Contribution ID: **129**

Type: **Presentazione orale**

Cyber security EU legal Framework and the open-source scenario

Thursday, 25 May 2023 15:45 (30 minutes)

The innovative aspect of the EU Legal Framework concerning cyber security extends the scope and the application of the obligation imposed by the NIS Directive.
The new legal framework, compared to the first edition, covers 18 sectors, and distinguishes between 'Essential Entities' and 'Important Entities'.
The EU cybersecurity certification framework for ICT products enables the creation of tailored and risk-based EU certification schemes.
Certification plays a crucial role in increasing trust and security in critical products and services for the digital world.
In the other hand, the implementation of the Open Science and Open Access and FAIR principles assumes a crucial role in EU legislation.
The paradigm of the use of Open-Source technologies and software are one the most important milestone in the EOSC prospective.
Open source is involved in the application of the Cyber security legal framework, but it is also a challenge in the contest of the application of the same rules.
Cybersecurity tools based on open-source technology have a clear advantage in this situation. The NIS2 directive recall explicitly the Open Source cybersecurity tools. and applications can leverage the wider developer community, enabling diversification of suppliers".
Additionally, NIS2 states that: Policies promoting the introduction and sustainable use of open-source cybersecurity tools are of particular importance for small and medium-sized enterprises facing significant costs for implementation, which could be minimised by reducing the need for specific applications or tools".
The talk aims to analyse the new principles and the discipline introduced by the new European legal framework on cyber security, and in particular the NIS 2 Directive relating to measures for a common and high level of cybersecurity in the Union, the directive 2022/ 2557 relating to the resilience of critical subjects, as well as Regulation (EU) 2019/881 of 17 April 2019 relating to ENISA, the European Union Agency for Cybersecurity and the certification of cybersecurity for information and communication technologies.
The analysis of regulatory innovations will also be addressed considering the practical repercussions in the contexts in which Open-Source technology is leveraged.
In this perspective, the applicability of the requirements of the new discipline to open source software developed in the context of INFN Cloud will be evaluated. Especially for developing and managing of orchestrator services, IAM and cryptographic key management. The goal is to try to define what are the regulatory requirements that our applications must comply with and how to apply in the development cycle principles such as "security by design", "defense in depth", "security by default", "default deny"", "fail securely", "distrust input from external applications", "security in deployment", "assume breach", "least privilege", "usability and manageability"and "least functionality".

Primary authors: MARTELLI, Barbara (Istituto Nazionale di Fisica Nucleare); FOGGETTI, Nadina (Istituto Nazionale di Fisica Nucleare)

Co-authors: VIANELLO, Enrico (Istituto Nazionale di Fisica Nucleare); GIACOMINI, Francesco (Istituto Nazionale di Fisica Nucleare); ANTONACCI, Marica (Istituto Nazionale di Fisica Nucleare)

Presenter: FOGGETTI, Nadina (Istituto Nazionale di Fisica Nucleare)

Session Classification: Servizi ICT

Track Classification: Servizi ICT