Italo Vignoli / The Document Foundation

Cosa potrebbe cambiare per il FOSS con il Cyber Resilience Act


EU Cyber Resilience Act
For safer & more secure
digital products
#DigitalEU #CyberSecEU

Background / Introduzione

La Commissione Europea sta elaborando una nuova normativa - Cyber Resilience Act (CRA) - per migliorare la sicurezza informatica dei prodotti software e hardware disponibili in Europa, con l'obiettivo di:

- Migliorare la sicurezza di tutti i prodotti digitali disponibili in Europa
- Richiedere che tutti i produttori privilegino la sicurezza sia nei processi di sviluppo che nel ciclo di vita dei prodotti una volta nelle mani degli utenti
- Richiedere che i produttori applichino il marchio CE a tutti i prodotti per indicare la conformità ai requisiti del CRA

Altri Dettagli

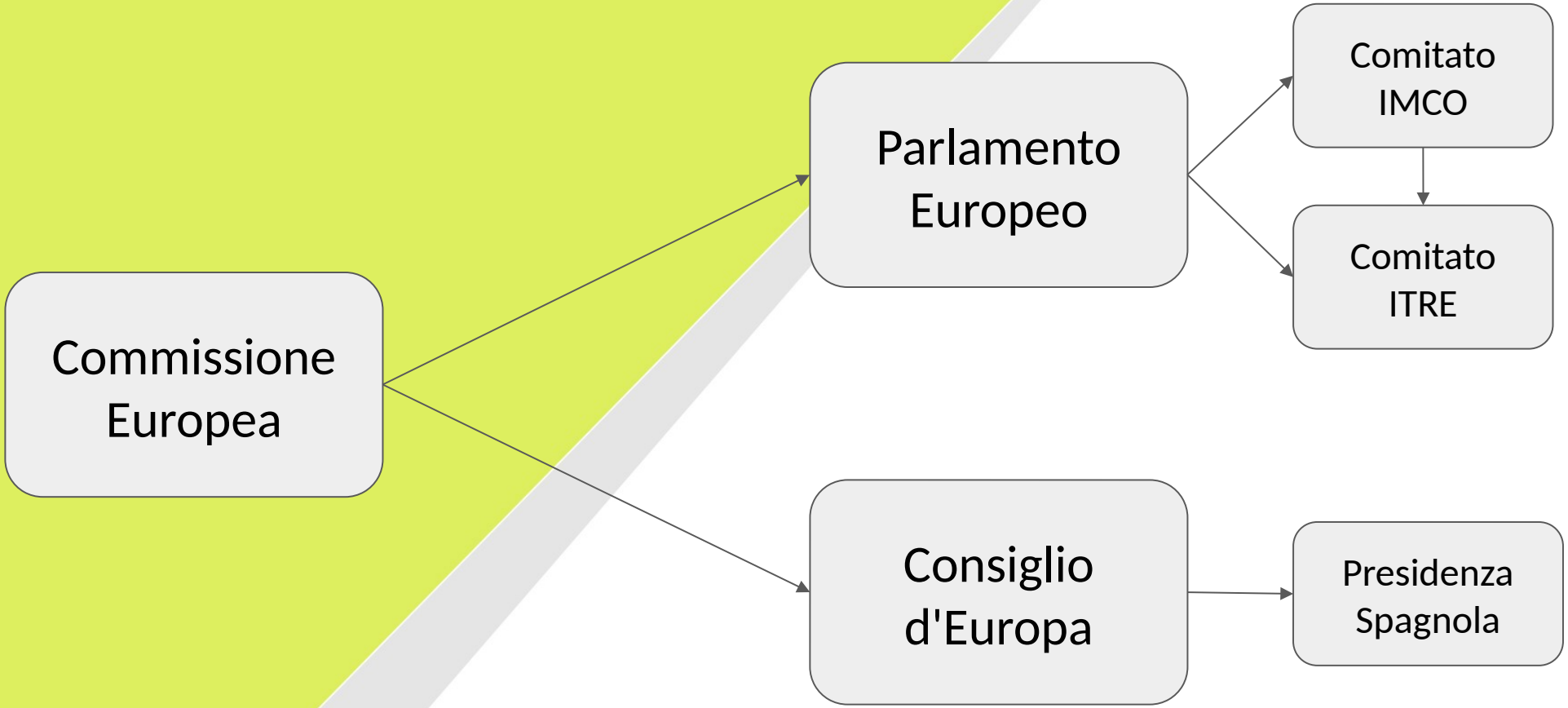
- Requisiti di processo:
  - SBOM, patch di sicurezza, protocollo di "richiamo"
  - Impone il supporto dei prodotti per non meno di 5 anni
  - Limita la pubblicazione di software non finito a scopo di test
  - Impone requisiti di processo e documentazione per ogni rilascio
- Requisiti del marchio CE:
  - Tre livelli di tipologia di prodotto, con obblighi di conformità crescenti per i prodotti "critici" e "molto critici"
  - I prodotti critici e molto critici devono ricorrere ad audit esterni per la certificazione del rilascio

CE

Sanzioni

L'inosservanza dei requisiti essenziali di cibersicurezza di cui all'allegato I e degli obblighi di cui agli articoli 10 e 11 è soggetta a sanzioni amministrative pecuniarie fino a 15 milioni di euro o, se il trasgressore è un'azienda, fino al 2,5% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

Processo Legislativo



CRA: Stato Attuale

- Il Comitato ITRE è giunto alla ferma conclusione che la maggior parte dei progetti open source e tutte le fondazioni open source dovrebbero essere responsabili della conformità con il marchio CE
  - Questo è intenzionale, e non si tratta di un malinteso
- La loro motivazione:
  - Per le PMI europee è troppo costoso implementare il CRA
  - Ridurre l'onere finanziario sull'economia dell'UE affidando ai progetti OSS e alle fondazioni OSS la responsabilità della conformità
  - Presuppone che la conformità con il marchio CE sia transitiva

Draft ITRE: Problema 1

- Qualsiasi progetto open source con committer impiegati da un'entità commerciale viene considerato un'attività commerciale
- Perché è un problema?
  - Questo in pratica include tutti i progetti open source significativi sul pianeta
  - Crea un effetto perverso per molti progetti, spingendoli a rifiutare i contributi da parte delle aziende che utilizzano il loro software
  - Le aziende, a loro volta, potrebbero vietare ai propri dipendenti di partecipare o contribuire a progetti open source

Draft ITRE: Problema 2

- Qualsiasi progetto che accetti donazioni ricorrenti da entità commerciali viene considerato commerciale
- Perché è un problema?
  - La sostenibilità dell'open source è un problema serio
  - I progetti potrebbero essere incentivati a rifiutare le donazioni, che sono quasi sempre fondamentali per la loro esistenza

Draft ITRE: Problema 3

- La pubblicazione di build intermedie, o di altro tipo, deve essere limitata nel tempo a una specifica area geografica, e solamente per effettuare dei test
- Perché questo è un problema?
  - La pubblicazione di build – anche giornaliere – con licenza open source è considerata una buona pratica da oltre 30 anni, e spesso queste build sono preziose per la Quality Assurance
  - Questo metterà in difficoltà o addirittura proibirà alcune tra le più diffuse pratiche di sviluppo open source

Draft ITRE: Problema 4

- Tutte le vulnerabilità devono essere segnalate all'ENISA entro poche ore, indipendentemente dalla disponibilità di una soluzione
- Perché è un problema?
  - Va contro le best practice per la divulgazione coordinata delle vulnerabilità
  - Per le vulnerabilità prive di patch, va contro le best practice che limitano la divulgazione solo a coloro che sono in grado di contribuire alla correzione
  - La creazione di un archivio centrale delle vulnerabilità prive di patch non contribuisce a rendere il software più sicuro
  - Rappresenta un precedente infausto per gli altri legislatori

Valutazione d'Impatto (1)

Per essere conformi, i progetti, le comunità e le fondazioni dovranno:

- Sviluppare, documentare e implementare politiche e procedure per ogni progetto, tra cui tutti:
  - Il rispetto dei requisiti di sicurezza per lo sviluppo e il rilascio stabiliti nell'Allegato I, compresa la fornitura di meccanismi di notifica e aggiornamento
  - Il rispetto dei requisiti di documentazione per gli utenti (di cui all'Allegato II)
  - La creazione di documentazione tecnica del prodotto (di cui all'Allegato V)
  - La verifica della conformità con il CRA di tutte le librerie di terze parti utilizzate da ciascun progetto

Valutazione d'Impatto (2)

Per essere conformi, i progetti, le comunità e le fondazioni dovranno:

- Per ogni release del prodotto, preparare la documentazione specifica di progetto richiesta dall'Allegato V
- Per ogni release del prodotto, determinare se soddisfa la definizione di "prodotto con elementi digitali", "prodotto critico con elementi digitali" o "prodotto molto critico con elementi digitali"
- Per ogni release del prodotto, documentare che è stato seguito il processo di marcatura CE pertinente

Impatto del Marchio CE

- Marcatura CE per i prodotti software
  - Estendere il regime del Marchio CE a tutti i prodotti digitali venduti in Europa
  - Integrata con la Product Liability Directive per estendere il regime a tutto il software
- Ipotesi:
  - Il processo sarà applicato agli OSS resi disponibili con licenze OS e forniti gratuitamente, apparentemente con licenze che escludono qualsiasi responsabilità o garanzia
- La nostra preoccupazione:
  - Il CRA potrebbe alterare radicalmente il contratto sociale che sta alla base dell'intero ecosistema open source: software open source fornito gratuitamente, per qualsiasi scopo, che può essere modificato e ulteriormente distribuito gratuitamente, ma senza garanzie o responsabilità per gli autori, i collaboratori o i distributori open source

CRA: Rischio 1

- I produttori extraeuropei di software open source non ne consentiranno l'uso in Europa
  - Una risposta ragionevole e razionale per non accettare gli obblighi di responsabilità legale per qualcosa che si rende disponibile gratuitamente
  - L'impossibilità di accedere a Linux, Kubernetes, Apache, e altri prodotti da parte dell'Unione Europea paralizzerebbe il suo processo di innovazione

CRA: Rischio 2

- I produttori europei di software open source saranno svantaggiati rispetto ai concorrenti internazionali
  - Non potendo evitare gli obblighi di responsabilità imposti dal CRA, saranno costretti ad accettarli come parte delle loro attività di sviluppo
  - In alcuni casi, probabilmente sarà più semplice chiudere il progetto e togliere il codice sorgente da internet

CRA: Rischio 3

- Costringere le imprese europee a smettere di contribuire ai progetti open source
- Attualmente si ritiene che il rischio che i contributi all'open source possano comportare responsabilità per l'azienda sia basso
- Il CRA può cambiare questa equazione, e di conseguenza le aziende europee potrebbero ridurre le loro collaborazioni con i progetti open source
- Questo è estremamente rischioso per l'economia dell'innovazione in Europa, ed è in contrasto con numerose strategie europee (sovranità digitale, GAIA-X, Catena-X, Dataspaces, Digital Twins e Industria 4.0)

Grazie

Italo Vignoli
italo@vignoli.org
italo@libreoffice.org