CRA interoperabilnost između normi i prakse

"CURIUM Project"

Prof.dr.sc. Miroslav Bača

CEO, Cyber Security d.o.o

29.05.2025

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre ('granting authority'), under the powers delegated by the European Commission ('European Commission'), under the Grant Agreement No. 101190372. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC. Neither the European Union nor the granting authority can be held responsible for them.

Vizija

- Projekt CURIUM osigurava sigurniji i otporniji digitalni krajolik jačanjem sigurnosti, privatnosti i odgovornosti hardverskih i softverskih proizvoda digitalnim elementima.
- U svojoj srži, CURIUM uvodi novi kontinuum usklađenosti – skup alata i usluga orijentiranih na kibernetičku sigurnost osmišljenih za pružanje informacija, smjernica, pouzdanog testiranja sigurnosti i pojednostavljene usklađenosti sa Zakonom o kibernetičkoj otpornosti (CRA).
- Pojednostavljivanjem i automatizacijom usklađenosti, CURIUM osnažuje europska mala i srednja poduzeća – posebno mikro i mala poduzeća – da provode samoprocjene, pripreme se za certifikaciju treće strane i smanje troškove, a istovremeno ubrzaju vrijeme izlaska na tržište.

Ciljevi

- Razvoj inovativnog kontinuuma usklađenosti za automatizaciju usklađenosti s propisima CRA.
- Poticanje širokog usvajanja modularnim, isplativim i rješenjima otvorenog koda prilagođenim potrebama industrije.
- Poticanje znanja i izgradnje kapaciteta za podršku implementaciji CRA.
- Korištenje agilnog procesa validacije s kontinuiranim povratnim petljama.
- Poticanje dugoročne održivosti aktivnim uključivanjem dionika industrije i kreatora politika u razvoj i obuku alata.

Konzorcij


CYBER SECURITY D.O.O.


NATIONAL
CYBER
SECURITY
AUTHORITY
GR


NET
EMERGING NETWORKS & APPLICATIONS


eit
Digital


nealogic


APIROPLUS
SERVICES


AEGIS
IT RESEARCH


Sphynx


COMMISSIONER
OF COMMUNICATIONS
Digital
Security
Authority

CRA

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024, on horizontal cybersecurity requirements for **products with digital elements** and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828

= CRA

CRA se primjenjuje od **11 studenog 2027**.
Članak 14 (izvještavanje) primjenjuje se od **11 rujna 2026**
Poglavlje IV (članci 35 do 51)primjenjuju se od **11 srpnja 2026**.

The subject

Uredba propisuje

- (a) pravila za stavljanje na tržište proizvoda s digitalnim elementima radi osiguranja kibernetičke sigurnosti takvih proizvoda;
- (b) esecijalne kibernetičke sigurnosne zahtejve za dizajn, razvoj i proizvodnju proizvoda s digitalnim elementima, te obaveze gospodarskih subjekata u vezi s tim proizvodima u pogledu kibernetičke sigurnosti;
- (c) esencijalni kibernetički sigurnosni zahtjevi za procese upravljanja ranjivostima koje su proizvođači uspostavili kako bi osigurali kibernetičku sigurnost proizvoda s digitalnim elementima tijekom razdoblja u kojem se očekuje da će proizvodi biti u upotrebi te obaveze gospodarskih subjekata u vezi s tim procesima;
- (d) pravila o nadzoru tržišta, uključujući praćenje i provedbu pravila i zahtjeva.

Proizvod s digitalnim elementima

‘**proizvod s digitalnim elementima**’ – softverski ili hardverski proizvod i njegova rješenja za daljinsku obradu podataka, uključujući softverske ili hardverske komponente koje se stavljaju na tržište zasebno (Članak 3, Definicije) uz iznimke i specifičnosti

CyReA

Cyber Resilience Assessment

Utvrđuje spada li proizvod s digitalnim elementima **u područje primjene CRA** i određuje potreban postupak ocjenjivanja sukladnosti.

Proizvod s digitalnim elementima

Proizvod s digitalnim elementima biti će dostupni na tržištu samo ako:

- ispunjavaju **bitne zahtjeve kibernetičke sigurnosti** utvrđene u dijelu I Anexa, pod uvjetom da su pravilno instalirani, održavani, koriste se za svoju namjeru ili pod uvjetima koji se razumno mogu predvidjeti I, gdje je primjenjivo, da su instalirana potrebna sigurnosna ažuriranja i

- **procesi koje je uspostavio proizvođač** su u skladu sa bitnim zahtjevima kibernetičke sigurnosti utvrđenima u dijelu II Anexa I.

Proizvod s digitalnim elementima

Proizvođači provode **procjenu rizika kibernetičke sigurnosti**.

Proizvođači uzimaju u obzir ishod te procjene tijekom faza planiranja, projektiranja, razvoja, proizvodnje, isporuke i održavanja proizvoda s digitalnim elementima s ciljem minimiziranja rizika kibernetičke sigurnosti, sprječavanja incidenata i minimiziranja njihovog utjecaja, uključujući I u odnosu na zdravlje i sugrunost korisnika.

Procjena rizika kibernetičke sigurnosti mora se **dokumentirati i ažurirati.**

DPRA

Digital Product Risk management

Podržava proizvođače u **procjeni rizika kibernetičke sigurnosti** tijekom životnog ciklusa proizvoda kako bi proaktivno smanjili sigurnosne prijetnje.

Proizvod s digitalnim elementima

Proizvođači provode **procjenu rizika kibernetičke sigurnosti**.

Procjena rizika kibernetičke sigurnosti moram naznačiti jesu li i ako jesu, na koji način sigurnosni zahtjevi u dijelu I. u točki 2 Anexa I primjenjivi na relevantni proizvod s digitalnim elementima I kako se ti zahtjevi provode na temelju procjene rizika kibernetičke sigurnosti. Također potrebno je naglasiti kako proizvođač treba primjeniti dio I. točku 1 Anexa I I zahttjeve za rukovanje ranjivostima utvrđenima u dijeli II Anexa I.

DPMA

Digital Product Maturity Assessment

Nudi strukturirani **okvir za ublažavanje rizika** temeljen na zrelosti proizvoda, pomažući proizvođačima da implementiraju učinkovite sigurnosne mjere.

Proizvod s digitalnim elementima

Proizođači proizvoda s digitalnim elementima moraju:

(1) **identificirati I dokumentirati ranjivosti** i komponente sadržane u proizvodima s digitalnim elementima, uključujući izradu softverskog popisa materijala u uobičajeno korištenom I strojno čitljivom format koji pokriva barem dio najviše ovisnosti proizvoda;

(2) u vezi s rizicima koji su povezani s proizvodima s digitalnim elementima, **bez odgode riješiti I otkloniti ranjivosti**, uključujući pružanje sigurnosnih ažuriranja, gdje je to tehnički izvedivo, nova sigurnosna ažuriranja moraju se provesti neovisno od ažuriranja funkcionalnosti

PSTVA

Penetration Self-Testing and Vulnerability Assessment

Oprema korisnike alatima za **procjenu ranjivosti, pregled koda i penetracijsko testiranje**, jačajući napore u skladu s propisima.

Proizvod s digitalnim elementima

Proizođači proizvoda s digitalnim elementima moraju:

(3) **primjeniti učinkovitei redovite testove i preglede** sigurnosti proizvoda s digitalnim elementima;

(4) nakon što je u sigurnosni ažuriranje dostupno, **dijeliti i javno objavljivati informacije o ispravljenim ranjivostima…**

STVA

Penetration Self-Testing and Vulnerability Assessment

Oprema korisnike alatima za **procjenu ranjivosti, pregled koda i penetracijsko testiranje**, jačajući napore u skladu s propisima.

Proizvod s digitalnim elementima

Proizvođači uz proizvod s digitalnim elementima dostavljaju ili **presliku EU izjave o sukladnosti ili pojednostavljenu EU izjavu o sukladnosti**. Ako se dostavlja pojednostavljena EU izjava o sukladnosti, ona mora sadržavati točnu internetsku adresu na kojoj je dostupna potpuna EU izjava o sukladnosti. Sastavljanjem EU izjave o sukladnosti proizvođač preuzima odgovornost za sukladnost proizvoda s digitalnim elementima.

Conformity Assessment and Compliance

Osigurava vođeni prostup **tehničkoj dokumentaciji i samoanalizi**, osiguravajući usklađenost sa zahtjevima CRA.

Izgradnja kapaciteta

- **Obuka**: Platforma CURIUM nudit će prilagođene materijale i aktivnosti za obuku, koristeći resurse partnera u konzorciju ivanjskih izvora. Sadržaj će obuhvaćati alate za usklađenost CURIUM-a I relevanten politike EU-a.
- **Eksperimentiranje i testiranje**: Partner CURIUM-a p-NET osigurati će infrastruktu za testiranje u oblaku na razini konzorcija kao i za vanjske dionike, osiguravajući sigurno I posuzdano poslovanje.
- **Konzultantske usluge i podrška**: konzultantske usluge povezati će industriju i mala i srednja poduzeća sa relevantnim stručnim znanjem, rješavajući kibernetičku otpornost i usklađenost s propisima u EU.

Izgradnja kapaciteta

- **Podizanje razine svijesti I transfer znanja**: Cilj CURIUM-a je podići razinu svijesti i angažirati dionike u različitim sektorima (javna uprava, akademski sektor, industrija...) kako bi se maksimizirao njegov utjecaj na europsko gospodarstvo i društvo. Aktivnosti će promovirati inovacije i javno razumijevanje tehnologija energetske održivosti. Akademija vještina kibernetičke sigurnsoti EU biti će ključni partner u naporima za obuku i širenje informacija. Radionice I informativni dani održavat će se kako bi se podržala aktivnost.
- **Suradnja i održivost**: Održivost nakon projekta biti će osigurana putem partnera CURIUM-a, EIT-a, koji aktivno sudjeluje u više europskih centara za digitalne inovacije. Osim toga suradnja s ENIS-om, nacionalnim vlastima i Europskim centrum za kompetencije u kibernetičkoj sigurnosti (ECCC) ojačat će europske sposobnosti u području kibernetičke sigurnosti I potaknuti dugoročni rast.

Ako želite saznati više...

curium-project

@Curium_Project

curium-project.eu

https://ec.europa.eu/eusurvey/runner/EU_CRA_CURIUM

Hvala na pažnji

Prof.dr.sc. Miroslav Bača

CEO, Cyber Secutiy d.o.o.

ceo@cyber-security.hr