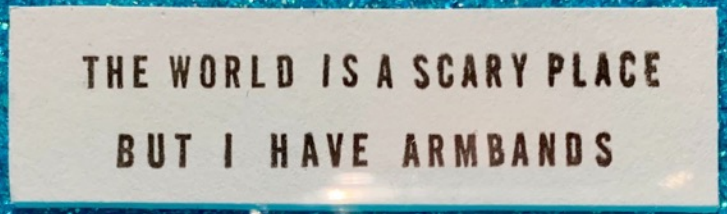
EU Cyber Resilience Act



Un (altro) Game Changer per l'Economia Europea

Agenda

1. Dal GDPR al CRA: la Strategia Europea
2. Il CRA in breve
3. Gli Impatti economici attesi dal CRA
4. Q&A

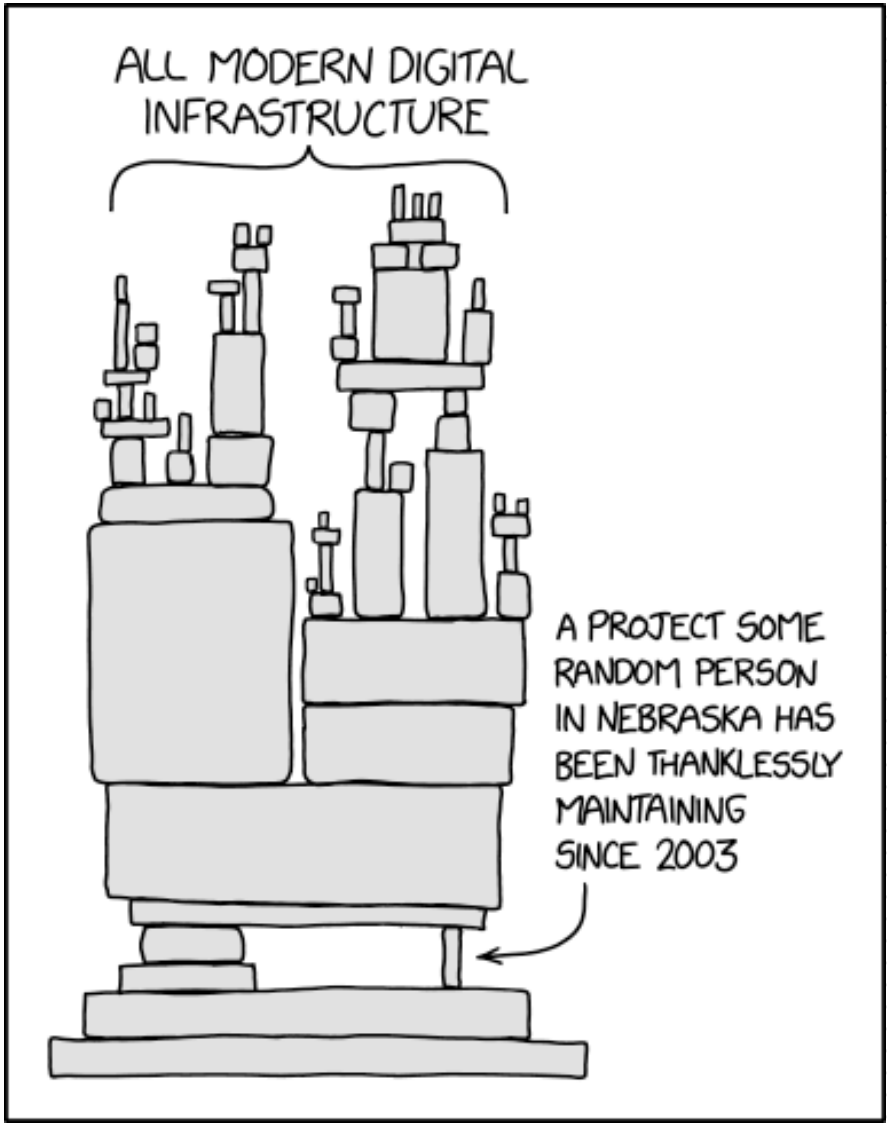
Dal GDPR al CRA: la Strategia Europea sul dato e i prodotti

- GDPR
- ePrivacy Regulation (?)
- Cyber Security Act
- Direttiva NIS2;
-UE Commision Blue Print
-Data Act
-Data Governance Act
-AI Act
-Product Liability Act
-Cyber Resilience Act
- Cyber Solidarity Act

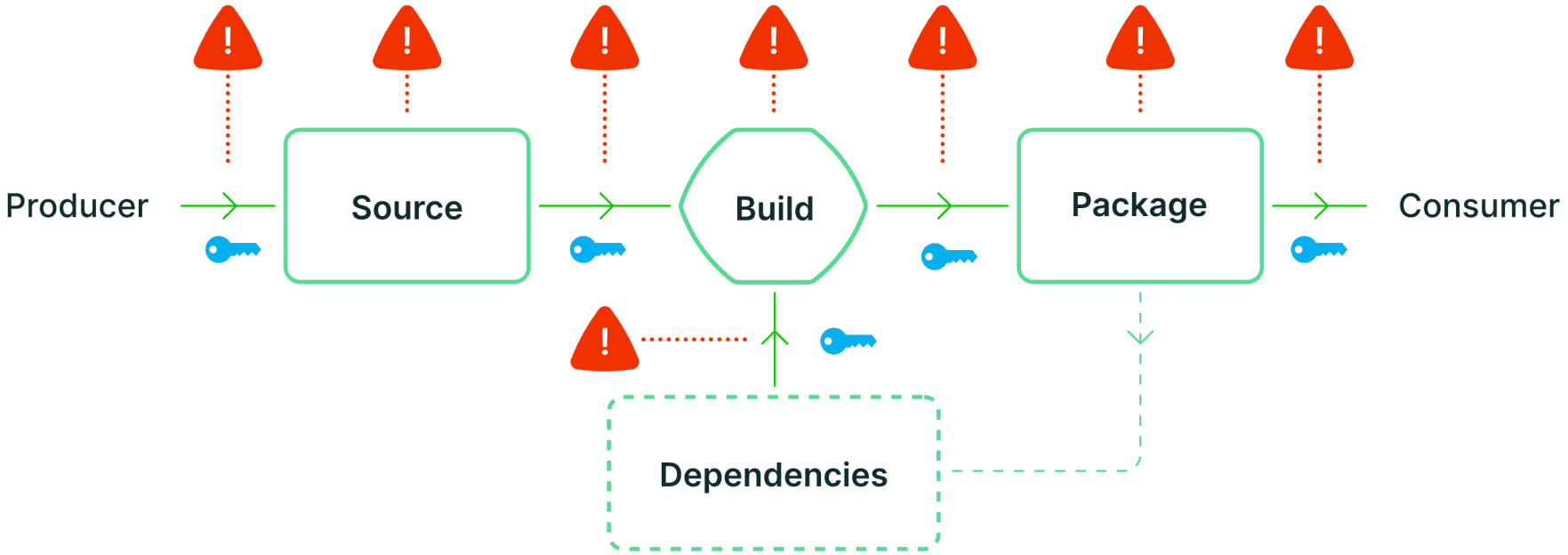
- Accountability
- Risk-based approach
- By design
- By default

Extra «fatti» di software

- La maggior parte del software proprietario fa affidamento su sw fornito da terze parti
- 90% circa del software commerciale è fatto di open-source
- -Foto divertente di open source



Extra «fatti» di software



- Il mio software e ogni «dependency» può avere problemi
- Ogni dipendenza ha un costo Cost Per Dependency cd. CPD
- È necessario regolare/proteggere questi processi (es. hash, signed logs, SBOM)
- Problema di fondo: il software è un'opera letteraria

Si tutela il codice, non l'eseguibile..

```
package rentalStore;
import java.util.Enumeration;
import java.util.Vector;

class Customer {
    private String _name;
    private Vector<Rental> _rentals = new Vector<Rental>();

    public Customer(String name) {
        _name = name;
    }
    public String getMovie(Movie movie) {
        Rental rental = new Rental(new Movie("", Movie.NEW_RELEASE), 10);
        Movie m = rental._movie;
        return movie.getTitle();
    }
    public void addRental(Rental arg) {
        _rentals.addElement(arg);
    }
    public String getName() {
        return _name;
    }
```

=

Opera letteraria sì….ma con anche responsabilità da prodotto!

- UE Product liability act (PLA) il software è un «prodotto» ma «*ai fini di questo Regolamento*»

- Altre normative di responsabilità da prodotto:
  - ✓ Medical Devices Regulation (Regulation (EU) 2017/745);
  - ✓ In Vitro Diagnostic Medical Devices Regulation (Regulation (EU) 2017/746)
  - ✓ Vehicle General Safety Regulation (Regulation (EU) 2019/2144)
  - ✓ Common Rules in Civil Aviation Regulation (Regulation (EU) 2018/1139).

….Ma cos'è la responsabilità da prodotto?

Barbie

La responsabilità del produttore si estende anche alle «dependencies»

Da Barbie® al CRA: il problema sottostante

Nel 2020, la criminalità informatica globale è costata 5,5 trilioni di euro e la criminalità informatica globale costerà probabilmente 10,5 trilioni di euro entro il 2025.

Per combattere questi crescenti costi della cibersicurezza e affrontare le vulnerabilità, la Commissione rileva quattro obiettivi specifici per gli obiettivi del Cyber Resilience Act:

Garantire che i produttori migliorino la cibersicurezza dei prodotti coperti durante l'intero ciclo di vita;

Creare un quadro unico e coerente per la conformità alla cibersicurezza nell'UE;

Aumentare la trasparenza delle pratiche e delle proprietà di sicurezza informatica dei prodotti e dei loro produttori; e

Fornire ai consumatori e alle imprese prodotti sicuri pronti per l'uso.

CRA come soluzione alla conformità del software / hardware (di Barbie)

Sulla base del New Legislative Framework (quadro legislativo consolidato dell'UE relativo ai prodotti):

- ✓ Obblighi per fabbricanti, distributori e importatori.

Norme di cibersicurezza per l'immissione sul mercato di hardware e software

- ✓ a qualsiasi prodotto software o hardware e alle sue soluzioni di elaborazione remota dei dati, compresi i componenti software o hardware da immettere sul mercato separatamente durante l'intero ciclo di vita.
- ✓ Nell'ambito di una "attività commerciale" (Considerando 10 CRA)
- ✗ No per prodotti fià regolati (dispositivi medici, veicoli, ecc.)
- ✗ No per software-as-a-service a meno che il software-as-a-service non faccia parte di soluzioni integrali di elaborazione dati remota per un prodotto con elementi digitali.

- ✓ Requisiti essenziali di sicurezza informatica per tutto il ciclo di vita (5 anni).
- ✓ Norme armonizzate da seguire.
- ✓ Valutazione della conformità – differenziata per livello di rischio. (MARCATURA CE)
- ✓ Vigilanza del mercato e applicazione delle norme (CSIRT ed ENISA)

CRA: Sicurezza by design & risk-based

CRA: to do & enforcement

Fase di progettazione e sviluppo

- Valutazione dei rischi associati a un prodotto.

- Requisiti essenziali relativi ai prodotti (Allegato I, sezione 1 CRA).

- Requisiti essenziali per la gestione delle vulnerabilità (Allegato I, sezione 2 CRA).

- Fascicolo tecnico, comprese le informazioni e le istruzioni per l'uso (Allegato II + V CRA).

- Valutazione della conformità, marcatura CE, dichiarazione di conformità UE (Allegato IV CRA).

- Art. 8 Interplay con AI ACT

Fase di manutenzione (5 anni o per tutta la durata del prodotto, a seconda di quale sia il più breve)

Obbligo di comunicazione all'ENISA entro 24 ore:

(1) Vulnerabilità sfruttate;

(2) Incidenti che hanno un impatto sulla sicurezza del prodotto.

Entra in vigore bi-fase

1. Riportare vulnerabilità e breach (12 mesi)
2. Implementare i requisiti del CRA (entro 24 mesi)

Enforcement

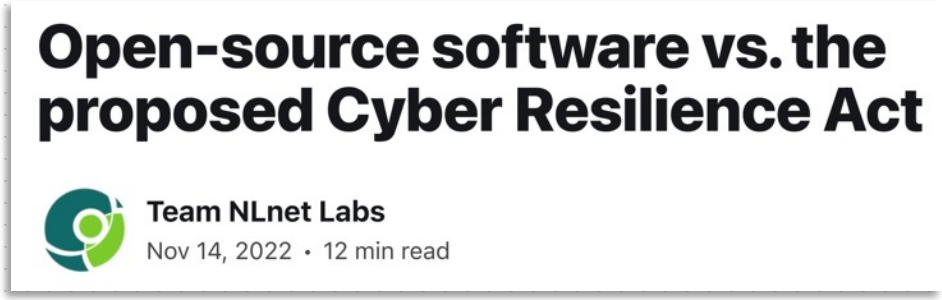
- Congiunto tra CSIRTs NIS, ENISA, Commissione (atti delegati)
- Sanzioni
  - € 15mil o 2,5% (Annex I + Artt 10 e 11 CRA)
  - € 10mil o 2% (CRA)
  - € 5mil o 1% (cooperazione distorta con authorità)

Impatti economici attesi

Fine dell'open source?

Considerando 10 CRA + Artt. 10 e 11

1. Sviluppatori = produttori
2. Attività commerciale vs. modelli di business open source
3. C10: include anche sfruttamento dei dati personali come mezzo di pagamento.



Costi di compliance e marchiatura

1. Maggiori costi per dependencies (CDP)
2. Creazione di SBOM e vulnerability handling
3. Costi per skill-sets (compliance, legal, implementation)
4. Costi di auditing di terze parti soprattutto per SME e no-profit (vedi anche ART 24.5 CRA)
5. Competenze di auditing in progetti open-source vs. processi di business.
6. Costi per pubblicizzare la marchiatura (specie per classe I di prodotti);
7. Costi gestione contenziosi rispetto alle dependencies e agli “intended purposes”.
8. Costo di incertezza: non tutti i difetti del software generano problem per chi li usa.

Benefici attes(ish)

1. Maggiore accountability (responsabilità da prodotto) sui produttori
2. Riduzione progressiva del numero prodotti non marchiati CE sul mercato UE;
3. Riduzione dell'ambito di applicabilità del "as is" o dei software in caso di vulnerabilità o mancati patch management specie se per software proprietary (by design e by default).
4. "Presunzione" di prodotti più sicuri nel mercato UE (CE vs C E);
5. Trasparenza verso i consumatori?

ICTLC | FEDERPRIVACY

Grazie per l'attenzione!

Nicola Franchetto

Avv. LL.M - Partner

Avvocato Partner di ICT Legal Consulting si è laureato in Giurisprudenza presso l'Università degli Studi di Treno. Perito informatico, certificato Privacy Officer (TUV) e Data Protection Officer (ECPC – Maastricht University, NL), è anche Lead Auditor ISO 27001:2013 (Bureau Veritas), ISO 27701:2019 e Lead Auditor EuroPrivacy, confermando il ruolo di "uomo di mezzo" tra le esigenze legali e le questioni ICT altamente complesse.

Milano - Bologna - Roma – Amsterdam – Madrid - Helsinki – Melbourne - Atene