Cyber security EU legal Framework and the Open-Source scenario

Nadina Foggetti

INFN Bari

INFN
Istituto Nazionale di Fisica Nucleare

Sommary

- New legal framework concerning cyber sercurity
- The impact on Open Souce Software
- Possible solutions
- Conclusion

New Legal Framework

- Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
- Proposal for a Regulation on cybersecurity requirements for products with digital elements 2022/027 COD (Cyber resilience Act)
- Proposal for a Directive on liability for defective products 2022/0302(COD)
- Proposal for a Directive on the adaptation of the rules on non-contractual civil liability to artificial intelligence (artificial intelligence liability directive) 2022/0303(COD)

Why?

- IT products increasingly subject to cyber attacks
- low level of cyber security, mirrored by widespread vulnerabilities, poor security updates
- low level of user awareness of the cybersecurity aspects of products and their use

What?

Obligations relating to documentation (risk assessment, declaration of conformity)

vulnerability monitoring

updating instruction manuals with descriptions of cyber security aspects

availability of security updates

vulnerability management

digital product supply chain: subject to cyber security activities and controls

How

Manufacturers

upon product release: cybersecurity risk assessment

for 5 years: obligation to manage product vulnerabilities

for 5 years: adoption of corrective measures or withdrawal of the product from the market

Reporting obligations of manufacturers

Distributors

check that the product has the CE marking

verify that the manufacturer and the importer have complied with their obligations

ensure that corrective measures have been taken

notify the supervisory authority

Application to OS software

- **Whereas 10 of CRA:**

In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation.

for technical assistance services

provision of a software platform

use of personal data

In OS contest

not just only a price for a product!

A contradiction

Manufacturer (art. 3 comma 18)

means any natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark, whether for payment or free of charge;

Who?

- research institutions
- software developer

Article 16 Cyber Resilience Act

Other cases in which obligations of manufacturers apply

- A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements.

any programmer who contributes to the development of software whose use is regulated by free licenses becomes, legally, a producer and therefore is responsible "regardless" even if he does not receive a fee for the work he has done for the community

Among the obligations of the manufacturers

- “When a vulnerability is identified in a component, including an open source component, integrated into the product with digital elements, manufacturers report it to the person or entity who maintains that component”.

what effects?

- Obstacle for Open Source software developers
- Obstacle for software distribution platforms: platforms such as e.g. Github are qualified as distributors and therefore subject to the obligations pursuant to art. 14 par. 2

distributor means any natural or legal person in the supply chain, other than the manufacturer or importer, who makes a product with digital elements available on the Union market without changing its properties.

Open issues

Beta versions: Recital 21 of the Regulation

interaction between OS software produced inside and outside the EU

application to systems of Artificial Intelligence Open Source

International research activities

Proposal

To introduce a dialogue mechanism between the EU and the open source community

To create an optional quality seal and only certify when needed in the supply chain

To insert the obligation to adopt policies and guidelines that ensure compliance with the requirements for open source software

important to send an input comment to the European Commission in view of the entry into force of the Cyber Resilience Act

Conclusion

CNR.BiOmics

BIG DATA FOR BETTER LIFE

nfoggetti@infn.it

THANK
YOU
FOR
YOUR
ATTENTION