technology
- Long tradition of collaboration and knowledge sharing

RIPE DNS BCP Task Force

RIPE DNS Resolver Best Current Practices

- Measurements show that most users use their ISP's DNS resolver
- Concern that large open DNS resolvers will become central point of operations
- Common set of operational practices
- Make use of the expertise of the RIPE community
- RIPE Task Force will publish a set of best current practices
- Useful guidance for DNS4EU initiative

RIPE

Discussion: CRA / DNS / Sender Pays…