SECURE
Cyber Resilience for SMEs

Cerințele esențiale de securitate cibernetică prevăzute de CRA: Anexa I, Partea I

20/10/2025

Funded by the European Union

Declarație privind finanțarea UE: Finanțat de Uniunea Europeană în cadrul GA nr. 101190325. Opiniile și punctele de vedere exprimate aparțin însă exclusiv autorului (autorilor) și nu reflectă neapărat punctul de vedere al Uniunii Europene sau al Centrului european de competență în domeniul securității cibernetice, al tehnologiei și al cercetării. Nici Uniunea Europeană, nici autoritatea care acordă finanțarea nu pot fi considerate responsabile pentru acestea.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Declarație de exonerare de răspundere a ECCC: Proiectul este susținut de Centrul european de competență în domeniul securității cibernetice și de membrii săi

DECLARAȚIE DE RESPONSABILITATE

Acest document face partedin livrabilul D4.1 „Ghiduri și materiale pentru conformitatea IMM-urilor la CRA" al proiectului SECURE.

Acest document este o versiune tradusă a ghidului original redactat în limba engleză. Acronimele sunt păstrate în limba engleză, așa cum se poate vedea în lista de acronime.

Primul autor: *Centrul pentru Securitate Cibernetică din Belgia (CCB)*

Al doilea autor: *Autoritatea pentru Digitalizarea României-NCC-RO (ADR-NCC-RO)*

Cuprins

Lista tabelelor și figurilor

Abrevieri

API – Interfață de programare a aplicațiilor

APT – Amenințări persistente avansate

BSIMM – Model de maturitate pentru securitatea clădirilor

CI/CD – Integrare continuă și livrare/implementare continuă

CRA – Legea privind reziliența cibernetică

CVD – Dezvăluirea coordonată a vulnerabilităților

CVE – Vulnerabilități și expuneri comune

CVSS – Sistem comun de evaluare a vulnerabilităților

DAST – Testare dinamică a securității aplicațiilor

DoS – Refuzul serviciului

DREAD – Daune, reproductibilitate, exploatabilitate, utilizatori afectați și detectabilitate

ENISA – Agenția Uniunii Europene pentru Securitate Cibernetică

EOL – Sfârșitul ciclului de viață

EPSS – Sistem de evaluare a predicției exploatării

ETSI – Institutul European de Standardizare Tehnică

UE – Uniunea Europeană

FIRST VCMM – Modelul de maturitate al coordonării vulnerabilităților FIRST

GDPR – Regulamentul general privind protecția datelor

HTTPS/TLS – Protocolul hipertext securizat/Securitatea stratului de transport

ICS – Sistem de control industrial

IEC – Comisia Electrotehnică Internațională

IoT – Internetul obiectelor

IPSec – Securitate protocol internet

ISO – Organizația Internațională de Standardizare

JTAG – Grupul de acțiune comună pentru testare

LINDDUN – Legare, identificare, nerepudiere, detectare, divulgare de date, necunoaștere și neconformitate

MFA – Autentificare multifactorială

MITRE ATT&CK – Tactici, tehnici și cunoștințe comune ale adversarilor

MQTT – Transport telemetric de cozi de mesaje

NIST – Institutul Național de Standarde și Tehnologie (Statele Unite)

NIST SSDF – Cadrul NIST pentru dezvoltarea de software securizat

NTIA – Administrația Națională pentru Telecomunicații și Informații (Statele Unite)

OPENSSF VEX – Fundația pentru securitate open-source Vulnerability Exploitability eXchange

OS – Sistem de operare

OTA – Over The Air

OWASP – Proiectul mondial deschis pentru securitatea aplicațiilor

OWASP ASVS – Standardul OWASP de verificare a securității aplicațiilor

OWASP SAMM – Modelul de maturitate al asigurării software-ului OWASP

PDE – Produs cu elemente digitale

PSIRT – Echipa de răspuns la incidente de securitate a produselor

SAST – Testare statică a securității aplicațiilor

SBOM – Lista componentelor software

SCA – Analiza compoziției software

SIEM – Gestionarea informațiilor și evenimentelor de securitate

SME – Întreprinderi mici și mijlocii

SOC – Centru de operațiuni de securitate

SQL – Limbaj de interogare structurat

SSDLC – Ciclul de viață al dezvoltării software-ului securizat

SSL – Secure Sockets Layer

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

TPM – Modul de platformă de încredere

UART – Receptor-transmițător asincron universal

USB – Bus serial universal

VPN – Rețea privată virtuală

Introducere

Pentru a respecta Actul privind reziliența cibernetică (Cyber Resilience Act – CRA), Regulamentul (UE) 2024/2847, în calitate de producător, CRA prevede o multitudine de cerințe și obligații. Printre acestea, una esențială este obligația de a vă asigura că produsul cu elemente digitale (PDE) pe care îl introduceți pe piață „a fost proiectat, dezvoltat și produs în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în Partea I a Anexei I”[1]. Anexa I conține două părți: Partea I se concentrează pe cerințele de securitate cibernetică referitoare la proprietățile produsului, iar Partea a II-a vizează cerințele privind gestionarea vulnerabilităților. Partea I constă, la rândul său, din două puncte, dintre care primul prevede că:

> *„Produsele cu elemente digitale trebuie proiectate, dezvoltate și fabricate astfel încât să asigure un nivel adecvat de securitate cibernetică în funcție de riscuri”*[2].

Punctul 2 specifică cerințele pe care produsele dvs. trebuie să le respecte.

Prezentul ghid, elaborat în cadrul proiectului SECURE[3] cu scopul de **a sprijini întreprinderile mici și mijlocii (IMM-uri)**, aprofundează ambele puncte din Anexa I, Partea I, oferind **sugestii practice și tehnice, exemple și abordări cu caracter neexhaustiv, pentru a sprijini conformarea cu fiecare cerință**. Este important de menționat că orice referire la standarde, instrumente și cadre existente are un caracter exclusiv orientativ, cu intenția de a face cerințele CRA cât mai concrete și ușor de aplicat. Recomandările formulate se bazează pe cele mai bune practici recunoscute și pe abordări uzuale. Atât instrumentele menționate în cadrul ghidului, cât și ghidul în sine vor fi actualizate pe măsură ce elaborarea standardelor specifice CRA și a măsurilor de punere în aplicare ale Comisiei Europene va avansa pe parcursul perioadei de adaptare 2024–2027.

[1] Art. 13(1), CRA.

[2] Anexa I, partea I alineatul (1), CRA.

[3] Proiectul „Consolidarea rezilienței cibernetice a IMM-urilor din UE” (SECURE) oferă sprijin financiar și îndrumare IMM-urilor pentru a se conforma CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cerințele esențiale de securitate cibernetică ale CRA: Anexa I, Partea I

1. Abordarea securității cibernetice bazată pe riscuri

Punctul 1 din anexa I, partea I prevede că:

> *„Produsele cu elemente digitale trebuie proiectate, dezvoltate și fabricate astfel*
>
> *încât să asigure un **nivel adecvat de securitate cibernetică în funcție de** riscuri"*[4] .

Acest punct este esențial pentru CRA și se bazează pe principiul „security by design and by default" („securitate prin proiectare și implicit").

În esență, aceasta înseamnă că trebuie să dezvoltați pentru produsul dvs. o **abordare a securității cibernetice bazată pe riscuri** Această adaptare bazată pe riscuri trebuie să fie justificabilă, documentată și proporțională. Gândiți-vă la conformitatea CRA ca la un „parcurs trasabil":

contextul produsului → risc → controale → dovezi

Raționamentul acestui parcurs trebuie documentat cu atenție în documentația tehnică obligatorie[5], fiind esențial pentru conformitate și pentru posibilitatea de auditare.

În practică, producătorii trebuie:

1. Să evalueze riscurile de securitate cibernetică asociate cu produsele cu elemente digitale (PDE) pe tot parcursul ciclului lor de viață;
2. Să adapteze măsurile de securitate la nivelul de risc (de exemplu, un termostat inteligent vs. un sistem industrial de control);
3. Să ia în considerare modelele de amenințare, suprafețele de atac și impactul potențial asupra utilizatorilor și sistemelor.

Un prim pas crucial în conformitatea cu CRA este, așadar, efectuarea unei **evaluări a riscurilor** pentru PDE. Acest capitol explică modul modul în care poate fi efectuată o astfel de evaluare a riscurilor, prezentând posibile abordări și oferind sugestii tehnice.

Înainte de a intra în detalii, mai jos este oferită o prezentare generală de două pagini de tip „Risk Assessment 101". Elementele reapar într-o formă mai detaliată în primul capitol al acestui ghid, pe care vă recomandăm să îl consultați. Cu toate acestea, din motive de accesibilitate, acest rezumat simplificat prezintă modul în care sunt abordate în general evaluările riscurilor[6] .

[4] Anexa I, partea I(1), CRA.

[5] Art. 31, CRA.

[6] Este esențial să se rețină că orientările oficiale privind modul de efectuare a evaluării riscurilor pentru CRA trebuie încă elaborate de Comisia Europeană. Orientările furnizate aici rezumă etapele principale ale oricărei abordări de evaluare a riscurilor. Se poate utiliza orice altă abordare, standard sau metodologie, atâta timp cât aceasta este în conformitate cu abordarea raportată.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Evaluarea riscurilor 101

Atunci când se efectuează o evaluare a riscurilor, pot fi luate în considerare **șase etape**:

1) Identificarea **activelor** și a **amenințărilor** = *identificarea fiecărui activ (ceea ce trebuie protejat) în funcție de expunerea sa la o amenințare (ceea ce ar putea merge prost);*
2) Evaluarea **vulnerabilităților** = *evaluați vulnerabilitățile*;
3) Analiza și evaluarea **impactului** și a **probabilității** = *planificați impactul și probabilitatea vulnerabilităților acest* proces conduce la identificarea unor *„riscuri" specifice*;
4) **Analiza** și **acceptarea** riscurilor = *planificați fiecare risc și luați în considerare nivelul dvs. de acceptare pentru a prioritiza acțiunile* necesare;

În plus față de această evaluare a riscurilor, ultimele două etape includ:

5) Implementarea **măsurilor** de **reducere a riscurilor** = *selectați și aplicați controale de securitate pentru fiecare risc;*
6) Monitorizarea și reevaluarea = *monitorizarea amenințărilor și riscurilor pe parcursul fiecărei etape a ciclului de viață al PDE și actualizarea evaluării riscurilor.*

Pentru **etapele unu până la trei**, puteți dezvolta o **matrice** care vă permite să clasificați fiecare amenințare, vulnerabilitate și impact în funcție de un anumit nivel de risc și scor. Pentru a face acest lucru, trebuie mai întâi să definiți ce înseamnă fiecare nivel (și scor) pentru dvs. Prin intermediul unor tabele descriptive[7] .

- Scăzut
- Scăzut-mediu
- Mediu
- Mediu-ridicat
- Ridicat

Tabelul 1 :
Exemplu de matrice

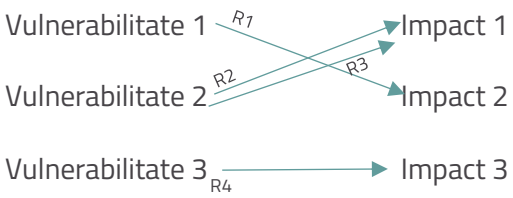
Risc/Amenințare	Amenințare 1	Amenințare 2	Scor
Ridicat			10
Mediu-ridicat			
Mediu			
Scăzut Mediu			
Scăzut			0

[7] De exemplu, în ceea ce privește apariția amenințărilor, un nivel „scăzut" ar putea însemna o amenințare care poate apărea o dată la 10 ani, în timp ce „ridicat" ar putea însemna o amenințare care poate apărea o dată pe săptămână. Aveți nevoie de tabele descriptive separate pentru amenințări, vulnerabilități și impacturi, precum și pentru riscuri – acestea din urmă susțin definirea nivelului dvs. de acceptare.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

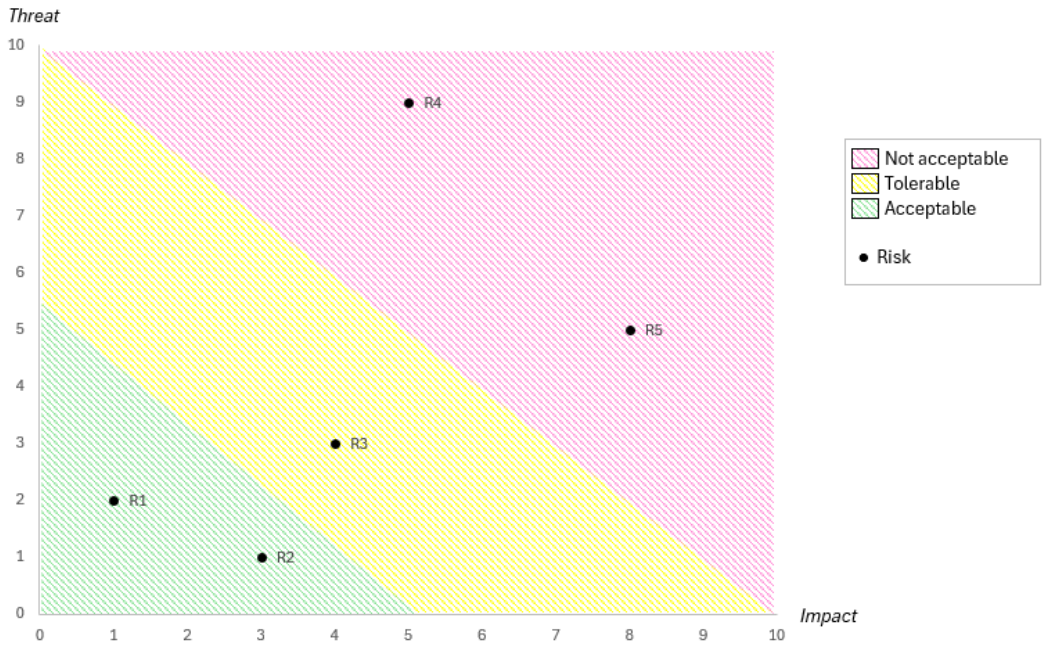
Corelarea vulnerabilităților cu impacturile vă permite ulterior să vizualizați diferitele riscuri (R):

Figura 1 :
Vizualizarea riscurilor



Pentru **etapa a patru**, este important să se identifice riscurile întâlnite și să se definească nivelul de acceptare a acestor riscuri - acest lucru se realizează adesea prin codificare color, de exemplu:

Figura 2 :
Graficul de acceptare a riscurilor



Acest lucru vă permite să stabiliți prioritățile în ceea ce privește măsurile care trebuie luate și să elaborați măsuri de atenuare și controale de securitate pentru fiecare risc, astfel încât riscurile reziduale să fie reduse la un nivel acceptabil.

După cum s-a menționat anterior, aceste elemente ale evaluării riscurilor sunt tratate mai detaliat în continuare (capitolul 1 din prezentul ghid), oferind exemple și instrumente și cadre recomandate pentru a vă sprijini.

1.1. Evaluarea riscurilor de securitate cibernetică pe parcursul ciclului de viață

Deoarece riscurile de securitate cibernetică asociate cu PDE-ul dvs. trebuie evaluate pe tot parcursul ciclului de viață al produsului, efectuarea unei **evaluări a riscurilor de securitate cibernetică pe**

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

durata ciclului de viață implică **identificarea, analizarea și atenuarea riscurilor de securitate cibernetică** în fiecare etapă a ciclului de viață al unui produs:

1. Proiectare
2. Dezvoltare
3. Producție
4. Implementare
5. Operare și mentenanță
6. Sfârșitul ciclului de viață (EOL)

Evaluarea riscurilor trebuie actualizată continuu pe parcursul „perioadei de asistență”[8] , adică o perioadă de cel puțin cinci ani (sau, dacă durata de viață a produsului este mai scurtă de cinci ani, cel puțin până la sfârșitul duratei de viață a produsului).

1.1.1. Etape cheie în evaluarea riscurilor pe durata ciclului de viață

La efectuarea evaluării riscurilor, pot fi luate în considerare șase etape, fiecare dintre acestea fiind clarificată în Tabelul 2 de mai jos.

Tabelul 2 :
Etape cheie în evaluarea riscurilor pe durata ciclului de viață

Etapă cheie	Clarificări și sugestii
1. Identificarea activelor și a amenințărilor	Distingeți între: • Active: ce trebuie protejat? de exemplu, firmware, date utilizatorilor, canale de comunicare. • Amenințări: ce ar putea merge prost? De exemplu, injectarea de malware, accesul neautorizat.
2. Analizați vulnerabilitățile	Utilizați instrumente precum: • Analiza statică a codului; • Analiza compoziției software (SCA);

[8] Art. 13 alineatul (8) din CRA: Perioada de asistență trebuie stabilită de producător, ținând seama de perioada în care se preconizează că produsul va fi utilizat, de așteptările utilizatorilor, de natura (scopul) produsului și de legislația Uniunii.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

	• Testarea de penetrare; • Modelarea amenințărilor ([9] , de exemplu STRIDE, DREAD). Notă: CVSS și STRIDE pot fi utilizate împreună într-un proces de modelare a amenințărilor. STRIDE poate ajuta la identificarea potențialelor amenințări, iar CVSS poate fi apoi utilizat pentru a evalua severitatea vulnerabilităților asociate acestor amenințări, permițând o mai bună prioritizare a eforturilor de atenuare[10] .
3. Evaluați impactul și probabilitatea riscului	Utilizați o matrice de risc pentru a stabili prioritățile pe baza: • Impact (de exemplu, încălcarea securității datelor, defecțiuni ale sistemului); • Probabilitate (de exemplu, exploatare cunoscută, suprafață de atac).
4. Analizați riscurile și acceptabilitatea acestora	Definiți nivelul de acceptabilitate și planificați riscurile în funcție de amenințare și impact pentru a clasifica și prioritiza acțiunile.
5. Implementați măsuri de atenuare	Aplicați controale de securitate: de exemplu, criptare, autentificare, pornire securizată.
6. Monitorizați și reevaluați	Monitorizați continuu apariția de noi amenințări și actualizați evaluările de risc în consecință.

1.1.2. Cazuri de utilizare în funcție de etapa ciclului de viață

Pentru a face evaluarea riscurilor pe durata ciclului de viață mai concretă, Tabelul 3 de mai jos oferă o imagine de ansamblu asupra unor cazuri de utilizare, incluzând, pentru fiecare etapă a ciclului de viață, un exemplu de risc și o strategie de atenuare.

[9] Modelarea amenințărilor este discutată mai detaliat la punctul 1.3.1

[10] CVSS evaluează gravitatea vulnerabilității, în timp ce riscul ia în considerare și impactul asupra activității și probabilitatea.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabelul 3 :
Cazuri de utilizare în funcție de etapa ciclului de viață

Etapa ciclului de viață	Caz de utilizare	Risc	Atenuare
Proiectare	Cameră inteligentă pentru casă	Acces neautorizat la fluxul video	Implementarea criptării end-to-end și a setărilor implicite sigure
Dezvoltare	Firmware dispozitiv	Vulnerabilitate de depășire a memoriei tampon	Utilizați practici de programare sigură și scanare automată a vulnerabilităților
Producție	Gateway IoT industrial	Compromis în timpul fabricării	Asigurați securitatea lanțului de aprovizionare și a hardware-ului, sigilii inviolabile de tip „ ” și aprovizionare sigură
Implementare	Router pentru consumatori	Datele de autentificare implicite rămân neschimbate	Forțarea schimbării parolei la prima utilizare
Operare și mentenanță	Vehicul conectat	Vulnerabilități software necorectate	Actualizări OTA (Over-The-Air) cu verificări de integritate
Sfârșitul ciclului de viață	Termostat inteligent	Dispozitiv abandonat cu firmware exploatabil	Furnizați instrucțiuni pentru scoaterea din uz în condiții de securitate și pentru ștergerea datelor, precum și o politică privind actualizările de securitate la sfârșitul ciclului de viață (EOL) și exportul datelor pentru utilizatori.

1.1.3. Instrumente și cadre de referință care vă pot sprijini

Lista de mai jos evidențiază câteva instrumente și cadre de referință care pot oferi sprijin, deși o listă mai exhaustivă și standarde armonizate sunt încă în curs de elaborare.

- ISO/IEC 27005 – Gestionarea riscurilor
- NIST SP 800-30 – Metodologie de evaluare a riscurilor
- ENISA Threat Landscape – Informații actualizate privind amenințările
- OWASP ASVS – Verificarea securității aplicațiilor
- Modelul STRIDE
- Modelul de evaluare a riscurilor DREAD
- LINDDUN
- CVSS

1.2. Măsuri de securitate adaptate

A doua dimensiune a unei abordări a securității cibernetice bazate pe riscuri constă în adaptarea măsurilor de securitate la nivelul de risc. Adaptarea trebuie să fie proporțională cu riscurile identificate în Anexa I, Partea I(1). Să analizăm ce înseamnă acest lucru cu ajutorul a șase etape clare, principii și două exemple de produse: un termostat inteligent (risc scăzut până la moderat) și un sistem de control industrial (ICS) (risc ridicat).

1.2.1. Efectuați clasificarea riscurilor produsului

Atunci când se efectuează o evaluare a riscurilor specifice produsului, este important să se ia în considerare următoarele dimensiuni.

- **Expunerea la amenințări**: Produsul este
  - Conectat la internet?
  - Utilizat pe scară largă?
  - Destinat publicului larg?
  - Destinat unei utilizări prevăzute vs. unei utilizări greșite rezonabil previzibile?
- **Impactul compromiterii**: Care ar fi impactul asupra siguranței, pierderilor financiare, confidențialității, infrastructurii critice?
- **Atractivitatea atacului:** Ar putea reprezenta un punct de plecare pentru mișcări laterale?
- **Profilul utilizatorului:** consumator, IMM, operator de infrastructură critică?

Pe baza acestor considerente, produsul poate fi clasificat ca având risc scăzut - acceptabil, risc moderat - tolerabil sau risc ridicat - inacceptabil[11] .

1.2.2. Definirea obiectivelor de securitate în funcție de nivelul de risc

Tabelul 4 ilustrează modul în care obiectivele de securitate pot fi adaptate la nivelul de risc al produsului stabilit anterior.

Tabelul 4 :
Obiective de securitate în funcție de nivelul de risc

Nivel de risc	Obiective de securitate
Scăzut (de exemplu, termostat inteligent)	• Prevenirea exploatării banale; • Asigurarea confidențialității; • Menținerea capacității de actualizare.
Moderat	• Detectarea și atenuarea vectorilor de atac cunoscuți; • Impunerea autentificării • Asigurarea unei comunicații securizate. •
Ridicat (de exemplu, ICS)	• Consolidarea posturii de securitate • Apărarea în profunzime; • Încrederea în lanțul de aprovizionare; • Pornirea securizată; • Monitorizarea incidentelor.

1.2.3. Corelarea cerințelor esențiale CRA cu nivelul de risc

În funcție de nivelul de risc, cerințele esențiale CRA pot avea aplicări practice diferite. Tabelul 5 ilustrează acest lucru pentru nivelurile de risc scăzut și ridicat precum și pentru exemplele de produse corespunzătoare, respectiv termostatul inteligent și sistemul industrial de control (ICS).

[11] Acest lucru necesită definirea în prealabil a modului de evaluare a acestor elemente utilizând o matrice și a modului în care scorurile corespund nivelurilor de risc. Pentru o clasificare mai precisă, pot fi luate în considerare cinci niveluri de risc, în loc de trei: risc scăzut, mediu-scăzut, mediu, mediu-ridicat, ridicat.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabelul 5 :
Cerințe esențiale CRA în funcție de nivelul de risc

Cerință CRA	Risc scăzut	Risc ridicat
Securitate prin proiectare și în mod implicit (Secure-by-Design and Default)	Dezactivarea porturilor de depanare; setări implicite robuste	Lista completă a componentelor software (SBOM[12]); pornire securizată; sistem de operare consolidat
Gestionarea vulnerabilităților	Politică publică privind divulgarea coordonată a vulnerabilităților (CVD); Fișier security.txt; monitorizarea canalelor de raportare a vulnerabilităților; mecanism pentru distribuirea și aplicarea actualizărilor de securitate.	divulgare coordonată a vulnerabilităților; PSIRT; răspuns rapid la incidente și vulnerabilități.
Jurnalizare și monitorizare	Jurnale de evenimente locale	Jurnalizare la distanță; integrare SIEM
Controlul accesului	Autentificare prin PIN sau aplicație	Acces bazat pe roluri; MFA; privilegii minime
Mecanism de actualizare	Actualizări OTA cu consimțământul utilizatorului	Actualizări semnate; revenire la starea anterioară în caz de eșec
Protecție împotriva accesului neautorizat	Reguli de bază pentru firewall	Sisteme de detectare a intruziunilor la nivel de gazdă; verificarea integrității firmware-ului

[12] SBOM este clarificat în secțiunea 4.1.

1.2.4. Utilizarea modelării amenințărilor pentru rafinarea măsurilor de securitate

În cadrul modelării amenințărilor, pot fi utilizate metode precum STRIDE, LINDDUN sau arborii de atac pentru a verifica dacă măsurile de control sunt adecvate.

Pentru exemplele de produse menționate, aceasta înseamnă:

- **Termostat inteligent**: accent pe amenințări de tip spoofing (falsificarea identității), tampering (modificarea neautorizată) și denial of service (denegarea serviciului);
- **ICS**: acoperirea tuturor amenințărilor din modelul STRIDE, precum și a amenințărilor persistente avansate (APT).

1.2.5. Selectarea controalelor în funcție de nivelul de risc

Tabelul 6 propune diferite controale grupate pe domenii de securitate pentru cazurile practice analizate, termostatul inteligent (risc scăzut) și sistemul de control industrial - ICS (risc ridicat).

Tabelul 6 :
Controale în funcție de nivelul de risc

Domeniul de securitate	Risc scăzut	Risc ridicat
Autentificare	Autentificare prin aplicație; obligativitatea schimbării parolei implicite	autentificare multifactor (MFA); controlul al accesului bazat pe certificate digitale
Securitatea firmware-ului	Firmware semnat digital; actualizări OTA; mecanisme sigure de revenire la starea inițială în caz de eroare	Pornire securizată; integrare cu TPM; măsuri de asigurare a încrederii în lanțul de aprovizionare
Comunicare	HTTPS/TLS	VPN-uri; IPSec; segmentarea rețelei; arhitectură de tip zero trust
Monitorizare	Rotație de bază a logurilor	Jurnalizare în timp real; detectarea anomaliilor; integrare SOC; Loguri sincronizate temporal

Interfață	Interfață simplă de configurare	Consolă de administrare cu control detaliat; funcționalități de audit și trasabilitate

1.2.6. Documentarea dovezilor de conformitate

Așa cum s-a menționat anterior, un element cheie pentru conformitatea cu CRA îl reprezintă documentarea următoarelor dovezi, cel puțin:

- Justificarea clasificării nivelului de risc
- Deciziile privind controalele de securitate, corelate cu riscurile identificate;
- Rezultatele testării și validării;
- Politici privind actualizările și gestionarea vulnerabilităților;
- Alinierea la un ciclu de dezvoltare securizată a produsului (de exemplu, ISO/IEC 27034, IEC 62443-4-1);
- Matrice de trasabilitate care corelează riscurile → controale → teste de verificare → dovezi (de păstrat în documentația tehnică)

1.2.7. Exemple

Tabelul 7 oferă exemple suplimentare de măsuri de implementare pentru cazurile practice corespunzătoare nivelurilor de risc scăzut și ridicat.

Tabelul 7 :
Măsuri de implementare în funcție de nivelul de risc

Produs	**Termostat inteligent**	**ICS**
Considerații privind riscurile	• Conectat la internet, controlează sistemul de încălzire în locuințe private; • Implică aspecte sensibile legate de viața privată, dar are un impact redus asupra	• Utilizat în infrastructuri critice (de exemplu, în tratarea apei); • Impact ridicat asupra siguranței și funcționării.

	siguranței sau asupra pierderilor economice.	
Clasificarea riscurilor	Risc scăzut	Risc ridicat
Măsuri de implementare	• Schimbarea parolei implicite la prima utilizare; • Comunicare securizată prin HTTPS cu infrastructură backend; • Actualizări de firmware semnate digital; • Doar înregistrare locală[13] ; • Formular de contact pentru raportarea vulnerabilităților de bază.	• Hardware securizat prin design (Secure by design) cu integrare TPM; • Pornire securizată și actualizări semnate digital cu mecanism de revenire la o versiune anterioară; • Acces bazat pe roluri și autentificare multifactor (MFA); • Segmentarea rețelei și reguli de firewall; • Conectare la SIEM central; • SBOM complet la fiecare actualizare; • Proces coordonat de divulgare a vulnerabilităților (CVD);

1.3. Luarea în considerare a modelelor de amenințări, a suprafețelor de atac și a impactului potențial asupra utilizatorilor și sistemelor

CRA pune accentul pe o abordare a securității cibernetice bazată pe riscuri. Așa cum s-a arătat mai sus, aceasta înseamnă că producătorii trebuie să-și adapteze măsurile de securitate la amenințările reale, la punctele de expunere și la consecințele potențiale pentru utilizatori și sisteme. Nu este

[13] De reținut: jurnalele locale reduc valoarea criminalistică, se recomandă exportul opțional cu consimțământul utilizatorului.

vorba despre o cerință formală lipsită de substanță, ci despre necesitatea unei abordări fundamentate și adaptate contextului. Pentru a pune în aplicare în mod eficient această obligație, trebuie luate în considerare împreună trei concepte cheie: modelele de amenințări, suprafețele de atac și analiza impactului, care constituie a treia și ultima dimensiune a abordării securității cibernetice bazate pe risc. Să analizăm pe rând aceste elemente și să vedem cum se corelează între ele.

1.3.1. Modele de amenințări: cine atacă, de ce și cum?

Modelarea amenințărilor este un proces structurat prin care identificați cine ar putea ataca produsul dvs., cum ar putea face acest lucru și care este motivația. Vă puteți gândiți, de exemplu, la script kiddies, grupări de criminalitate informatică organizată sau chiar la actorii statali. Motivele lor pot varia de la câștiguri financiare la sabotaj sau spionaj, iar abilitățile lor variază de la cele de bază la cele avansate.

Pentru a structura acest proces, se pot utiliza metode precum:

- STRIDE;
- MITRE ATT&CK pentru tehnici de atac cunoscute;
- LINDDUN pentru amenințări orientate spre protecția vieții private;
- Arbori de atac sau lanțuri de compromitere cibernetică (*cyber kill chains*), pentru cartografierea căilor de atac.

Revenind la exemplele practice menționate, aceasta înseamnă:

- **Termostat inteligent**: amenințările sunt adesea limitate la vecini curioși sau atacuri aleatorii, în care cineva ar putea manipula setările de temperatură sau consumul de energie;
- **ICS** (de exemplu, într-o stație de tratare a apei): amenințările sunt fundamental diferite - de exemplu, grupurile APT sau rețele de ransomware pot încerca să saboteze procesele fizice sau să oprească activitatea unei organizații.

Rezultatul modelării amenințărilor este o listă clară de obiective de securitate specifice produsului și mediului în care acesta funcționează.

1.3.2 Suprafețe de atac: Pe unde poate pătrunde un atacator?

O suprafață de atac reprezintă totalitatea tuturor punctelor prin care un atacator poate interacționa cu sistemul sau îl poate influența. Cu cât există mai multe interfețe și puncte de acces, cu atât riscul este mai mare.

Suprafețele de atac tipice sunt:

- Interfețe de rețea, cum ar fi Wi-Fi, Bluetooth, MQTT sau HTTP;
- Interfețe locale, cum ar fi USB, UART, JTAG (pentru depanare);
- Mecanisme de actualizare, cum ar fi actualizările OTA sau USB;
- API-uri, aplicații mobile, interfețele cloud de administrare
- Componente externe provenite din lanțul de aprovizionare.

Analiza acestor suprafețe implică verificarea componentelor care sunt expuse inutil, a serviciilor care sunt activate fără a fi necesare, și a protecției adecvate a accesului. În mod ideal, suprafața de atac ar trebui limitată prin:

- aplicarea unor principii de securitate precum expunerea minimă, configurările implicite sigure și măsurile de întărire a securității
- Dezactivarea porturilor sau serviciilor neutilizate;
- Autentificare și criptare la nivelul fiecărei interfață.

Aplicat la exemple menționate, acest lucru înseamnă:

- **Termostat inteligent**: va utiliza de obicei Wi-Fi și, eventual, Bluetooth, cu o conexiune simplă la cloud. Interfețele de depanare pot rămâne active în etapa de testare, dar trebuie dezactivate în mediul de producție;
- **Gateway ICS**: va fi protejat fizic, cu actualizări USB securizate, rețele segmentate și fără interfețe externe expuse.

Prin urmare, cartografierea atentă a suprafeței de atac este esențială pentru a înțelege unde sunt cu adevărat necesare măsurile de securitate.

1.3.3 Analiza impactului: Ce se întâmplă dacă lucrurile merg prost?

Ultimul pas constă în determinarea impactului potențial al unui atac reușit. CRA impune ca măsurile de securitate să fie proporționale cu acest impact. Acesta nu se limitează la prejudiciile tehnice, ci include și:

- Riscuri pentru utilizator (de exemplu, vătămări cauzate de controlul temperaturii);
- Încălcarea vieții private (de exemplu, deducerea obiceiurilor de viață pe baza datelor colectate de termostat
- Pierderea disponibilității sau a continuității activității (de exemplu, închiderea fabricii);

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Răspunderea legală (de exemplu, încălcarea CRA sau GDPR);
- Prejudiciul reputațional și riscuri de piață.

Impactul trebuie luat în considerare din mai multe perspective:

- La nivelul utilizatorului: de la un disconfort minor la situații care pun viața în pericol;
- La nivel organizațional: de la creșterea volumului de muncă al serviciului de asistență până la întreruperea activității;
- La nivel societal: de la erori aparent inofensive până la amenințări la adresa infrastructurii critice.

Și în acest caz, proporționalitatea este esențială – un robot de jucărie nu necesită același nivel de securitate ca o pompă medicală.

1.3.4 Integrare: de la analiză la măsuri

Atunci când aceste trei elemente de bază sunt corelate - modelul de amenințare, suprafața de atac și impactul - se creează o bază solidă pentru adaptarea măsurilor de securitate.

O abordare tipică arată astfel:

1. Definirea utilizării și a contextului produsului;
2. Realizarea modelării amenințărilor pentru a înțelege actorii implicați, motivațiile și căile de atac;
3. Cartografierea suprafeței de atac și identificarea vulnerabilităților;
4. Analiza impactului asupra utilizatorilor, organizațiilor și societății;
5. Selectarea măsurilor în funcție de risc (risc = probabilitate × impact);
6. Documentarea tuturor elementelor în vederea conformității cu CRA și a auditului.

Pentru exemplele practice analizate, aceasta înseamnă:

- **Termostat inteligent**: măsuri precum criptare, o politică solidă privind parolele, actualizări OTA semnate digital și o declarație simplă privind confidențialitatea;
- **Gateway ICS**: măsuri precum pornire securizată, rădăcină hardware de încredere (*hardware root of trust*), rețele segmentate, înregistrare SIEM, gestionarea rolurilor și un SBOM complet însoțit de monitorizarea vulnerabilităților.

2. Proiectare și dezvoltare securizate

Revenind la punctul 1 din Anexa I, Partea I a CRA, abordarea securității cibernetice bazată pe risc și adaptarea măsurilor la nivelul de risc se întemeiază pe principiul „security by design and by default", adică produsele cu elemente digitale trebuie să fie proiectate și dezvoltate astfel încât să fie sigure de la bun început. Nu mai este suficient securitatea să fie adăugată ulterior ca un strat opțional; aceasta trebuie să constituie o componentă esențială a întregului proces de dezvoltare a produsului. „Securitatea prin proiectare", „securitatea prin configurare implicită" și utilizarea unor practici de dezvoltare securizată constituie nucleul unei strategii solide privind produsele digitale reziliente. Acestea asigură faptul că securitatea nu este tratată ca un element secundar, ci ca o componentă integrată structural și demonstrabilă a produsului - exact ceea ce prevede CRA.

Prin utilizarea unor standarde internaționale precum IEC 62443, ISO 27034, OWASP și ghidurile ENISA, producătorii pot aplica în mod eficient aceste principii, respectând în același timp obligațiile de conformitate care le revin.

Produsele trebuie să fie:

1. **Securizate prin proiectare (Secure by design)**: securitatea este integrată încă din primele etape de dezvoltare;
2. **Securizate prin configurare implicită (Secure by default)**: setările implicite trebuie să acorde prioritate securității (de exemplu, parole puternice, porturi deschise minime etc.)
3. **Dezvoltate în condiții de siguranță**: prin utilizarea unor practici de programare sigură și a modelării amenințărilor.

2.1. Securitate prin proiectare (Secure by design) - Securitate încă din faza inițială de proiectare

„Securitate prin proiectare" înseamnă că securitatea cibernetică este luată în considerare încă din faza de concept în deciziile privind arhitectura, selecția componentelor și interacțiunea dintre subsisteme. Securitatea trebuie să fie la fel de fundamentală ca funcționalitatea sau ușurința în utilizare.

Exemplu practic:

La proiectarea unui modul de încuietoare inteligentă pentru ușă, se iau de la bun început următoarele decizii:

- Aplicarea criptării end-to-end între aplicație și încuietoare;
- Stocarea securizată a cheilor în siguranță într-un TPM sau Secure Element;
- Dezactivarea fizică a porturilor de depanare după etapa producție.

Standardele și ghidurile relevante în acest sens includ:

- IEC 62443-4-1: Prevede integrarea securității în ciclul de viață al software-ului;
- ISO/IEC 27034: Securitatea aplicațiilor în ciclul de viață al dezvoltării software-ului;
- NIST SP 800-218 SSDF;
- Ghidul ENISA privind bunele practici pentru dezvoltarea securizată a software-ului

2.2. Securitate implicită – Securitate fără configurare din partea utilizatorului

Securitate implicită (Secure by default) înseamnă că produsele sunt livrate în mod standard, cu cea mai sigură configurație. Utilizatorul nu ar trebui să fie nevoit să ghicească dacă măsurile de securitate sunt activate. Securitatea trebuie să constituie nivelul de bază, nu o opțiune suplimentară de tip „setare avansată".

Exemple de setări implicite sigure:

- Fără setări implicite comune; configurarea credențialelor la prima pornire trebuie impusă sau trebuie utilizată asocierea fără parolă, bazată pe factori de securitate adecvați.
- Doar porturile de rețea strict necesare rămân deschise (principiul expunerii minime);
- Actualizările de firmware semnate și verificate în mod implicit;
- Jurnalizarea și păstrarea unei de audit sunt activate în mod implicit pentru funcțiile critice.

Ghidurile relevante în acest sens includ:

- OWASP Secure Configuration: Cele mai bune practici pentru configurări implicite sigure;
- NIST SP 800-128: Ghid pentru gestionarea configurării axată pe securitate.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2.3. Practici de programare securizată (Secure Coding Practices)

CRA impune ca dezvoltarea de software să se realizeze în conformitate cu practici de dezvoltare securizată și dovedite, acordând o atenție continuă amenințărilor. Aceasta înseamnă, printre altele:

Programare securizată:

- Validarea datelor introduse (împotriva atacurilor de tip SQL injection, depășirilor de memorie tampon - buffer overflow etc.);
- Utilizarea de biblioteci sigure și criptare;
- Testarea de tip fuzzing și analiza statică a codului.

Modelarea amenințărilor:
Pentru fiecare componentă software, trebuie evaluate următoarele aspecte:

- Cine ar putea ataca această componentă?
- Cum ar putea face acest lucru?
- Care ar fi impactul?

Cadrele precum STRIDE (Microsoft), OWASP Threat Dragon și MITRE ATT&CK pot ajuta la identificarea sistematică a vulnerabilităților și a căilor de atac.

Standardele și ghidurile relevante în acest sens includ:

- Lista de verificare a practicilor de programare securizată OWASP (OWASP Secure Coding Practices Checklist)
- ISO/IEC 27001 Anexa A.14: Cerințe de securitate în procesul dezvoltare;
- ENISA Threat Modelling Guidelines (2022);
- BSI TR-03161 (Germania): Dezvoltarea de software securizat.

2.4. În termeni concreți pentru producători

Pentru a rezuma, o organizație care dorește să dezvolte produse cu elemente digitale conforme cu CRA ar trebui

- Să adopte un ciclu de viață securizat al dezvoltării software-ului (SSDLC), așa cum este descris în IEC 62443-4-1 sau NIST SP 800-218 SSDF;

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Să aibă o politică de revizuire și testare a codului care să se concentreze pe identificarea vulnerabilităților (SAST, DAST, fuzzing);
- Să aplice în mod sistematic modelarea amenințărilor pentru fiecare componentă importantă;
- Să furnizeze produse cu porturi închise în mod implicit, jurnalizare activată și porturi de acces securizate;
- Să adopte o funcție PSIRT cu roluri clar definite și procese de permanență (*on-call*);
- Să definească praguri de control al calității de securitate în cadrul CI/CD (SAST, DAST, SCA, scanare secrete) însoțite de politici de tip fail-the-build.

3. Managementul securității pe parcursul ciclului de viață

Dincolo de proiectarea, dezvoltarea și producția securizată a produselor cu elemente digitale, produsul dvs. trebuie să rămână sigur pe tot parcursul ciclului său de viață. Produsele digitale evoluează - iar securitatea lor trebuie să evolueze odată cu ele. Acest lucru înseamnă că securitatea trebuie gestionată și luată în considerare în mod continuu, chiar și după introducerea pe piață a produsului cu elemente digitale.

În mod concret, producătorii sunt obligați să:[14]

1. Monitorizeze continuu vulnerabilitățile;
2. Furnizeze actualizări și remedieri de securitate în timp util;
3. Mențină o politică de divulgare a vulnerabilităților și să comunice riscurile în mod transparent riscurile către utilizatori și autoritățile de reglementare.

3.1. Monitorizarea continuă a vulnerabilităților

Odată ce un produs a fost introdus pe piață, producătorii trebuie să continue să identificevulnerabilitățile în mod activ și sistematic. Aceasta include:

- Monitorizarea bazelor de date privind vulnerabilitățile, cum ar fi baza de date europeană privind vulnerabilitățile[15] ;
- Monitorizarea alertelor și notificărilor emise de furnizori;

[14] Deși cerințele privind gestionarea vulnerabilităților sunt tratate în detaliu în anexa I, partea II, acestea decurg din punctele 1 și 2 din anexa I, partea I, și, prin urmare, sunt deja abordate în prezentul ghid.
[15] Art. 17 alineatul (5) din CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Urmărirea vulnerabilităților și expunerilor comune (CVE) asociate componentele sau bibliotecile utilizate;
- Utilizarea SBOM pentru identificarea și urmărirea dependențelor;
- Monitorizarea internă pentru identificarea de noi vulnerabilități prin programe de recompensare a descoperirii de bug-uri (bug bounty), teste de penetrare sau audituri de securitate.

Exemplu:

Un producător de camere de supraveghere de rețea utilizează module firmware open-source. Baza de date CVE relevă faptul că unul dintre aceste module conține o vulnerabilitate critică (de exemplu, CVE-2023-XXXXX). Producătorul este obligat să monitorizeze și să evalueze aceste informații și, dacă este cazul, să ia măsurile corespunzătoare.

Sursele relevante în acest sens includ:

- CVE;
- EPSS (Sistemul de evaluare a predicției exploatării);
- Ghidul ENISA privind gestionarea vulnerabilităților;
- ISO/IEC 30111: Procese de gestionare a vulnerabilităților.

3.2. Actualizări și remedieri (patch-uri) de securitate furnizate la timp

CRA impune producătorilor să răspundă rapid la vulnerabilitățile cunoscute și să distribuie în mod eficient și gratuit, actualizări de securitate pe întreaga durată a perioadei de suport.

Aceste actualizări trebuie:

- Să fie semnate digital și validate;
- Să includă un mecanism de revenire la starea inițială în caz de eroare;
- Să poată fi instalate automat, cu opțiuni de renunțare (*opt-out*) și/sau cu o interacțiune minimă din partea utilizatorului;
- Să rămână disponibile timp de cel puțin 10 ani de la punerea pe piață sau pe durata rămasă a perioadei de suport, oricare dintre aceste perioade este mai lungă.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Exemplu:

Un producător de termostate inteligente identifică o vulnerabilitate în vulnerabilitate în componenta software responsabilă de comunicația Wi-Fi. În termen de două săptămâni, se dezvoltă, se testează și se distribuie un patch de securitate prin intermediul unei actualizări OTA semnate digital. Utilizatorii primesc o notificare clară, iar actualizarea se instalează automat la repornirea dispozitivului.

Surse relevante în acest sens includ:

- ISO/IEC 29147: Dezvăluirea coordonată a vulnerabilităților;
- NIST SP 800-40: Ghid pentru gestionarea patch-urilor la nivel organizațional;
- ETSI EN 303 645: Nivel de referință de securitate pentru IoT de consum (inclusiv mecanisme de actualizare a software-ului).

3.3. Politica de raportare a vulnerabilităților și de comunicare transparentă

Transparența este esențială. CRA impune producătorilor următoarele obligații:

- Publicarea unei politici de divulgare coordonată a vulnerabilităților (CVD);
- Furnizarea unui punct de contact (de exemplu, security@company.eu) pentru raportarea vulnerabilităților;
- Informarea rapidă a utilizatorilor și a autorităților, cum ar fi ENISA sau autoritatea națională de supraveghere, în cazul unor riscuri grave;
- Comunicarea în mod transparent despre patch-urile disponibile, măsurile de atenuare și riscurile rămase.

Exemplu:

Un hacker etic raportează o vulnerabilitate critică într-un sistem de alarmă conectat prin intermediul platformei publice de divulgare coordonată a vulnerabilităților (CVD) a producătorului. În termen de 72 de ore, se confirmă primirea și, după o analiză internă, ENISA este informată prin intermediul platformei unice de raportare ENISA (prin punctele naționale de contact). În termen de trei săptămâni se distribuie un patch și toți utilizatorii sunt informați cu privire la risc și la soluția disponibilă prin e-mail și notificări în aplicație.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Surse relevante în acest sens includ:

- Modelul de maturitate pentru coordonarea vulnerabilităților (VCMM) al FIRST;
- ISO/IEC 29147: Ghiduri pentru divulgarea vulnerabilităților;
- Ghiduri ENISA privind divulgarea coordonată a vulnerabilităților (2022);
- OpenSSF VEX (Vulnerability Exploitability eXchange).

4. Securitatea lanțului de aprovizionare

CRA recunoaște faptul că un produs nu este niciodată complet „independent": acesta este alcătuit din zeci, uneori sute de componente provenite de la furnizori externi, din proiecte open-source și de la parteneri hardware. De aceea, CRA stabilește cerințe explicite pentru gestionarea riscurilor de securitate cibernetică în cadrul lanțului de aprovizionare.

În practică, producătorii trebuie:

1. Să mențină o evidență actualizată și transparentă a componentelor software utilizate prin intermediul unui SBOM;
2. Să solicite furnizorilor să respecte cerințe de securitate conforme cu CRA;
3. Să monitorizeze și să gestioneze în mod activ riscurile asociate cu dependențele open-source și externe.

4.1. Lista componentelor software (SBOM)

Un SBOM poate fi comparat cu lista de ingrediente a unui produs software: acesta conține o evidență generală a tuturor componentelor software utilizate, a versiunilor acestora și a originii lor, inclusiv a bibliotecilor open-source.

CRA impune producătorilor să mențină un SBOM și să îl poată pune la dispoziția autorităților și organismelor de reglementare, la cerere. Publicarea SBOM pentru utilizatori este opțională[16] . Acest SBOM constituie baza pentru:

- Analiza vulnerabilităților (de exemplu, prin monitorizarea CVE);
- Evaluarea impactului în cazul vulnerabilităților de tip zero-days;
- Audituri ale lanțului de aprovizionare.

[16] Dacă este pus la dispoziția utilizatorilor, clarificați unde/cum pot accesa utilizatorii acest document.

Exemplu:

Un producător de routere inteligente întocmește un SBOM care menționează în mod clar că produsul utilizează:

- OpenSSL 1.1.1n;
- BusyBox 1.35.0;
- O versiune modificată a unui modul firewall open-source.

Atunci când este divulgată o vulnerabilitate în OpenSSL (CVE-2022-XXXX), producătorul poate verifica imediat dacă produsul este afectat și poate răspunde în mod adecvat.

Surse relevante în acest sens includ:

- CycloneDX, SPDX: formate pentru SBOM (recomandate și de ENISA și NTIA);
- ISO/IEC 5230 (OpenChain): conformitatea software în lanțul de aprovizionare;
- Instrumente OpenSSF pentru generarea de SBOM și detectarea vulnerabilităților.

4.2. Cerințe de securitate pentru furnizori

CRA impune, de asemenea, producătorilor să se asigure că furnizorii și dezvoltatorii externi respectă cerințe de securitate comparabile cu cele aplicabile propriei echipe. Responsabilitatea nu poate fi transferată; vulnerabilitățile din componentele furnizate de terți pot genera, la rândul lor, obligații de conformitate în temeiul CRA.

Concret, aceasta înseamnă:

- Includerea clauzelor de securitate cibernetică în contractele cu furnizorii;
- Efectuarea unei verificări de securitate la selectarea furnizorilor de software;
- Verificarea periodică a conformității partenerilor cu, de exemplu:
    - ISO/IEC 27001 (securitatea informațiilor);
    - IEC 62443-4-1 (dezvoltarea securizată de produse);
    - Modelele de maturitate OWASP SAMM sau BSIMM.
- Drepturi contractuale de audit și niveluri minime de asigurare (de exemplu, certificarea conformității) pentru componentele critice;
- Notificarea în termen de 24 de ore a vulnerabilităților critice identificate de furnizor care afectează produsele dumneavoastră cu elemente digitale.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Exemplu:

Un producător de dispozitive medicale IoT colaborează cu un furnizor de software din Asia. Contractul stipulează că acest furnizor:

- Dezvoltă în condiții de siguranță, în conformitate cu IEC 62443-4-1;
- Documentează toate componentele open-source utilizate;
- Menține o politică de vulnerabilitate cu raportare obligatorie în termen de 24 de ore.

4.3. Gestionarea riscurilor asociate componentelor open-source și bibliotecilor externe

Software-ul open-source oferă numeroase avantaje, dar implică și o serie de riscuri: vulnerabilități, actualizări lipsă, licențe neclare sau administratori nesiguri. CRA impune producătorilor să gestioneze și să monitorizeze în mod activ aceste riscuri.

Cele mai bune practici includ:

- Utilizarea unor instrumente de scanare a dependențelor (de exemplu, OWASP Dependency-Check, Snyk, Trivy);
- Alertele automate pentru vulnerabilități (de exemplu, prin GitHub Advisories);
- Utilizarea exclusivă a proiectelor open-source mature și întreținute în mod activ;
- Aplicarea unor filtre de securitate în pipeline-urile CI/CD (care blochează build-urile atunci când sunt identificate CVE-uri cunoscute);
- Utilizarea VEX pentru a reduce volumul de alerte generate de CVE-uri care nu sunt exploatabile în practică;
- Impunerea unui nivel minim de receptivitate din partea mentenanților la selectarea componentelor OSS.

Exemplu:

Un producător utilizează o bibliotecă JavaScript populară (de exemplu, Log4j) într-o interfață web. Atunci când este descoperită vulnerabilitatea Log4Shell (CVE-2021-44228), producătorul știe imediat, pe baza analizei SBOM, care sunt versiunile afectate și poate izola și remedia produsele vizate.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Surse relevante în acest sens includ:

- NIST SSDF (Cadrul de dezvoltare a software-ului securizat);
- Ghidurile de securitate ENISA OSS;
- OpenSSF Scorecard: Evaluarea obiectivă a calității proiectelor open-source.

Concluzie

Prezentul ghid reprezintă o primă **transpunere tehnică a cerințelor prevăzute în Anexa I, Partea I, a CRA în sugestii și recomandări practice**. Acesta evidențiază **patru componente** esențiale pentru conformitatea cu CRA: (1) o abordare a securității cibernetice bazată pe riscuri, care implică o evaluare a riscurilor, măsuri de securitate adaptate și luarea în considerare a modelelor de amenințări, a suprafețelor de atac și a impactului; (2) principiul securității prin proiectare și prin configurare implicită; (3) obligațiile de gestionare a securității pe tot parcursul ciclului de viață al produsului cu elemente digitale; (4) considerente și controale privind lanțul de aprovizionare. Pentru fiecare dintre aceste componente sunt formulate sugestii practice privind modul de implementare și de respectare a obligațiilor aferente, pe baza bunelor practici și standardelor recunoscute. Totuși, aceste orientări pot suferi modificări, în funcție de evoluția discuțiilor privind standardele aflate în curs de elaborare și de viitoarele dezvoltări de reglementare. Ca pași următori pentru IMM-uri, se recomandă consultarea unor orientări suplimentare disponibile în baza de date (Repository central) **SECURE**, precum **CRA Methodological Compliance Assessment Framework** care oferă un set de instrumente și o listă de verificare pas cu pas pentru conformitatea cu CRA dincolo de Anexa I, precum și **CRA 101: Understanding CRA Obligations**, care oferă o prezentare sintetică, accesibilă începătorilor, a obligațiilor juridice care decurg din CRA.