Cyber Resilience Act and Open Source: problemi aperti e prospettive future.

Nadina Foggetti

INFN Bari

ConfGARR23

SAPERI INTERCONNESSI

La nuova disciplina

Proposta di Regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 COM(2022) 454 final

Aspetti documentali (Risk assesment, dichiarazione di conformità)

Monitoraggio continuo nel tempo delle possibili vulnerabilità

Manuali di istruzione aggiornati con descrizioni sugli aspetti di sicurezza

Disponibilità di aggiornamenti di sicurezza

Gestione delle vulnerabilità

Tutta la filiera (Supply Chain) di produzione di un prodotto digitale (software, hardware, connettività ecc.) diventa quindi soggetta ad attività e controlli di cyber security

Obblighi

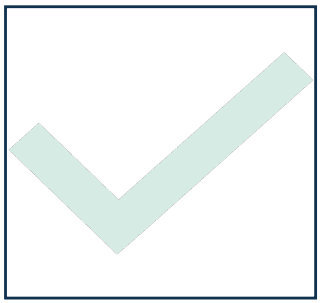
Fabbricanti

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



Distributori

Verificare che il prodotto abbia il marchio CE

Verificare che il fabbricante e l'importatore abbiano rispettato gli obblighi

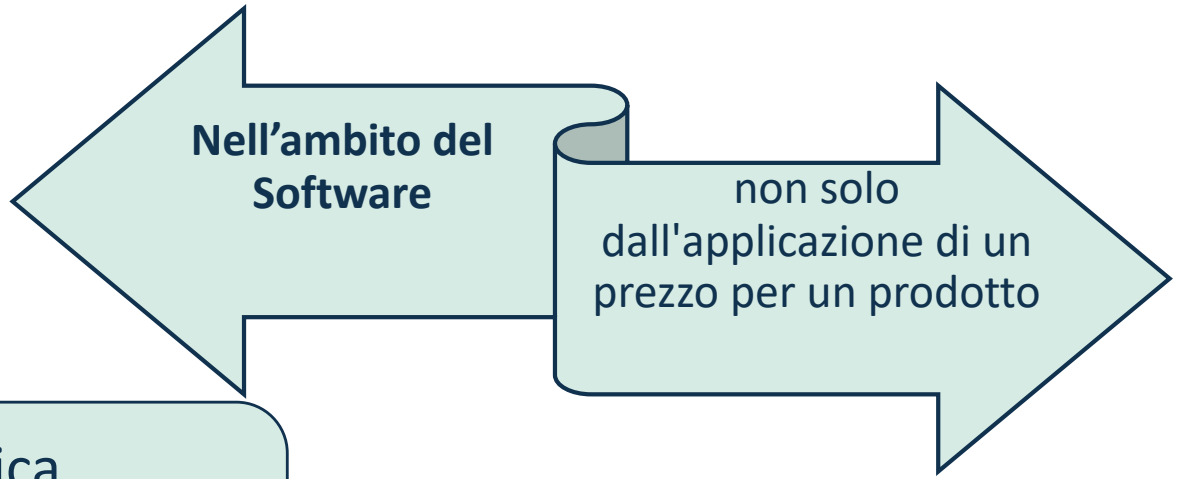
Assicurarsi che siano state adottate le misure correttive

Avvisare l'autorità di vigilanza

Applicazione al software OS

- **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»



per i servizi di assistenza tecnica

fornitura di una piattaforma software

utilizzo di dati personali

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.

Chi sono?

- Enti di ricerca
- Singolo sviluppatore di software

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.

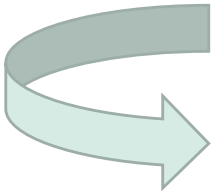
Qualsiasi programmatore che contribuisce allo sviluppo di un software il cui uso è regolato da licenze libere diventa, giuridicamente, un **produttore e dunque responsabile "a prescindere" anche se non viene pagato** per il lavoro che ha svolto per la comunità.

Tra gli obblighi dei fabbricanti

“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”.

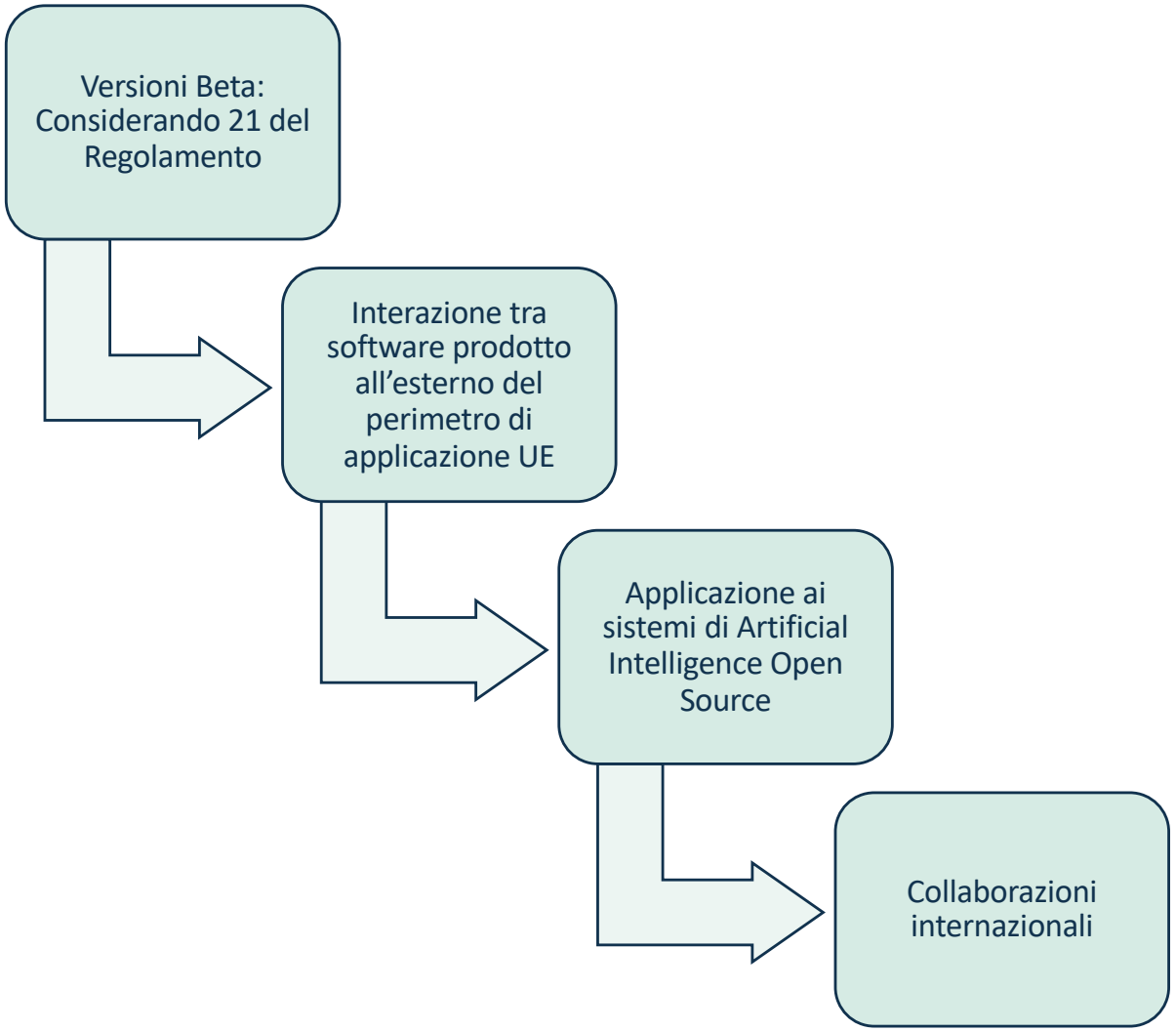
Che ricadute?

- Ostacolo per gli sviluppatori di software Open Source
- Ostacolo per le piattaforma di distribuzione del software: piattaforme come es. Github sono qualificate come ***distributori*** e quindi soggetti agli obblighi di cui all'art. 14 par. 2



"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.

Problemi aperti



Proposte possibili

Stabilire un meccanismo di dialogo tra UE e la comunità open source,

Creare un sigillo di qualità facoltativo e procedere alla certificazione solo quando serva nella supply chain

Inserire un’espressa richiesta di adozione di policy e linee guida che assicurino, per il software open source la compliance con i requisiti

Importante inviare un commento/input in vista dell’applicazione del Cyber Resilience Act

Conclusioni

nfoggetti@infn.it

ConfGARR23

SAPERI INTERCONNESSI