RIPE NCC Response to the *Cyber resilience act – new cybersecurity rules for digital products and ancillary services*

23/1/2023

The RIPE NCC welcomes the European Commission's efforts to further harmonise and improve cybersecurity in the Europe Union by setting essential cybersecurity requirements for all products with digital elements that are placed on the EU market.

In particular, we appreciate the risk-based approach in the proposed Cyber Resilience Act (CRA), which we believe will help ensure that lower-risk products are subject to minimal requirements and fewer mandatory compliance checks compared to higher risk or "critical" products. We also support the proposal's cybersecurity-by-design approach, as well as the obligation for manufacturers and other relevant operators to provide end users with clear and understandable information about their products with digital elements. Manufacturers, distributors and other relevant operators can benefit from the legal clarity and certainty created by avoiding fragmentation on the topic between different Member States within the EU's single market.

Further Clarification Required

However, the RIPE NCC believes that the current proposal leaves several important questions unanswered, and that further clarification is needed in a number of places in order to provide legal certainty for all stakeholders. Depending on the precise definitions that are currently missing, some of the requirements and obligations may not be practical, or even feasible, for certain (if not all) manufacturers of products with digital elements.

It is our understanding that the CRA intends to cover any software and hardware product, and its remote data processing solutions, that is connected to the Internet (either logically or physically) and which is placed on the market as an independent product to be distributed for end use. In other words, it is our understanding that software that is connected to the Internet but is not placed on the market as a product with the aim to be distributed to end users — such as, for example, a customer portal — would not fall under the scope of the CRA.

However, the proposal is not explicit about this point, and further clarity is therefore needed. Extending the scope to any software that is made available online would massively expand the scope of the regulation, creating administrative and compliance overburden for the economic operators involved — particularly to those smaller enterprises that may struggle disproportionately with the financial costs and resource allocation required to maintain compliance.

Similarly, the obligation on manufacturers to create a software bill of materials (SBOM) to ensure not only the cybersecurity of the products they develop, but also of the products that are built on top of those products, can become overly burdensome. This obligation therefore also requires further clarification as to the extent to which manufacturers will be expected to go when developing the SBOM. In many cases, it may not be feasible for the manufacturer

to be required to include technical information of the entire supply chain and all software dependencies. We note with appreciation the text in Annex I 2.1 that states the manufacturer will be responsible for "covering at the very least the top-level dependencies of the product" and urge the European Commission, as it develops the specifications for the SBOM, to keep the scope to a reasonable level.

Another question arises around the proposal's transitional provisions, which stipulate that products already on the market before the CRA comes into effect will only be subject to the reporting obligations described in Article 11, unless these products are "substantially modified" in their design or intended purpose. Further clarity is again needed around what "substantially modified" means. For example, if a software product is updated in order to provide additional functions, would this qualify as having been substantially modified?

Impact on the RIPE NCC

Looking specifically at the impact this proposal will have on the RIPE NCC's own operations, it is our interpretation that RIPE Atlas probes and anchors would fall within scope, but that they would not be considered "critical products". RIPE Atlas is a global network of software and hardware devices that measure Internet connectivity and reachability, providing a view of the health of the Internet in real time from more than 11,000 vantage points all over the world.[1] Volunteers place these probes/anchors within their own networks in order to perform measurements for the benefit of network operators and the wider Internet community. The RIPE NCC makes this data publicly available.

The RIPE NCC already performs security checks on RIPE Atlas software and hardware probes and anchors, and takes the issue of security very seriously; however, the current proposal would likely add additional requirements in order to ensure compliance. Although many of the proposal's stated requirements appear reasonable, there are a number of instances in which we require further clarity. We have concerns about the reporting requirements for actively exploited vulnerabilities and incidents impacting a product's security stated in Article 11, specifically around the time frame of "within 24 hours of becoming aware of it" and the lack of definition around what constitutes an "exploited vulnerability" and an "incident having impact on the security of the product". We would urge the European Commission to adopt a framework that is already commonly used and understood by the security community, such as the Common Vulnerability Scoring System (CVSS). This will be crucial to ensuring reporting harmonisation across Member States and to keep ENISA, Member States and market surveillance authorities from overcompliance and becoming completely overburdened by an enormous number of reports of low-impact vulnerabilities and incidents.

We are also concerned about the lack of distinction between lower and higher security risks and impact. This is an important distinction because we believe it's important that the required response, including the required response times, should be proportional to the risk/impact of the vulnerability/incident. As we understand the current proposal, the reporting obligations are the same for all exploited vulnerabilities/incidents, regardless of their severity and potential impact, and expects that corrective or mitigating actions will be taken or that an incident will have been investigated within 24 hours. Whereas this may be proportional for high-impact or critical vulnerabilities and incidents, we do not believe it is proportional for medium-impact and low-impact incidents. Even when dealing with high-risk exploited vulnerabilities and high-impact incidents, it is our view that security teams should divert all their resources to fixing the vulnerability or mitigating the impact of an incident, and that the 24-hour requirement may be too short even in some severe cases. The proposal also assumes that organisations have 24/7 support available to triage vulnerabilities/incidents.

[1] https://atlas.ripe.net/landing/about/

This will simply be unfeasible for all but the largest organisations; the RIPE NCC would certainly struggle to meet this requirement.

Another aspect we looked at during our impact analysis is the fact that we publish the source code for several products/services, under various public licences, via repositories such as GitHub. This includes source code related to RIPE Atlas[2] as well as Resource Public Key Infrastructure (RPKI), a security framework that helps network operators make more secure routing decisions. We do so because the technical community that uses these products/services is often interested in reviewing the source code to assess the methodology used, for research purposes or because they strongly support the use of open-source code. Because this source code is not made available with the intention to be distributed as an independent product for end users, and we publish it outside our standard business context/activities as a Regional Internet Registry, it is our understanding that it would not fall within the scope of the CRA. However, we believe that clarity is required with respect to what may constitute commercial activity and whether the RIPE NCC, as a not-for-profit organisation providing services for the good of the Internet, would fall under scope for providing this source code for those purposes.

RIPE Community Concerns

In addition to the above analysis regarding the CRA's impact on our own operations, we would like to note several broader concerns that have been discussed within the RIPE community. We do so in our role as secretariat for RIPE, which is an open, inclusive community that welcomes the participation of anyone with an interest in IP-based networking. It is this community that develops policies around the allocation and distribution of Internet number resources (IP addresses and Autonomous Systems) within the RIPE NCC's service region of Europe, the Middle East and parts of Central Asia, and it is the role of the RIPE NCC to implement these policies, which are developed via a consensus-based, multistakeholder approach.

As such, we feel it is important to highlight some of the feedback we've heard from the RIPE community at recent RIPE Meetings and on various RIPE mailing lists regarding the potential impact the CRA could have on the open-source community and the development of open-source software and services that play an essential role in the functioning of the open, global Internet and of a resilient and innovative Internet ecosystem within Europe.

While the European technical community has welcomed the exception for open-source software provided by the proposed text, the exemption applies only to open-source software that is "developed or supplied outside the course of a commercial activity". This wording leaves a lot of room for interpretation as to what, precisely, constitutes commercial activity, especially when taking into consideration the fact that charging for technical support services is considered commercial activity, as is the monetisation of other services provided via a software-sharing platform.

The RIPE community has pointed out that open-source developers often don't work for an established organisation and are not paid for their efforts in developing software, but may well earn money by contributing support services. As such, the CRA could place undue burden on these developers, who often contribute to open-source projects as a hobby and for the good of the Internet, and who will simply be unable to follow and comply with complex regulatory measures. Alternatively, several not-for-profit organisations contribute open-source software that is widely used by technical operators around the world, yet the definition of commercial activity makes it unclear whether these organisations would be

[2] https://atlas.ripe.net/docs/tools-and-code/probe-source-code.html

exempt from the CRA or would fall under scope depending on how their software development is funded, whether via a membership, sponsorship, donations or other means.

We've also heard feedback that further clarity is needed around other terms used in the CRA, including who can be considered a product's "manufacturer" and who can be considered the party who places a product on the market. These terms, as they currently stand, are not always congruent with the way in which open-source software is commonly developed and distributed. Often, open-source software is not developed as a product to be placed on the market but is published to a repository, in a similar fashion to content being published in a technical or scientific journal, for example. Introduction to the market may follow, but at the initiative of a "downstream" party independent of the developer (or author) who sees advantage in using the software as a component in their own commercial product. Matching the reality of such a supply chain to the product/manufacturer model on which the CRA is based poses a challenge, with further clarity needed on such questions.

In addition, the community feels it is important to ensure that the emphasis is placed not on the type of licence via which software is distributed or used, but on the purpose and scope of its use. For example, a large bank should be subject to stricter security obligations in using an open-source password manager than should an individual running a personal website.

Another concern is that, while larger organisations will be able to afford certification and compliance, smaller players may well be priced out of the market, thereby decreasing competition and innovation — which would move the EU further away from its stated goals, rather than help achieve them. Open-source software developers may simply decide that the cost of compliance within the EU is too high or that the lack of legal clarity is not worth the hassle, which could lead them to placing geographical restrictions on their products. While this may result in better harmonisation within the EU, it would also reduce the overall availability of open-source software within the EU and would create a more fractured global landscape, which would again be counter to the EU's ambitions and its recognition of the important role that open-source software development plays in furthering innovation and supporting Internet development.[3]

Finally, RIPE community members pointed out that the current open-source ecosystem is a complex one in which there is often no clear distinction between commercial and non-commercial products, as product development is an ongoing process that builds upon itself with designs, technologies, standards and code being shared in myriad ways for myriad purposes. This rich interplay and open access are the very features of the open-source ecosystem that allow for innovation — and which strengthen resilience and security.

For these reasons, we would urge the European Commission, on behalf of the RIPE community, to further clarify what is meant by "the course of a commercial activity", who will be considered the "manufacturer" and who will be deemed to be responsible for placing software and products on the market — and to do so with the aim of encouraging and strengthening open-source developers and the existing open-source ecosystem for the common good of the Internet and European citizens.

We would also encourage the European Commission to work directly with the open-source community and the RIPE community, as a source of technical expertise, when developing proposals for regulatory measures that will have a significant impact on the technical community, the technical operation of the Internet and the Internet landscape within the European Union.

[3] https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/open-source-software-strategy_en

For a more detailed discussion of these concerns within the technical community, please consult the following:

The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem
Olaf Kolkman, Internet Society
https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/

Open-source software vs. the proposed Cyber Resilience Act
NLnet Labs
https://blog.nlnetlabs.nl/open-source-software-vs-the-cyber-resilience-act/

Cyber Resilience Act Effects on OSS (presentation at RIPE 85 Meeting)
Maarten Aertsen
https://ripe85.ripe.net/archives/video/911/

ICANN Training Series - Nordic Region: Why some Internet Legislation Might Cause a Headache
Lars-Johan Liman, Netnod
https://features.icann.org/event/icann-organization/icann-training-series-nordic-region-why-some-internet-legislation-might

Archive of discussion on RIPE Cooperation mailing list
https://www.ripe.net/ripe/mail/archives/cooperation-wg/2022-October/001609.html