SECURE
Cyber Resilience for SMEs

Requisiti essenziali di cibersicurezza del CRA:

Allegato I, Parte I

20/10/2025

Funded by
the European Union

Dichiarazione sui finanziamenti dell'UE: Finanziato dall'Unione Europea con il GA n. 101190325. Le opinioni e i pareri espressi sono tuttavia esclusivamente dell'autore o degli autori e non riflettono necessariamente quelle dell'Unione Europea o del Centro europeo di competenza industriale, tecnologica e di ricerca sulla sicurezza informatica.
Né l'Unione Europea né l'autorità che eroga il finanziamento possono essere ritenute responsabili per esse.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Dichiarazione di non responsabilità dell'ECCC: Il progetto è sostenuto dal Centro europeo di competenza per la sicurezza informatica e dai suoi membri.

DISCLAIMER

Il presente documento fa parte del Deliverable D4.1 "Linee guida e materiali per la conformità CRA delle PMI" del progetto SECURE.

Questa versione è una traduzione dell'originale in lingua inglese; in caso di discrepanze o ambiguità interpretative, prevale la versione originale.

Primo autore: *Centre for Cybersecurity Belgium (CCB)*

Secondo autore: *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Indice

Elenco delle tabelle e delle figure

Abbreviazioni

API – Application Programming Interface

APT – Advanced Persistent Threats

BSIMM – Building Security in Maturity Model

CI/CD – Continuous Integration and Continuous Delivery/Deployment

CRA – Cyber Resilience Act

CVD – Coordinated Vulnerability Disclosure

CVE – Common Vulnerabilities and Exposures

CVSS – Common Vulnerability Scoring System

DAST – Dynamic Application Security Testing

DoS – Denial of Service

DREAD – Damage, Reproducibility, Exploitability, Affected Users, and Discoverability

ENISA – European Union Agency for Cybersecurity

EPSS – Exploit Prediction Scoring System

ETSI – European Technical Standard Institute

UE – Unione Europea

FIRST VCMM - FIRST Vulnerability Coordination Maturity Model

GDPR – General Data Protection Regulation

HTTPS/TLS – Hyper Text Protocol Secure/Transport Layer Security

ICS – Industrial control system,

IEC – International Electrotechnical Commission

IoT – Internet of Things

IPSec – Internet Protocol Security

ISO – International Standards Organisation

JTAG – Joint Test Action Group

LINDDUN – Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness and Non-compliance

MFA – Multi-Factor Authentication

MITRE ATT&CK – Adversarial Tactics, Techniques and Common Knowledge

MQTT – Message Queuing Telemetry Transport

NIST – National Institute of Standards and Technology (United States)

NIST SSDF – NIST Secure Software Development Framework

NTIA – National Telecommunications and Information Administration (United States)

OPENSSF VEX – Open-Source Security Foundation Vulnerability Exploitability eXchange

OS – Operating System

OTA – Over The Air

OWASP – Open Worldwide Application Security Project

OWASP ASVS – OWASP Application Security Verification Standard

OWASP SAMM – OWASP Software Assurance Maturity Model

PED – Prodotto con elementi digitali

PMI – Piccole Medie Imprese

PSIRT – Product Security Incident Response Team

SAST – Static Application Security Testing

SBOM – Software Bill of Materials

SCA – Software Composition Analysis

SIEM – Security Information and Event Management

SOC – Security Operations Centre

SQL – Structured Query Language

SSDLC – Secure Software Development Lifecycle

SSL – Secure Sockets Layer

STRIDE – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

TPM – Trusted Platform Module

UART – Universal Asynchronous Receiver-Transmitter

USB – Universal Serial Bus

VPN – Virtual Private Network

Introduzione

Al fine di ottemperare al **Cyber Resilience Act** (CRA), Regolamento (UE) 2024/2847, in qualità di produttore, il CRA stabilisce una serie di requisiti e obblighi. Tra questi, è fondamentale garantire che il prodotto con elementi digitali (PED) immesso sul mercato " sia stato progettato, sviluppato e prodotto conformemente ai requisiti essenziali di cibersicurezza di cui alla parte I dell'allegato I "[1] . L'allegato I contiene due parti: la parte I si concentra sui requisiti di cibersicurezza relativi alle proprietà del prodotto, mentre la parte II riguarda i requisiti di gestione delle vulnerabilità. La parte I si compone a sua volta di due punti, il primo dei quali stabilisce che

> *' I prodotti con elementi digitali sono progettati, sviluppati e prodotti in modo da garantire un livello adeguato di cibersicurezza in base ai rischi '*[2] .

Il punto 2 specifica i requisiti che i vostri prodotti devono soddisfare.

La presente linea guida, elaborata nell'ambito del **progetto SECURE**[3] con l'obiettivo di **sostenere le piccole e medie imprese (PMI)**, approfondisce entrambi i punti dell'allegato I, parte I, fornendo **suggerimenti pratici e tecnici non esaustivi, esempi e approcci per sostenere la conformità a ciascun requisito**. È importante notare che qualsiasi riferimento a norme, strumenti e quadri esistenti è di **natura** puramente **indicativa,** con l'intento di rendere i requisiti CRA il più possibile intellegibili. Le raccomandazioni formulate si basano sulle migliori pratiche riconosciute e approcci comuni. Sia gli strumenti citati nella linea guida che la linea guida stessa saranno aggiornati man mano che lo sviluppo di norme CRA specifiche e delle misure di attuazione della Commissione europea progrediranno ulteriormente durante il periodo di adattamento dal 2024 al 2027.

[1] Art. 13(1), CRA "*All'atto dell'immissione sul mercato di un prodotto con elementi digitali, i fabbricanti assicurano che esso sia stato progettato, sviluppato e prodotto conformemente ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I*"..

[2] Allegato I, parte I, paragrafo 1, CRA.

[3] Il progetto "Strengthening EU SMEs Cyber Resilience" (SECURE) offre sostegno finanziario e orientamento alle PMI per conformarsi al CRA.

Requisiti essenziali di cibersicurezza del CRA: Allegato I, Parte I

1. Approccio alla cibersicurezza basato sul rischio

Il punto 1 dell'allegato I, parte I, stabilisce che

> *' I prodotti con elementi digitali sono progettati, sviluppati e prodotti in modo da garantire **un livello adeguato di cibersicurezza in base ai rischi** "*[4] .

Questo punto è fondamentale per il CRA e si basa sul principio della "sicurezza fin dalla progettazione e per impostazione predefinita". In sostanza, significa che è necessario sviluppare per il proprio prodotto un **approccio alla cibersicurezza basato sul rischio**. Questo approccio personalizzato basato sul rischio deve essere sostenibile, documentato e proporzionato. Pensate alla conformità al CRA come a un "percorso tracciabile":

contesto del prodotto → rischio → controlli → prova

La logica di questo percorso deve essere diligentemente documentata nella documentazione tecnica obbligatoria[5], fondamentale per la conformità e la verificabilità.

In pratica, i produttori devono:

1. Valutare i rischi di cibersicurezza associati al PDE durante il suo ciclo di vita;
2. Adattare le misure di sicurezza al livello di rischio (ad esempio, un termostato intelligente rispetto a un sistema di controllo industriale);
3. Considerare i modelli di minaccia, le superfici di attacco e il potenziale impatto sugli utenti e sui sistemi.

Un primo passo fondamentale per la conformità al CRA è quindi quello di condurre una **valutazione dei rischi** per il proprio PED. Questo capitolo approfondisce come condurre tale valutazione dei rischi, illustrando possibili approcci e offrendo suggerimenti tecnici.

Prima di entrare nel dettaglio, di seguito viene fornita una panoramica **sulla valutazione dei rischi 101**. Gli elementi vengono riproposti in modo più dettagliato nel primo capitolo di questa linea guida, che si consiglia di consultare. Tuttavia, per motivi di accessibilità, il riassunto semplificato illustra come vengono generalmente affrontate le valutazioni dei rischi[6] .

[4] Allegato I, parte I, punto 1, CRA.

[5] Art. 31, CRA.

[6] È fondamentale notare che la Commissione europea deve ancora elaborare orientamenti ufficiali su come condurre la valutazione dei rischi per il CRA. Gli orientamenti forniti nel presente documento riassumono le

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Valutazione dei rischi 101

Quando si effettua una valutazione dei rischi, bisogna considerare **sei fasi**:

1) Identificazione delle **risorse** e **delle minacce** = *identificare ciascuna risorsa (ciò che deve essere protetto) in base alla sua esposizione a una minaccia (ciò che potrebbe andare storto);*
2) Valutazione delle **vulnerabilità** = *valutare le vulnerabilità*;
3) Considerazione e valutazione degli **impatti** e **della probabilità** = *tracciare gli impatti e la probabilità delle vulnerabilità → questo porta a 'rischi' specifici*;
4) **Analisi** e **accettazione** dei rischi = *tracciare ciascun rischio e considerare il rispettivo livello di accettazione per stabilire le priorità delle azioni da intraprendere;*

Oltre a questa valutazione dei rischi, due fasi finali includono:

5) Attuazione delle **misure di mitigazione** = *selezionare e applicare controlli di sicurezza per ciascun rischio;*
6) Monitoraggio e rivalutazione = *monitorare le minacce e i rischi in ogni fase del ciclo di vita dei PED e mantenere aggiornata la valutazione dei rischi.*

Per **le fasi da uno a tre**, è possibile sviluppare una **matrice** che consenta di classificare ciascuna minaccia, vulnerabilità e impatto in base a un determinato livello di rischio e punteggio. A tal fine, è necessario innanzitutto definire il significato di ciascun livello (e punteggio) attraverso tabelle descrittive[7].

- Basso
- Basso-medio
- Medio
- Medio-alto
- Alto

Tabella1 :
Matrice di esempio

Rischio/Minaccia	Minaccia 1	Minaccia 2	Punteggio
Alto			10
Medio-alto			
Medio			
Basso Medio			
Basso			0

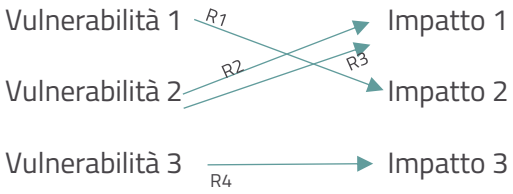
Collegando le vulnerabilità agli impatti è possibile visualizzare i diversi rischi (R):

fasi principali di qualsiasi approccio di valutazione dei rischi. È possibile utilizzare qualsiasi altro approccio, standard o metodologia, purché sia in linea con l'approccio riportato.

[7] Ad esempio, per quanto riguarda il verificarsi di una minaccia, un livello "basso" potrebbe significare una minaccia che può verificarsi una volta ogni 10 anni, mentre un livello "alto" potrebbe significare una minaccia che può verificarsi una volta alla settimana. Sono necessarie tabelle descrittive separate per le minacce, le vulnerabilità, gli impatti e i rischi: questi ultimi supportano la definizione del livello di accettazione.

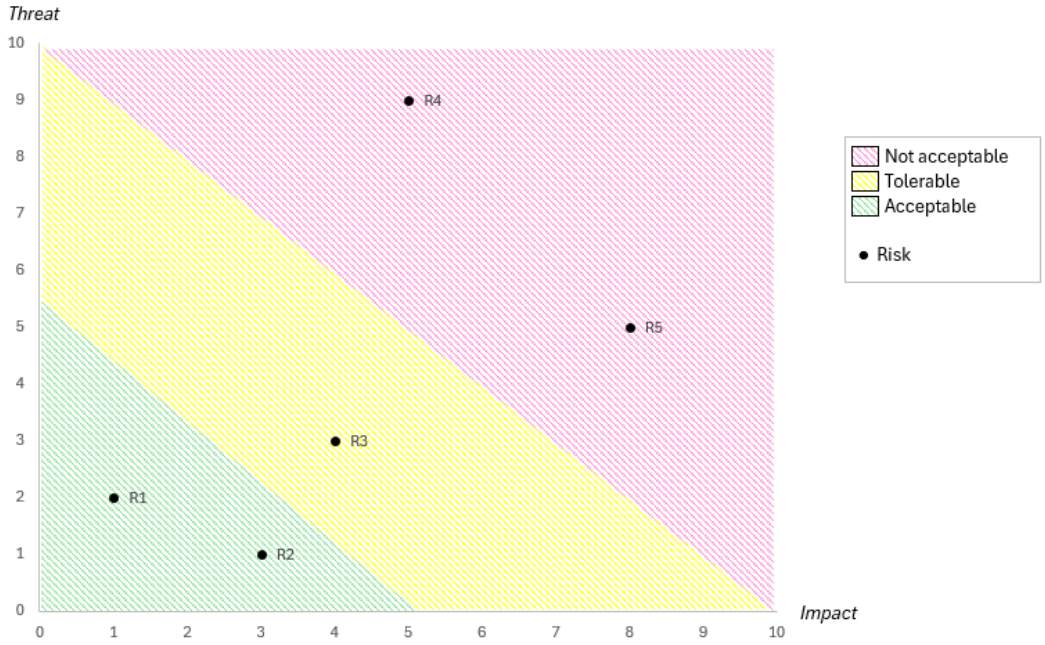
Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Figura1 :
Visualizzazione dei rischi



Per **la fase quattro**, è importante tracciare i rischi incontrati e definire il rispettivo livello di accettazione di tali rischi; spesso ciò avviene tramite un codice cromatico, ad esempio:

Figura2 :
Grafico di accettazione del rischio



Ciò consente di stabilire le priorità su cui intervenire e di sviluppare misure di mitigazione e controlli di sicurezza per ciascun rischio, al fine di ridurre i rischi residui a un livello accettabile.

Come affermato in precedenza, questi elementi della valutazione dei rischi sono trattati in modo più dettagliato di seguito (capitolo 1 della presente linea guida) fornendo esempi e strumenti e quadri di riferimento raccomandati a supporto.

1.1. Valutazione del rischio di cibersicurezza nel ciclo di vita del prodotto

Poiché i rischi di cibersicurezza associati al vostro PED devono essere valutati durante tutto il ciclo di vita del prodotto, la conduzione di una **valutazione dei rischi di cibersicurezza nel ciclo di vita**

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

del prodotto comporta **l'identificazione, l'analisi e la mitigazione dei rischi di sicurezza informatica** in ogni fase del ciclo di vita di un prodotto:

1. Progettazione
2. Sviluppo
3. Produzione
4. Implementazione
5. Funzionamento e manutenzione
6. Fine del ciclo di vita

La valutazione dei rischi deve essere aggiornata continuamente durante tutto il "periodo di supporto"[8], un periodo di almeno cinque anni (o, se la durata di vita del prodotto è inferiore a cinque anni, almeno fino alla fine della durata di vita del prodotto).

1.1.1. Fasi chiave nella valutazione del rischio lungo il ciclo di vita del prodotto

Quando si effettua la valutazione dei rischi, è possibile prendere in considerazione sei passaggi, ciascuno dei quali è chiarito nella tabella 2 riportata di seguito.

Tabella 2 :
Fasi chiave nella valutazione del rischio lungo il ciclo di vita del prodotto

Fase chiave	Chiarimenti e suggerimenti
1. Identificare le risorse e le minacce	Distinguere tra: • Risorse: cosa deve essere protetto? ad esempio firmware, dati utente, canali di comunicazione. • Minacce: cosa potrebbe andare storto? ad es. iniezione di malware, accesso non autorizzato.
2. Analizzare le vulnerabilità	Utilizzare strumenti quali: • Analisi statica del codice;

[8] Art. 13, paragrafo 8, CRA: Il periodo di assistenza deve essere determinato dal fabbricante, tenendo conto del tempo durante il quale si prevede che il prodotto sarà utilizzato, delle aspettative degli utenti, della natura (destinazione d'uso) del prodotto e del diritto dell'Unione.

	• Software composition analysis (SCA); • Test di penetrazione; • Modelli di minaccia[9] (ad esempio STRIDE, DREAD). Nota: CVSS e STRIDE possono essere utilizzati insieme in un processo di modellizzazione delle minacce. STRIDE può aiutare a identificare potenziali minacce, mentre CVSS può essere utilizzato per valutare la gravità delle vulnerabilità correlate a tali minacce, consentendo una migliore definizione delle priorità degli interventi di mitigazione[10] .
3. Valutare l'impatto e la probabilità del rischio	Utilizzare una matrice di rischio per stabilire le priorità in base a: • Impatto (ad esempio, violazione dei dati, guasto del sistema); • Probabilità (ad esempio, exploit noto, superficie di attacco).
4. Analizzare i rischi e la loro accettabilità	Definire il proprio livello di accettazione e tracciare i rischi in base alla minaccia e all'impatto per classificare e stabilire le priorità delle azioni da intraprendere.
5. Implementare le misure di mitigazione	Applicare controlli di sicurezza: ad esempio crittografia, autenticazione, avvio sicuro.
6. Monitorare e rivalutare	Monitorare continuamente le nuove minacce e aggiornare di conseguenza le valutazioni dei rischi.

1.1.2. Casi d'uso per fase del ciclo di vita del prodotto

Per rendere più tangibile la valutazione del rischio lungo il ciclo di vita del prodotto, la tabella 3 riportata di seguito offre una panoramica dei casi d'uso, compresi un esempio di rischio e una strategia di mitigazione, per ogni fase del ciclo di vita del prodotto.

[9] La modellizzazione delle minacce è ulteriormente discussa al punto 1.3.1

[10] Il CVSS valuta la gravità della vulnerabilità, mentre il rischio tiene conto anche dell'impatto sul business e della probabilità.

Tabella3 :
Casi d'uso per fase del ciclo di vita del prodotto

Fase del ciclo di vita del prodotto	Caso d'uso	Rischio	Mitigazione
Progettazione	Telecamera domestica intelligente	Accesso non autorizzato alle immagini video	Implementare la crittografia end-to-end e impostazioni predefinite sicure
Sviluppo	Firmware del dispositivo	Vulnerabilità di overflow del buffer	Utilizzare pratiche di codifica sicure e scansioni automatiche delle vulnerabilità
Produzione	Gateway IoT industriale	Compromissione durante la produzione	Catena di approvvigionamento sicura e radice hardware di fiducia, sigilli antimanomissione e provisioning sicuro
Implementazione	Router consumer	Credenziali predefinite lasciate invariate	Modifica obbligatoria della password al primo utilizzo
Funzionamento e manutenzione	Veicolo connesso	Vulnerabilità software non corrette	Aggiornamenti OTA (Over-The-Air) con controlli di integrità
Fine del ciclo di vita	Termostato intelligente	Dispositivo abbandonato con firmware vulnerabile	Fornire istruzioni sicure per la dismissione e la cancellazione dei dati, politica di aggiornamento della sicurezza alla fine del ciclo di vita del prodotto ed esportazione dei dati per gli utenti

1.1.3. Strumenti e framework di supporto

L'elenco riportato di seguito evidenzia diversi strumenti e framework che possono fornire supporto, sebbene un elenco più esaustivo e standard armonizzati siano ancora in fase di sviluppo.

- ISO/IEC 27005 – Gestione dei rischi
- NIST SP 800-30 – Metodologia di valutazione dei rischi
- ENISA Threat Landscape – Informazioni aggiornate sulle minacce
- OWASP ASVS – Verifica della sicurezza delle applicazioni
- Modello STRIDE
- Modello di valutazione dei rischi DREAD
- LINDDUN
- CVSS

1.2. Misure di sicurezza personalizzate

La seconda dimensione di un approccio alla sicurezza informatica basato sul rischio consiste nell'adattare le misure di sicurezza al livello di rischio. L'adattamento deve essere proporzionato ai rischi identificati nell'allegato I, parte I, punto 1. Analizziamo il significato di questo concetto attraverso sei chiari passaggi, principi e due esempi di prodotti: un termostato intelligente (rischio da basso a moderato) e un sistema di controllo industriale (ICS- industrial control system) (rischio elevato).

1.2.1. Eseguire la classificazione del rischio del prodotto

Quando si esegue una valutazione del rischio specifica per un prodotto, è importante considerare le seguenti dimensioni.

- **Esposizione alle minacce**: il prodotto è
    - Connesso a Internet?
    - Ampiamente diffuso?
    - Accessibile al pubblico?
    - Uso previsto vs. uso improprio ragionevolmente prevedibile?
- **Impatto della compromissione**: quale sarebbe l'impatto sulla sicurezza, sulle perdite finanziarie, sulla privacy, sulle infrastrutture critiche?

- **Attrattività dell'attacco:** potrebbe essere un trampolino di lancio per un movimento laterale?
- **Profilo dell'utente:** consumatore, PMI, operatore di infrastrutture critiche?

Sulla base di queste considerazioni, il prodotto può essere classificato come a basso rischio - accettabile, a rischio moderato - tollerabile o ad alto rischio - inaccettabile[11].

1.2.2. Definizione degli obiettivi di sicurezza per livello di rischio

La tabella 4 illustra come gli obiettivi di sicurezza possano essere adattati al livello di rischio del prodotto precedentemente stabilito.

Tabella4 :
Obiettivi di sicurezza per livello di rischio

Livello di rischio	Obiettivi di sicurezza
Basso (ad es. termostato intelligente)	• Prevenire sfruttamenti banali; • Garantire la privacy; • Mantenere la capacità di aggiornamento.
Moderato	• Rilevare e mitigare i vettori di attacco noti; • Applicare l'autenticazione; • Garantire la sicurezza delle comunicazioni.
Elevato (ad es. ICS)	• Postura di sicurezza rafforzata; • Difesa approfondita; • Fiducia nella catena di approvvigionamento; • Avvio sicuro; • Monitoraggio degli incidenti.

[11] Ciò richiede di definire in anticipo come valutare questi elementi utilizzando una matrice e come i punteggi corrispondono ai livelli di rischio. Per una classificazione più precisa, è possibile considerare cinque livelli di rischio invece di tre: basso, medio-basso, medio, medio-alto, alto.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.2.3. Correlazione tra i requisiti essenziali CRA e il livello di rischio

A seconda del livello di rischio, i requisiti essenziali CRA possono avere diverse applicazioni pratiche. La tabella 5 illustra questo aspetto per i livelli di rischio basso e alto e i rispettivi casi di prodotto di esempio, ossia un termostato intelligente e un ICS.

Tabella5 :
Requisiti essenziali CRA in base al livello di rischio

Requisito CRA	Rischio basso	Rischio elevato
Sicurezza intrinseca e impostazioni predefinite	Disabilitare le porte di debug; impostazioni predefinite rigorose	Elenco completo dei componenti software (SBOM[12]); avvio sicuro; sistema operativo rinforzato
Gestione delle vulnerabilità	Politica CVD pubblica; security.txt; monitoraggio della posta in arrivo; meccanismo di patch	Divulgazione coordinata; PSIRT; risposta rapida
Registrazione e monitoraggio	Registri eventi locali	Registrazione remota; integrazione SIEM
Controllo degli accessi	Autenticazione tramite PIN o app	Accesso basato sui ruoli; MFA; privilegio minimo
Meccanismo di aggiornamento	Aggiornamenti OTA con il consenso dell'utente	Aggiornamenti firmati; fail-safe rollback
Protezione da accessi non autorizzati	Regole firewall di base	Sistemi di rilevamento delle intrusioni nell'host; controlli di integrità del firmware

[12] SBOM ulteriormente chiarito nella sezione 4.1.

1.2.4. Utilizzo della modellazione delle minacce per perfezionare le misure

Per la modellazione delle minacce, è possibile applicare STRIDE, LINDDUN o gli alberi di attacco per convalidare l'adeguatezza dei controlli.

Per i casi di prodotti di esempio, ciò significa:

- **Termostato intelligente**: concentrarsi su spoofing, manomissione e denial of service;
- **ICS**: coprire tutte le minacce STRIDE e le minacce persistenti avanzate (APT- advanced persistent threats).

1.2.5. Selezionare i controlli in base al livello di rischio

La tabella 6 suggerisce diversi controlli per dominio di sicurezza per i casi pratici di esempio, termostato intelligente (rischio basso) e ICS (rischio elevato).

Tabella6 :
Controlli per livello di rischio

Dominio di sicurezza	Rischio basso	Rischio elevato
Autenticazione	Autenticazione basata su app; modifica della password predefinita	MFA; controllo degli accessi basato su certificati
Sicurezza del firmware	Firmware firmato; aggiornamenti OTA; fail-safe rollback	Avvio sicuro; integrazione TPM; garanzia della catena di fornitura
Comunicazione	HTTPS/TLS	VPN; IPSec; segmentazione di rete; zero trust
Monitoraggio	Rotazione di base dei log	Registrazione in tempo reale; rilevamento delle anomalie; integrazione SOC; log sincronizzati nel tempo
Interfaccia utente	Pannello di impostazioni semplice	Console di amministrazione dettagliata; funzionalità di audit trail

1.2.6. Prova di conformità dei documenti

Come affermato in precedenza, un elemento chiave per la conformità con il CRA è la documentazione delle seguenti prove, come minimo:

- Motivazioni della classificazione dei rischi;
- Decisioni di controllo legate ai rischi;
- Risultati dei test e della convalida;
- Politiche di aggiornamento e gestione delle vulnerabilità;
- Allineamento del ciclo di vita dello sviluppo sicuro (ad esempio, ISO/IEC 27034, IEC 62443-4-1);
- Matrice di tracciabilità che mappa rischi → controlli → test di verifica → prove (da conservare nella documentazione tecnica)

1.2.7. Esempi

La tabella 7 fornisce ulteriori esempi di misure di attuazione per i casi pratici a basso e alto rischio.

Tabella7 :
Misure di implementazione per livello di rischio

Prodotto	Termostato intelligente	ICS
Considerazioni sul rischio	• Connesso a Internet, controlla il riscaldamento nelle abitazioni private; • Sensibile alla privacy, ma con un impatto basso in termini di sicurezza o economico.	• Utilizzato in infrastrutture critiche (ad es. trattamento delle acque); • Elevato impatto sulla sicurezza e sul funzionamento.
Classificazione del rischio	Rischio basso	Rischio elevato

Misure di implementazione	• Modifica della password predefinita al primo utilizzo; • Comunicazione HTTPS con il backend; • Aggiornamenti firmware firmati; • Registrazione solo locale[13]; • Modulo di contatto di base per le vulnerabilità.	• Hardware sicuro fin dalla progettazione con TPM; • Avvio sicuro e aggiornamenti firmati con rollback; • Accesso basato sui ruoli e MFA; • Segmentazione di rete e regole firewall; • Registrazione su SIEM centrale; • SBOM completo con ogni aggiornamento; • Processo coordinato di divulgazione delle vulnerabilità (CVD);

1.3. Considerazione dei modelli di minaccia, delle superfici di attacco e del potenziale impatto su utenti e sistemi

Il CRA sottolinea l'importanza di un approccio alla cibersicurezza basato sul rischio. Come illustrato sopra, ciò significa che i produttori dovrebbero adattare le loro misure di sicurezza alle minacce realistiche, ai punti di esposizione e alle potenziali conseguenze per gli utenti e i sistemi. Non si tratta di una direttiva vuota, ma di un invito ad adottare un approccio concreto e consapevole in base al contesto. Per attuare efficacemente questo obbligo, è necessario considerare insieme tre concetti chiave: modelli di minaccia, superfici di attacco e analisi dell'impatto, che costituiscono la terza e ultima dimensione dell'approccio alla cibersicurezza basato sul rischio. Esaminiamo questi elementi uno per uno e vediamo come si integrano tra loro.

[13] Da notare: i registri solo locali riducono il valore forense, si raccomanda l'esportazione facoltativa previo consenso dell'utente.

1.3.1. Modelli di minaccia: chi attacca, perché e come?

La modellizzazione delle minacce è un processo strutturato in cui si identifica chi potrebbe attaccare il proprio prodotto, come lo farebbe e quale sarebbe la sua motivazione. Si pensi agli script kiddies, ai criminali informatici organizzati o persino agli attori statali. Le loro motivazioni variano dal guadagno finanziario al sabotaggio o allo spionaggio, e le loro competenze vanno da quelle di base a quelle avanzate.

Per strutturare questo processo, è possibile utilizzare metodi quali:

- STRIDE;
- MITRE ATT&CK per le tecniche di attacco note;
- LINDDUN per le minacce orientate alla privacy;
- Alberi di attacco o catene di attacchi informatici per mappare i percorsi di attacco.

Tornando agli esempi pratici, ciò significa:

- **Termostato intelligente**: le minacce sono spesso limitate a vicini curiosi o attacchi casuali, in cui qualcuno potrebbe manipolare le impostazioni di temperatura o il consumo energetico;
- **ICS** (ad esempio, in un impianto di trattamento delle acque): le minacce sono fondamentalmente diverse, ad esempio gruppi APT o bande di ransomware che cercano di sabotare i processi fisici o di chiudere un'attività.

Il risultato della modellazione delle minacce è un elenco chiaro di obiettivi di sicurezza specifici per il prodotto e il suo ambiente.

1.3.2 Superfici di attacco: dove può entrare un aggressore?

Una superficie di attacco è l'insieme di tutti i punti in cui un aggressore può interagire con il sistema o influenzarlo. Maggiore è il numero di interfacce e punti di accesso, maggiore è il rischio.

Le superfici di attacco tipiche sono:

- Interfacce di rete come Wi-Fi, Bluetooth, MQTT o HTTP;
- Interfacce locali come USB, UART, JTAG (per il debug);
- Meccanismi di aggiornamento come OTA o aggiornamenti USB;
- API, app mobili, dashboard cloud:
- Componenti esterni della catena di fornitura.

L'analisi di queste superfici comporta la verifica di quali componenti sono esposti inutilmente, quali

servizi sono abilitati ma non necessari e se l'accesso è adeguatamente protetto. Idealmente, è opportuno limitare la superficie di attacco tramite:

- Principi di sicurezza quali esposizione minima, impostazioni predefinite sicure e rafforzamento;
- Disabilitazione delle porte o dei servizi inutilizzati;
- autenticazione e crittografia su ogni interfaccia.

Applicato agli esempi, ciò significa:

- **Termostato intelligente**: utilizzerà tipicamente il Wi-Fi e possibilmente il Bluetooth, con una semplice connessione cloud - Le interfacce di debug possono essere aperte durante i test e devono essere disattivate in produzione;
- **Gateway ICS**: sarà protetto fisicamente, con aggiornamenti USB schermati, reti segmentate e nessuna interfaccia esterna.

È quindi essenziale mappare attentamente la superficie di attacco per sapere dove è realmente necessaria la sicurezza.

1.3.3 Analisi dell'impatto: cosa succede se le cose vanno male?

Il passo finale consiste nel determinare il potenziale impatto di un attacco riuscito. Il CRA richiede che le misure di sicurezza siano proporzionate a tale impatto. Ciò include non solo i danni tecnici, ma anche:

- Pericoli per l'utente (ad esempio, lesioni dovute al controllo della temperatura);
- Violazione della privacy (ad esempio, deduzione delle abitudini di vita dai dati del termostato);
- Perdita di disponibilità o continuità operativa (ad esempio, chiusura della fabbrica);
- Responsabilità legale (ad esempio, violazione del CRA o del GDPR);
- Danno alla reputazione e rischio di mercato.

L'impatto deve essere considerato su più dimensioni:

- Utente: da piccoli inconvenienti a situazioni potenzialmente letali;
- Organizzazione: dall'aumento del carico di lavoro dell'helpdesk all'interruzione dell'attività;
- Società: da bug innocui a minacce alle infrastrutture critiche.

Anche in questo caso, la proporzionalità è fondamentale: un robot giocattolo non richiede lo stesso livello di sicurezza di una pompa medica.

1.3.4 Integrazione: dall'analisi alle misure

Quando questi tre elementi fondamentali si uniscono - modello di minaccia, superficie di attacco e impatto - si crea una solida base per personalizzare le misure di sicurezza.

Un approccio tipico è il seguente:

1. Definire l'uso e il contesto del prodotto;
2. Eseguire la modellizzazione delle minacce per comprendere gli attori, i motivi e i percorsi di attacco;
3. Mappare la superficie di attacco e identificare le vulnerabilità;
4. Analizzare l'impatto su utenti, organizzazioni e società;
5. Selezionare le misure in base al rischio (rischio = probabilità × impatto);
6. Documentare tutto per la conformità CRA e le verifiche.

Per i casi pratici, ciò significa:

- **Termostato intelligente**: ottiene crittografia, politica di password complesse, aggiornamenti OTA firmati e una semplice informativa sulla privacy.
- **Gateway ICS**: ottiene avvio sicuro, root of trust hardware, reti segmentate, registrazione SIEM, gestione dei ruoli e SBOM completo con monitoraggio delle vulnerabilità.

2. Progettazione e sviluppo sicuri

Tornando al punto 1 dell'Allegato I, Parte I del CRA, l'approccio alla cibersicurezza basato sul rischio e la personalizzazione si fondano sul principio della "sicurezza fin dalla progettazione e per impostazione predefinita", ovvero i PED devono essere progettati e sviluppati in modo da essere sicuri fin dall'inizio. Non è più sufficiente aggiungere la sicurezza come livello opzionale a posteriori; essa deve essere una parte essenziale dell'intero processo di sviluppo del prodotto. "Sicurezza fin dalla progettazione", "sicurezza predefinita" e l'uso di pratiche di sviluppo sicure costituiscono il nucleo di una strategia resiliente per i prodotti digitali. Essi garantiscono che la sicurezza non sia un ripensamento, ma una parte strutturalmente e dimostrabilmente integrata nel prodotto, esattamente come richiesto dal CRA.

Utilizzando standard internazionali come IEC 62443, ISO 27034, OWASP e le linee guida ENISA, i produttori possono applicare in modo efficiente questi principi rispettando al contempo i loro obblighi di conformità.

I prodotti devono essere:

1. **Sicuri fin dalla progettazione**: la sicurezza è integrata sin dalle prime fasi di sviluppo;
2. **sicuri per impostazione predefinita**: le impostazioni predefinite devono dare priorità alla sicurezza (ad esempio, password complesse, porte aperte minime, ecc.)
3. **Sviluppati in modo sicuro**: utilizzando pratiche di codifica sicure e modelli di minaccia.

2.1. Security by design –Sicurezza fin dalla progettazione

"Security by design – Sicurezza fin dalla progettazione" significa che la sicurezza informatica viene presa in considerazione fin dalla fase concettuale nelle decisioni relative all'architettura, alla selezione dei componenti e all'interazione tra i sottosistemi. La sicurezza deve essere fondamentale quanto la funzionalità o la facilità d'uso.

Esempio pratico:

Quando si progetta un modulo di serratura intelligente, vengono prese immediatamente le seguenti decisioni:

- Applicare la crittografia end-to-end tra l'app e la serratura;
- Memorizzare le chiavi in modo sicuro in un TPM o Secure Element;
- Disabilitare fisicamente le porte di debug dopo la produzione.

Gli standard e le linee guida pertinenti a questo proposito includono:

- IEC 62443-4-1: richiede l'integrazione della sicurezza nel ciclo di vita del software;
- ISO/IEC 27034: sicurezza delle applicazioni nel ciclo di vita dello sviluppo del software;
- NIST SP 800-218 SSDF;
- ENISA Buone pratiche per lo sviluppo di software sicuro.

2.2. Security by default - Sicurezza senza configurazione da parte dell'utente

"Security by default – Sicurezza senza configurazione da parte dell'utente" significa che i prodotti vengono forniti con la configurazione più sicura come standard. L'utente non dovrebbe dover indovinare se la sicurezza è abilitata. La sicurezza è la base, non un'opzione nè una "impostazione avanzata".

Esempi di impostazioni predefinite sicure:

- Nessuna impostazione predefinita condivisa, impostazione obbligatoria delle credenziali al primo avvio o accoppiamento senza password con fattori di sicurezza;
- Apertura solo delle porte di rete necessarie (principio di esposizione minima);
- Aggiornamenti del firmware firmati e verificati di default;
- Registrazione e tracciabilità di audit abilitate di default per le funzioni critiche.

Le linee guida pertinenti a questo proposito includono:

- OWASP Secure Configuration: Best practice per impostazioni predefinite sicure;
- NIST SP 800-128: Guida per la gestione della configurazione incentrata sulla sicurezza.

2.3. Pratiche di codifica sicura

La CRA richiede che lo sviluppo del software sia effettuato in conformità con pratiche di sviluppo sicure comprovate e con continua attenzione alle minacce. Ciò significa, tra le altre cose:

Codifica sicura:

- Convalida degli input (contro SQL injection, buffer overflow, ecc.);
- Utilizzo di librerie sicure e crittografia;
- Test di fuzz e analisi statica del codice.

Modellazione delle minacce:
Per ogni componente del software, è necessario valutare quanto segue:

- Chi potrebbe attaccarlo?
- Come potrebbe farlo?
- Quale sarebbe l'impatto?

Framework come STRIDE (Microsoft), OWASP Threat Dragon e MITRE ATT&CK possono aiutare a identificare sistematicamente le vulnerabilità e i percorsi di attacco.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Gli standard e le linee guida pertinenti a questo proposito includono:

- OWASP Secure Coding Practices Checklist;
- ISO/IEC 27001 Allegato A.14: Requisiti di sicurezza nello sviluppo;
- Linee guida ENISA sulla modellizzazione delle minacce (2022);
- BSI TR-03161 (Germania): Sviluppo di software sicuro.

2.4. In termini concreti per i produttori

In sintesi, un'organizzazione che desidera sviluppare PED conformi a CRA dovrebbe:

- Adottare un ciclo di vita dello sviluppo software sicuro (SSDLC), come descritto nella norma IEC 62443-4-1 o NIST SP 800-218 SSDF;
- Disporre di una politica di revisione e test del codice incentrata sulle vulnerabilità (SAST, DAST, fuzzing);
- Applicare sistematicamente la modellazione delle minacce a ogni componente importante;
- Fornire prodotti con porte chiuse standard, registrazione abilitata e porte di accesso sicure;
- Adottare una funzione PSIRT con ruoli chiari e processi di reperibilità;
- Definire i controlli di qualità della sicurezza in CI/CD (SAST, DAST, SCA, scansione dei segreti) con politiche di fallimento della compilazione.

3. Gestione della sicurezza del ciclo di vita

Oltre alla progettazione, allo sviluppo e alla produzione sicuri dei PED, il vostro prodotto deve anche rimanere sicuro durante tutto il suo ciclo di vita. I prodotti digitali si evolvono e così deve fare anche la loro sicurezza. Ciò significa che la sicurezza deve essere gestita e considerata in modo continuo anche dopo che il PED è stato immesso sul mercato.

[14]Concretamente, i produttori sono tenuti a:

1. Monitorare continuamente le vulnerabilità;
2. Fornire tempestivamente aggiornamenti e patch di sicurezza;

[14] Sebbene i requisiti per la gestione delle vulnerabilità siano trattati in modo approfondito nell'allegato I, parte II, essi derivano dai punti 1 e 2 dell'allegato I, parte I, e sono quindi già stati affrontati nella presente linea guida.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3. Mantenere una politica di divulgazione delle vulnerabilità e comunicare i rischi in modo trasparente agli utenti e alle autorità di regolamentazione.

3.1. Monitoraggio continuo delle vulnerabilità

Una volta che un prodotto è sul mercato, i produttori devono continuare a individuare le vulnerabilità in modo attivo e sistematico. Questo include:

- Monitorare i database delle vulnerabilità, come il database europeo delle vulnerabilità[15];
- Monitorare gli avvisi dei fornitori;
- Monitoraggio delle vulnerabilità e delle esposizioni comuni (CVE - Common Vulnerabilities and Exposures) relative ai componenti o alle librerie utilizzati;
- Utilizzo di SBOM per identificare e tracciare le dipendenze;
- Monitoraggio interno delle nuove vulnerabilità attraverso programmi di bug bounty, test di penetrazione o audit di sicurezza.

Esempio:

Un produttore di telecamere di rete utilizza moduli firmware open source. Il database CVE rivela che uno di questi moduli contiene una vulnerabilità critica (ad esempio CVE-2023-XXXXX). Il produttore è tenuto a monitorare e valutare queste informazioni e, se del caso, ad adottare le misure appropriate.

Fonti rilevanti a questo proposito includono:

- CVE;
- EPSS (Exploit Prediction Scoring System);
- Linee guida ENISA per la gestione delle vulnerabilità;
- ISO/IEC 30111: Processi di gestione delle vulnerabilità.

[15] Art. 17(5), CRA "*Dopo la messa a disposizione di un aggiornamento di sicurezza o l'adozione di un'altra forma di misure correttive o di attenuazione, l'ENISA, d'intesa con il fabbricante del prodotto con elementi digitali interessato, aggiunge la vulnerabilità notificata a norma dell'articolo 14, paragrafo 1, o dell'articolo 15, paragrafo 1, del presente regolamento alla banca dati europea delle vulnerabilità istituita a norma dell'articolo 12 della direttiva (UE) 2022/2555*"..

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3.2. Aggiornamenti di sicurezza e patch tempestivi

Il CRA richiede ai produttori di rispondere rapidamente alle vulnerabilità note e di distribuire aggiornamenti di sicurezza gratuiti ed efficaci per tutto il periodo di assistenza.

Questi aggiornamenti devono:

- Essere firmati digitalmente e convalidati;
- Avere un meccanismo di fail-safe rollback;
- Essere installabili automaticamente con opzioni di rinuncia e/o con un'interazione minima da parte dell'utente;
- Rimanere disponibili per almeno 10 anni dopo il rilascio o per il resto del periodo di assistenza (a seconda di quale dei due sia più lungo).

Esempio:

Un produttore di termostati intelligenti scopre una vulnerabilità nello stack Wi-Fi. Entro due settimane viene sviluppata, testata e distribuita una patch di sicurezza tramite un aggiornamento OTA firmato. Gli utenti ricevono una chiara notifica e l'aggiornamento viene installato automaticamente al riavvio del dispositivo.

Fonti rilevanti a questo proposito includono:

- ISO/IEC 29147: Divulgazione coordinata delle vulnerabilità;
- NIST SP 800-40: Guida alla gestione delle patch aziendali;
- ETSI EN 303 645: Linee guida di sicurezza per l'IoT consumer (compresi i meccanismi di aggiornamento del software).

3.3. Segnalazione delle vulnerabilità e politica di comunicazione trasparente

La trasparenza è essenziale. Il CRA richiede ai produttori di:

- Pubblicare una politica CVD;
- Fornire un punto di contatto (ad es. security@company.eu) per le segnalazioni;

- Informare rapidamente gli utenti e le autorità come l'ENISA o l'autorità di vigilanza nazionale in caso di rischi gravi;
- Comunicare in modo trasparente in merito alle patch disponibili, alle misure di mitigazione e ai rischi residui.

Esempio:

Un hacker etico segnala una vulnerabilità critica in un sistema di allarme connesso tramite la piattaforma CVD pubblica del produttore. Entro 72 ore viene confermata la ricezione e, dopo un'analisi interna, l'ENISA viene informata tramite la piattaforma unica di segnalazione dell'ENISA (endpoint nazionali). Entro tre settimane viene distribuita una patch e tutti gli utenti vengono informati del rischio e della soluzione tramite e-mail e notifiche dell'app.

Fonti rilevanti a questo proposito includono:

- FIRST Vulnerability Coordination Maturity Model (VCMM);
- ISO/IEC 29147: Linee guida per la divulgazione delle vulnerabilità;
- Linee guida ENISA per la divulgazione coordinata delle vulnerabilità (2022);
- OpenSSF VEX (Vulnerability Exploitability eXchange).

4. Sicurezza della catena di approvvigionamento

Il CRA riconosce che un prodotto non è mai completamente "indipendente": è composto da decine, talvolta centinaia, di componenti provenienti da fornitori esterni, progetti open source e partner hardware. Per questo motivo il CRA stabilisce requisiti espliciti per la gestione dei rischi di cibersicurezza all'interno della catena di approvvigionamento.

In pratica, i produttori devono:

1. Mantenere una panoramica aggiornata e trasparente dei componenti software utilizzati tramite una SBOM;
2. Richiedere ai fornitori di conformarsi alla sicurezza prevista dal CRA;
3. Monitorare e gestire attivamente i rischi associati alle dipendenze open source ed esterne.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4.1. Software Bill of Materials (SBOM)

Una SBOM è simile a un elenco degli ingredienti per il software: contiene una panoramica di tutti i componenti, le versioni e le origini degli elementi software utilizzati, comprese le librerie open source.

Il CRA richiede ai produttori di mantenere una SBOM e di essere in grado di presentarla alle autorità di regolamentazione e alle autorità competenti su richiesta. La pubblicazione della SBOM per gli utenti è facoltativa[16]. Questa SBOM costituisce la base per:

- Analisi delle vulnerabilità (ad esempio tramite il monitoraggio CVE);
- Valutazione dell'impatto in caso di zero-day;
- Audit della catena di fornitura.

Esempio:

Un produttore di router intelligenti redige una SBOM che indica chiaramente che il prodotto utilizza:

- OpenSSL 1.1.1n;
- BusyBox 1.35.0;
- Una versione modificata di un modulo firewall open source.

Quando viene rivelata una vulnerabilità in OpenSSL (CVE-2022-XXXX), il produttore può verificare immediatamente se il prodotto è interessato e rispondere in modo appropriato.

Le fonti rilevanti a questo proposito includono:

- CycloneDX, SPDX: formati SBOM (raccomandati anche da ENISA e NTIA);
- ISO/IEC 5230 (OpenChain): conformità del software della catena di fornitura;
- Strumenti OpenSSF per la generazione di SBOM e il rilevamento delle vulnerabilità.

4.2. Requisiti di sicurezza per i fornitori

Il CRA richiede inoltre ai produttori di garantire che i loro fornitori e sviluppatori esterni rispettino requisiti di sicurezza paragonabili a quelli del proprio team. La responsabilità non può essere

[16] Se reso disponibile agli utenti, chiarire dove/come gli utenti possono accedervi.

trasferita; anche le vulnerabilità nei componenti di terze parti possono comportare obblighi di conformità al CRA.

In termini concreti, ciò significa:

- Inclusione di clausole di cibersicurezza nei contratti con i fornitori;
- Esecuzione di una due diligence di sicurezza nella selezione dei fornitori di software;
- Verifica periodica della conformità dei partner, ad esempio:
    - ISO/IEC 27001 (sicurezza delle informazioni);
    - IEC 62443-4-1 (sviluppo sicuro dei prodotti);
    - Modelli di maturità OWASP SAMM o BSIMM.
- Diritti di audit contrattuali e livelli minimi di garanzia (ad esempio, certificazione delle dichiarazioni di conformità) per i componenti critici;
- Notifica entro 24 ore delle vulnerabilità critiche individuate dai fornitori che interessano i vostri PED.

Esempio:

Un produttore di dispositivi medici IoT collabora con un fornitore di software in Asia. Il contratto stabilisce che tale fornitore:

- Sviluppi in modo sicuro in conformità con la norma IEC 62443-4-1;
- Documenti tutti i componenti open source utilizzati;
- Mantenga una politica di vulnerabilità con segnalazione obbligatoria entro 24 ore.

4.3. Gestione dei rischi delle librerie open source ed esterne

Il software open source offre molti vantaggi, ma comporta anche dei rischi: vulnerabilità, aggiornamenti mancanti, licenze poco chiare o manutentori inaffidabili. Il CRA richiede ai produttori di gestire e monitorare attivamente questi rischi.

Le migliori pratiche includono:

- Utilizzo di scanner di dipendenze (ad esempio OWASP Dependency-Check, Snyk, Trivy);
- Avvisi automatici per le vulnerabilità (ad esempio tramite GitHub Advisories);
- Utilizzare solo progetti open source manutenuti e maturi;
- Applicare controlli di sicurezza nelle pipeline CI/CD (bloccando le build con CVE noti);

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Utilizzare VEX per ridurre il rumore proveniente da CVE non sfruttabili;
- Richiedere una reattività minima da parte dei manutentori nella selezione dell'OSS.

Esempio:

Un produttore utilizza una libreria JavaScript popolare (ad esempio Log4j) in un'interfaccia web. Dopo aver scoperto Log4Shell (CVE-2021-44228), il produttore sa esattamente quali versioni sono interessate grazie all'analisi SBOM e può segmentare e applicare patch ai prodotti interessati.

Fonti rilevanti a questo proposito includono:

- NIST SSDF (Secure Software Development Framework);
- Linee guida ENISA sulla sicurezza OSS;
- OpenSSF Scorecard: valutazione oggettiva della qualità dei progetti open source.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Conclusione

La presente linea guida rappresenta una prima **traduzione tecnica dei requisiti dell'Allegato I, Parte I del CRA in suggerimenti e raccomandazioni pratiche**. Essa evidenzia **quattro componenti** fondamentali per la conformità al CRA: (1) un approccio alla cibersicurezza basato sul rischio, che comporta una valutazione dei rischi, misure di sicurezza su misura e una considerazione dei modelli di minaccia, delle superfici di attacco e degli impatti; (2) il principio della sicurezza fin dalla progettazione/per impostazione predefinita; (3) i compiti di gestione della sicurezza durante tutto il ciclo di vita del PED; (4) considerazioni e controlli sulla catena di fornitura. Per ciascuna componente vengono forniti **suggerimenti pratici** su come attuare e rispettare tali obblighi sulla base delle migliori pratiche e degli standard riconosciuti. Questi sono tuttavia soggetti a modifiche in attesa delle discussioni sugli standard attuali e di ulteriori sviluppi normativi. Come passi successivi per le PMI, si raccomanda di consultare ulteriori linee guida sul **repository SECURE**, come il **CRA Methodological Compliance Assessment Framework** per un toolkit passo dopo passo e una checklist sulla conformità al CRA, oltre all'Allegato I, nonché **CRA 101: Understanding CRA Obligations** per una panoramica sintetica e di facile comprensione degli obblighi legali previsti dal CRA.