Cyber security EU legal Framework and the open source scenario

Loano – 22-26/05/2023

INFN BARI — Nadina Foggetti, Marica Antonacci

INFN CNAF — Barbara Martelli, Enrico Vianello, Francesco Giacomini

Sommario

La nuova normativa in materia di cyber security

Il suo impatto sul software Open Source

Possibili soluzioni

Conclusioni

La nuova disciplina

- Proposta di Regolamento relativo ai requisiti di cybersecurity per i prodotti con elementi digitali COM(2022) 454 final

- Proposta di Direttiva sulla responsabilità per danno da prodotti difettosi COM (2022) 495 final

- Proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale) COM (2022) 496 final

Cyber Resilience Act

Perché una nuova normativa?

I prodotti informatici (software e Hardware) sempre più soggetti ad attacchi informatici

un basso livello di cybersecurity, rispecchiato da vulnerabilità diffuse e dalla fornitura insufficiente e incoerente di aggiornamenti di sicurezza per affrontarle

una comprensione e un accesso insufficienti alle informazioni da parte degli utenti, impedendo loro di scegliere prodotti con proprietà di cybersecurity adeguate o di utilizzarli in modo sicuro

Obiettivi

garantire che i fabbricanti migliorino la sicurezza dei prodotti con elementi digitali dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita

garantire un quadro coerente in materia di cybersecurity, facilitando la conformità per i produttori di hardware e software

migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali

consentire alle imprese e ai consumatori di utilizzare prodotti con elementi digitali in modo sicuro

Effetti

integrerà la direttiva NIS 2

requisiti di sicurezza informatica, comprese misure di sicurezza della catena di approvvigionamento

obblighi di segnalazione degli incidenti per gli enti essenziali e importanti, con l'obiettivo di aumentare la resilienza dei servizi che forniscono

- il miglioramento del livello di cybersecurity dei prodotti con elementi digitali potrebbe facilitare la conformità da parte dei soggetti che rientrano nell'ambito di applicazione della Network and Information Security Directive (NIS2) e rafforzare la sicurezza dell'intera catena di fornitura.

Norme per l'immissione sul mercato di prodotti con elementi digitali per garantire la cybersecurity

- requisiti essenziali per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali e obblighi per gli operatori economici in relazione a tali prodotti per quanto riguarda la cybersecurity;
- requisiti essenziali per i processi di gestione delle vulnerabilità messi in atto dai fabbricanti per garantire la cybersecurity dei prodotti con elementi digitali durante l'intero ciclo di vita e obblighi per gli operatori economici in relazione a tali processi;
- norme sulla vigilanza del mercato e sull'applicazione delle norme e dei requisiti.

Obblighi

- Fabbricanti
  - Atto di immissione del prodotto: Valutazione dei rischi di Cybersecurity
  - Per 5 anni obbligo di gestione delle vulnerabilità dei prodotti
  - Per 5 anni adozione delle misure correttive o ritiro del prodotto dal mercato
  - Obbligo di informazione e comunicazione con l'Autorità
  - Obbligo di emissione delle dichiarazione di conformità

- Distributori
  - Verificare che il prodotto abbia il marchio CE
  - Verificare che il fabbricante e l'importatore abbiano rispettato gli obblighi
  - Assicurarsi che siano state adottate le misure correttive
  - Avvisare l'autorità di vigilanza

Applicabilità ai prodotti Open Source

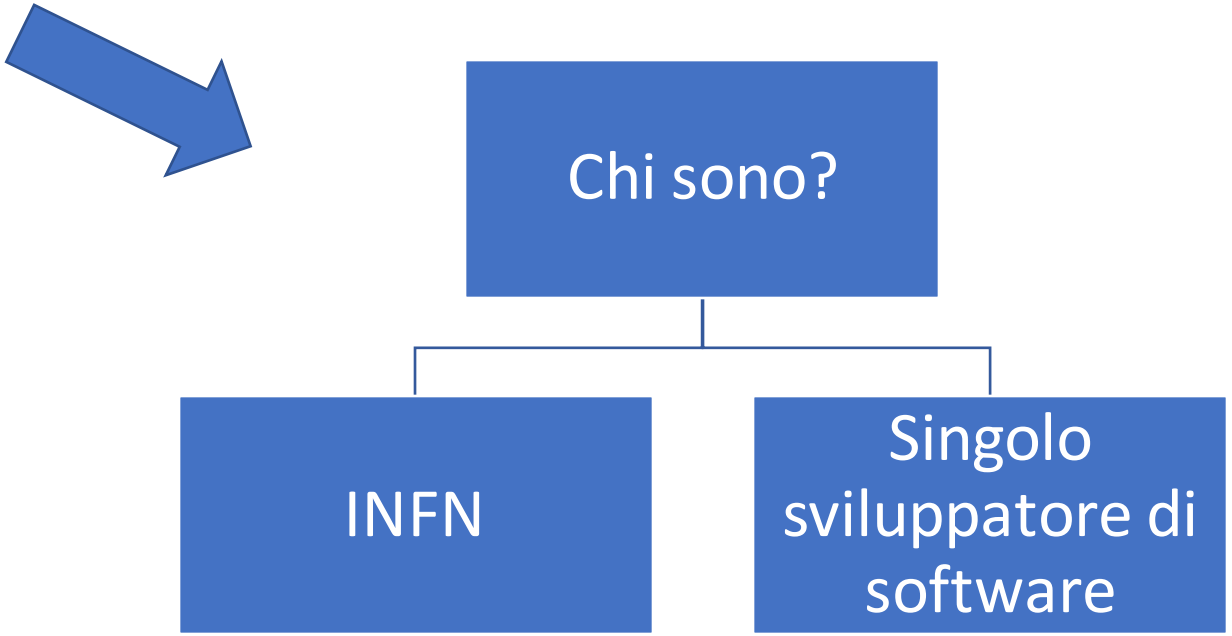
Applicazione al Software Open Source

- **Considerando 11 del Regolamento:**

«il presente regolamento non dovrebbe disciplinare il software libero e open source sviluppato o fornito al di fuori di un'attività commerciale»

Aspetto contraddittorio

- Fabbricante (art. 3 comma 18)
  - Qualsiasi persona fisica o giuridica che sviluppi o fabbrichi prodotti con elementi digitali o che faccia progettare, sviluppare o fabbricare prodotti con elementi digitali e li commercializzi con il proprio nome o marchio, a titolo oneroso o gratuito.

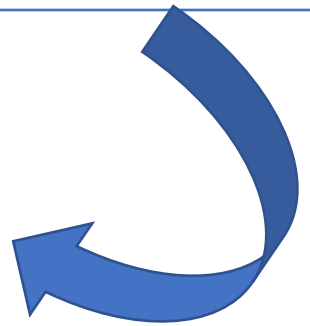


Articolo 16 Cyber Resilience Act

Altri casi in cui si applicano gli obblighi dei fabbricanti

- Una persona fisica o giuridica, diversa dal fabbricante, dall'importatore e dal distributore, che apporta una sostanziale modifica al prodotto con elementi digitali.

Qualsiasi programmatore che contribuisce allo sviluppo di un software il cui uso è regolato da licenze libere diventa, giuridicamente, un **produttore e dunque responsabile "a prescindere" anche se non viene pagato** per il lavoro che ha svolto per la comunità.



Tra gli obblighi dei fabbricanti

- Art. 11 obbligo di segnalazione

- “Quando è individuata una vulnerabilità in un componente, compreso un componente open source, integrato nel prodotto con elementi digitali, i fabbricanti la segnalano alla persona o al soggetto che si occupa della manutenzione di tale componente”.

Art. 4 Product Liability Directive

per “prodotto” si intende anche il software; e “fabbricante” identifica chi sviluppa, produce o fabbrica un prodotto per uso proprio

Gli sviluppatori non assumono responsabilità o offrono garanzie al pubblico

Contribuiscono all’ecosistema Open Source

Specificamente previsto dalle licenze Open Source

Eccezioni

- Art. 2: Ambito di applicazione
- Limitazioni all'applicazione della normativa
- L'uso di software Open Source: non rientra tra le esclusioni

Condizione per l'applicazione: non commerciale!

Che ricadute?

- Ostacolo per gli sviluppatori di software Open Source
- Ostacolo per le piattaforme di distribuzione del software: piattaforme come es. Github sono qualificate come ***distributori*** e quindi soggetti agli obblighi di cui all'art. 14 par. 2
- Uso di software sviluppato al di fuori dell'UE
- Impossiblità per programmatori UE di interagire

- Piattaforme sono responsabili del software pubblicato

Chi è il distributore?

- "distributore": qualsiasi persona fisica o giuridica nella catena di approvvigionamento, diversa dal fabbricante o dall'importatore, che mette a disposizione un prodotto con elementi digitali sul mercato dell'Unione senza modificarne le proprietà.

  - "messa a disposizione sul mercato": la fornitura, a titolo oneroso o gratuito, di un prodotto con elementi digitali perché sia distribuito o usato sul mercato dell'Unione nel corso di un'attività commerciale

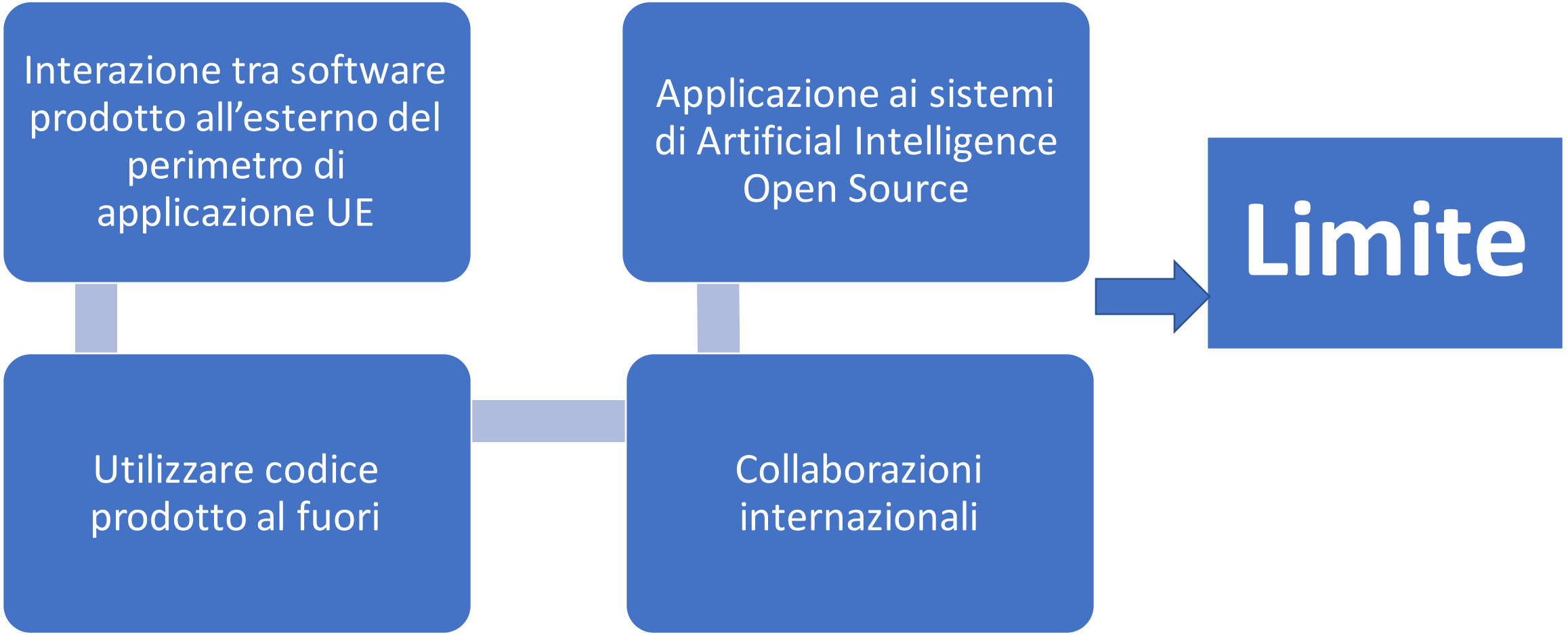
L'INFN potrebbe essere considerato distributore

E le versioni beta?

- **Software non finito**: considerando n. 21 del Regolamento
- a condizione che la versione sia messa a disposizione solo per il tempo necessario a testarla e a raccogliere riscontri. I fabbricanti dovrebbero provvedere affinché il software messo a disposizione a tali condizioni sia rilasciato solo a seguito di una valutazione dei rischi e sia conforme, per quanto possibile, ai requisiti di sicurezza relativi alle proprietà dei prodotti con elementi digitali imposti dal presente regolamento.

- I requisiti devono essere comunque rispettati
- Problema terminologico: software non finito. Quando un software Open Source può essere considerato finito?

Problemi aperti



Possibili proposte

Lettera aperta da parte delle associazioni open source

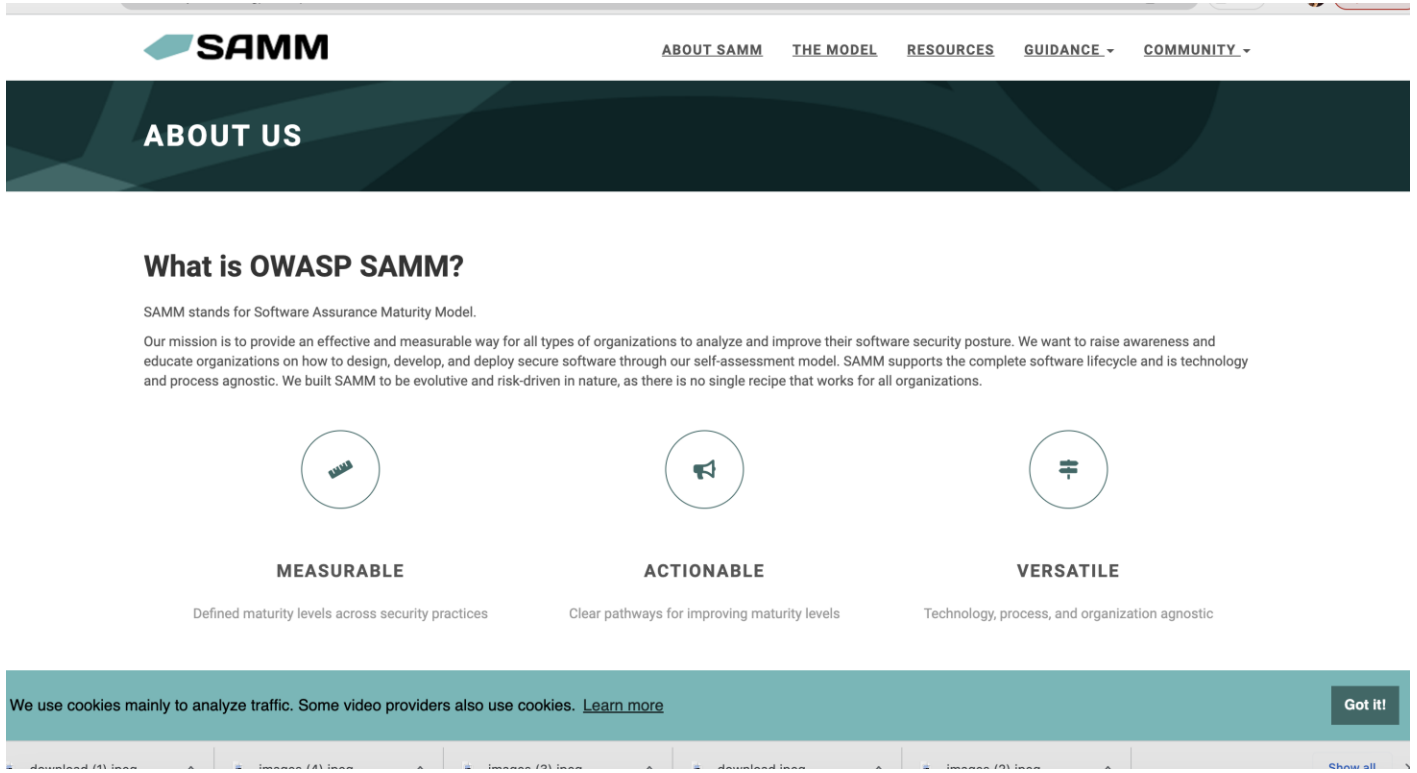
- Riconoscere le caratteristiche uniche del software open source e garantire che il Cyber Resilience Act non danneggi involontariamente l'ecosistema open source;
- Consultare la comunità open source durante il processo colegislativo;
- Garantire che qualsiasi sviluppo nell'ambito del Cyber Resilience Act tenga conto della diversità delle pratiche di sviluppo del software open source aperto e trasparente;
- Stabilire un meccanismo di dialogo e collaborazione costante tra le istituzioni europee e la comunità open source, per garantire che le future decisioni legislative e politiche siano informate.

Altre soluzioni

- Creare un sigillo di qualità facoltativo e procedere alla certificazione solo quando serva nella supply chain
- Modificare lo scopo del regolamento
- Inserire un’eccezione che riguardi direttamente il software open source
- Inserire un'espressa richiesta di adozione di policy e linee guida che assicurino, per il software open source, la compliance con i requisiti
- Attribuire l’obbligo di controllo dei requisiti e di autocertificazione su chi lo utilizza: valutazione del rischio e una dichiarazione di conformità

- Spostando l’onere sulla base del principio di accountability

Software per valutare il Maturity Model SAMM



- aiuta le organizzazioni ad analizzare le loro attuali pratiche di sicurezza del software, creare un programma di sicurezza in iterazioni definite, mostrare miglioramenti progressivi nelle pratiche di sicurezza e definire e misurare le attività relative alla sicurezza.

Open Source Software Adoption Policy

- Ispirate ai requisiti ISO (richiamati dai common critiria nel Cyber Resilience Act)
- Legal Compliance
- Documentazione a supporto
- Modifica periodica e audit annuale

- https://istnazfisnucl.sharepoint.com/:w:/s/INFNCloud9/Eds_y1ysfERHvC043apPN3kBGPM5-MOtbpgEj9F89w-jmQ?e=IfYVad

Advancing Software Security in the EU

- Linee guida che riguardano i diversi aspetti dello sviluppo del software nell'ambito del nuovo quadro di certificazione della cyber security dell'UE e dei sistemi di certificazione della cyber security dell'UE.

Conclusioni

Importante inviare un commento/input che rilevi le necessità concrete che INFN dovrà affrontare in vista dell'applicazione del Cyber Resilience Act

Focus sulla situazione: osservatorio permanente di questi aspetti

Migliorare le linee guida e contribuire alla definizione di linee guida uniformi

individuare il software interessato: IAM? PaaS Orchestrator?

Costruire una rete con enti che si occupano di ricerca scientifica (CNR - CERN)

Questione che interessa WP7 INFN Cloud

Focus sulla security a prescindere dalle norme!

E il software scientifico?

Link

- Proposta di Regolamento relativo a requisiti orizzontali dicibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 COM(2022) 454 final
- Proposta di Direttiva sulla responsabilità per danno da prodotti difettosi COM (2022) 495 final
- Proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale) COM (2022) 496 final
- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

Altri link utili

- https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or
- https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf
- https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro
- https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework
- https://owasp.org/

Grazie per l’attenzione