NIS2 + CRA

- A short introduction to NIS2 and CRA
- Current concerns
- Ramifications
- Suggested actions

WHAT IS NIS2?

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive 2022/2555)

- Increase cybersecurity in general, across EU
- Adopted on **Nov 28, 2022**
- Must be implemented in national laws by **Oct 17, 2024**
- Applies to **many businesses** (more later)
- Many new & sensible security demands (security professionals are positive)

Does NOT apply directly to Open Source projects – BUT…

NIS2 – DEMANDS

- Establish common policies on **risk analysis**, **incident handling**, **crisis management** & more
- Improve **supply chain security**, and **relationships** between suppliers and providers
- Improve vulnerability handling and disclosure
- Define basic cyber hygiene practices (e.g. **secure by default**)
- …and much more

NIS2 – LIABILITY

- Fines up to **€ 10,000,000** or **2% of global revenue** – whatever is higher
- Management liability (fines, jail)

NIS2 – APPLIES TO…

- …Large and medium-sized companies in EU/EEA
- …**Essential and important entities**
- …Businesses not based, but offer services within EU
  (est. 40,000 businesses in Germany alone)
  Does NOT apply to Open Source projects directly (**note)

NIS2 – ESSENTIAL AND IMPORTANT ENTITIES

Networks & communication	Energy
Banking & Finacial	Water supply
Healthcare	**Pharmaseuticals**
Waste management	Postal
Space	Chemicals
Digital services, social media	Food
Public administration	& More…

(**Reference**)

NIS2 – REFERENCES & LINKS

- https://www.nis-2-directive.com/
- https://www.endian.com/company/news/eu-directive-nis2-open-source-is-the-key-to-success-269/
- https://ec.europa.eu/newsroom/dae/redirection/document/72155

WHAT IS CRA?

- Cyber Resiliency Act
- Additional security requirements to hardware and software products and components (“digital elements”)
- “CE marking” of physical products, including it’s software, including Open Source dependencies
- Distinguishes between “critical products” (Class I) and “products” (Class II) – (Ref: CRA Annex III)

CRA – APPLIES TO…

Class I	Class II
Identity management systems	Operating systems
Network management systems	PKI infrastructure
Network monitoring	Firewalls, IDS
Update/patch management	& Much more!

Source

CRA – LIABILITY

- Maximum fines of €15,000,000 or 2.5% of annual turnover, whichever is highest.

CRA – REQUIREMENTS

- Any devices (hardware and software) must handle **essential cybersecurity requirements**
  - *Unclear what these are at the moment* – **TBD**
- If law applies, it requires business to do risk analysis self-assessment, according to published guidelines
- Law requires both risk assesment and documentation to show compliance
- Failing to do this risks Significant Fines.
- Open Source Software may or may not be part of this assessment
- Risk-averse businesses are likely to assess their OSS dependencies anyway!
  Est. 92-98% of applications use OSS in their stack (sources differ)
  Approx. 21% of security incidents are supply-chain attacks.

CRA – CURRENT CONCERNS

- Directive feedback periods are finished (Jan ‘23)
- Very few actual open source communities offered feedback
- Still some confusion on demarkation between “commercial” and “open source”
  Direct ramifications are likely to be resolved.
  Our main problems are likely to be with the INDIRECT ramifications.

CRA – COMMUNITY IMPACT

- Increased demand for…
  - Tooling and support for **dependency management**
  - Tooling and support for **risk and security assessment**
- Supply chain security issues are likely to become visibly problematic
- Auditor and compliance officers are also likely to require documentation

CRA – LINKS AND RESOURCES

- Excellent overview: **https://berthub.eu/articles/posts/eu-cra-secure-coding-solution/**
- EU source: **https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en**
- NLNet Labs excellent overview: **https://blog.nlnetlabs.nl/open-source-software-vs-the-cyber-resilience-act/**
- **https://www.european-cyber-resilience-act.com/**

BUSINESS RAMIFICATIONS

- NIS2/CRA compliance is a major upcoming cost center (some est. 21% increase in development cost).
- Ways to **reduce the cost of managing large dependency trees**
  - Option 1: Use existing community infrastructure that helps them manage and improve the risk landscape
  - Option 2: Roll your own // in-house // fork dependencies
  - Option 3: Reduce the number of communities to interact with

TPRF & COMMUNITY RAMIFICATIONS

- Increased focus on security is likely to reveal more bugs and a greater pressure on volunteers
- Inaction will lead to increased active disengagement
- Unproffesionalism will lead to worsening reputation
- Lack of transparency around these processes will reduce trust in community and TPRF's capabilities to manage the new reality
- If businesses choose to re-implement their stack, they may choose software ecosystens that offer superior security features.

REMEDIES

What can we do about this?

REMEDY 1/5 – FACT-FINDING

- Set up a project with the task to **research, enumerate and report** on ongoing and current issues with software, infrastructure, policy, and governance that must be addressed by the Perl/Raku/CPAN community members, TPRF or other (possibly funded) dedicated organizations.

REMEDY 2/5 – FUNDING

- Create **avenues for support & funding**, to offset existing risk of harrasment, reduce likelyhood of parallel work (waste). This includes offering well-published options for businesses who wish to fund cross-community efforts like this.
- Create avenues for **experts to receive funding** for solving tasks related to identified issues.
- Set up **statistics gathering** so we can get some real data on how many/who contacts TPRF, so this can be used as leads for further fund-raising.

REMEDY 3/5 – GUIDES

- Establish, publish and manage **clear and authoritative guides on how to stay informed** on incidents, practice responsible disclosure, and other common security-related issues and tasks.
- Offer **guides**, best practices and check-lists on **how to set up and manage a well-run Perl/Raku/CPAN application software lifecycle**.

REMEDY 4/5 – LIAISONS

- Set up and **fund a dedicated security auditor & OSPO community liaison**, that also can help resolve ongoing issues businesses may have.

REMEDY 5/5 – CULTURE

- Lead, execute and **promote efforts to establish and maintain a long-term healthy culture for security culture** within our communities.

LINKS AND RESOURCES

- https://berthub.eu/articles/posts/eu-cra-secure-coding-solution/
- https://fosdem.org/2023/schedule/event/cyber_resilience/
- https://blog.nlnetlabs.nl/open-source-software-vs-the-cyber-resilience-act/

THANK YOU!

Salve J. Nilsen (Oslo Perl Mongers)
Mastodon: @sjn@chaos.social
Twitter: @sjoshuan