CONFINDUSTRIA
VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

INNOVATION ROADMAP

Webinar tematici: INTELLIGENZA ARTIFICIALE

CYBERSECURITY PER L' AI E LA FABBRICA CONNESSA

CRA: Cyber Resilience ACT

Impatti, obblighi e prospettive per imprese e filiera digitale

Sandro Sana – CISO & Head of Cybersecurity (Eurosystem SpA)

16 Giugno 2026

Sandro Sana

CISO & Head of Cybersecurity di Eurosystem S.p.A.
Membro Comitato Scientifico – Competence Center Nazionale Cyber 4.0
Membro Dark Lab RHC, Direttore e voce Pod Cast Red Hot Cyber
Giornalista Red Hot Cyber & CyberSecurity360
Divulgatore – Docente AICA & ITS

CONFINDUSTRIA VENETO EST

Cos'è il CRA

REGOLAMENTO (UE) 2024/2847 DEL PARLAMENTO EUROPEO
Del 23 ottobre 2024, relativo ai requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (regolamento sulla cyber resilienza)

LEGGE n.36 del 17 marzo 2026 – ART. 15
Delega al Governo per l'adeguamento della normativa nazionale al Regolamento (UE) 2024/2847 – Cyber Resilience Act.

Individua **ACN** quale autorità nazionale di notifica e autorità di vigilanza del mercato per i requisiti orizzontali di cybersicurezza dei prodotti con elementi digitali.

Che cosa riguarda

Il CRA si applica ai «**prodotti con elementi digitali** messi a disposizione sul **mercato UE** la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete».

- **Prodotto con elementi digitali**: qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto (qualsiasi elaborazione dati a distanza la cui assenza impedirebbe al prodotto di svolgere una delle sue funzioni)

Esclusioni *(per applicazione di normative più specifiche):*

- **Dispositivi medici** → regolamento (UE) 2017/745
- **Dispositivi medico-diagnostici** → regolamento (UE) 2017/746
- **Automotive** → regolamento (UE) 2019/2144
- **Aviazione** → regolamento (UE) 2018/1139
- **Equipaggiamento marittimo** → direttiva n. 2014/90/UE

Chi riguarda e perchè

Aziende produttrici

- Ciò che produco lo creo in sicurezza

Aziende distributrici

- Ciò che rivendo deve essere marcato CE

Aziende acquirenti

- Ciò che acquisto e quello che mantengo devo aggiornarlo

CONFINDUSTRIA
VENETO EST

Rischi e Sanzioni

Stop alla vendita in UE

Danno reputazionale

Impatto su clienti/partner e trattative in corso

Sanzioni fino a 15M€ o 2,5%

Fino a 15 M€ o 2,5% fatturato worldwide per violazioni dei **requisiti essenziali** e di **Art. 13–14**.
Fino a 10 M€ o 2% per varie altre inadempienze procedurali/documentali.
Fino a 5 M€ o 1% per informazioni **false/incomplete** a organismi notificati o autorità.

CONFINDUSTRIA VENETO EST

Articoli focali

Articolo 13
Obblighi dei fabbricanti

Il fabbricante deve progettare, sviluppare e mantenere prodotti digitali sicuri per l'intero ciclo di vita, effettuando una valutazione dei rischi, gestendo vulnerabilità e aggiornamenti, garantendo documentazione tecnica, conformità CRA e cooperazione con le autorità.

Articolo 14
Obblighi di segnalazione dei fabbricanti

Il fabbricante deve notificare tempestivamente vulnerabilità sfruttate e incidenti significativi a ENISA/CSIRT, informare gli utenti e fornire aggiornamenti, mitigazioni e report entro le tempistiche previste.

Finestra transitoria

I prodotti già immessi sul mercato non devono essere rifatti da capo per continuare a esistere, **ma ci sono due limitazioni pesanti:**

Dal 11 settembre 2026	Dopo l'11 dicembre 2027
Scatta comunque l'Art. 14 anche se quel prodotto è "legacy" + Obbligo PATCH di sicurezza	Non si posso fare nuove vendite del prodotto legacy, e se sul legacy si fa una "modifica sostanziale", diventa un "nuovo" prodotto che rientra nel CRA

Modifica Sostanziale: Aggiunge una funzionalità o modifica la finalità del prodotto

Classificazione & Certificazione

Ordinari – Autocertificazione (+ indagini a tappeto)

- Es. gestionali ERP, CMS, App Mobile/Desktop, Videogiochi, Stampanti, IoT, Elettrodomestici/Allarmi Smart

Importanti Classe 1 – Organismi notificati

- Es. IAM, Browser, Password Manager, VPN, SIEM, Boot Manager, Router/Switch, Assistenti AI per case IoT (Alexa…)

Importanti Classe 2 – Organismi notificati

- Es. Hypervisor, Firewall, IDS, IPS, Microprocessori/Controllori a prova di manomissione

Critici – Certificazione europea di cybersicurezza

- Es. Dispositivi Hardware con cassette di sicurezza, Carte Intelligenti o dispositivi analoghi (passaporto, carta di credito, CIE…)

REGOLAMENTO DI ESECUZIONE (UE) 2025/2392

Certificazione & marcatura CE

- Security by design & by default, risk assessment, sicurezza intrinseca nella progettazione, SSDLC e niente vulnerabilità sfruttabili note al rilascio.
- Gestione vulnerabilità & supply-chain, SBOM, CVD, notifiche alle autorità e patch tempestive firmate.
- Update sicuri (auto-update on per default), logging utile, cifratura dati in transito e a riposo, reset di fabbrica a configurazioni sicure di default .
- Documentazione tecnica disponibile per audit, dichiarazione di conformità certificata e marcatura CE a livello software.

Security by Design & by Default: Principio per cui il software deve nascere sicuro fin dall'ideazione e avere impostazioni predefinite orientate alla sicurezza.
SSDLC: (Secure Software Developement Life Cycle) È un framework che integra pratiche, controlli e strumenti di sicurezza in ogni fase dello sviluppo del software
SBOM: (Software Bill of Materials - "Distinta base" del software) Un inventario completo delle librerie e componenti usati, utile a gestire rischi di supply-chain.
CVD: (Coordinated Vulnerability Disclosure) Processo di comunicazione e gestione delle vulnerabilità tra ricercatori, vendor e clienti.

Timeline

10 dicembre 2024	11 giugno 2026	11 settembre 2026	11 dicembre 2027
Entrata in vigore del CRA	Disposizioni su organismi di valutazione conformità (Capo IV)	Obblighi di segnalazione (Art. 14)	Piena applicazione del CRA

Per informazioni:
ricercainnovazione@confindustriavenest.it

Grazie per l’attenzione.