



CYBER RESILIENCE ACT VO VEREJNEJ SPRÁVE

Čo prináša nová európska regulácia kybernetickej bezpečnosti pre orgány verejnej správy — so zameraním na verejné obstarávanie

Národný bezpečnostný úrad

O ČOM BUDE REČ

- Čo je Cyber Resilience Act (CRA) a prečo vzniká
- Na koho sa CRA priamo vzťahuje
- Prečo je dôležitý aj pre orgány verejnej správy
- Kľúčové termíny nabiehania povinností
- Čo CRA prináša — v skratke (požiadavky, CE označenie, klasifikácia produktov)
- Dôsledky pre verejné obstarávanie
- Čo robiť už teraz
- Kde nájsť pomoc a informácie



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

ČO JE CYBER RESILIENCE ACT

- Nariadenie EÚ 2024/2847 o horizontálnych požiadavkách na kybernetickú bezpečnosť produktov s digitálnymi prvkami
- Prvý celoeurópsky predpis, ktorý stanovuje bezpečnostné požiadavky priamo na hardvér a softvér uvádzané na trh EÚ
- Cieľ: aby boli produkty s digitálnymi prvkami bezpečné už pri návrhu a počas celej doby používania
- Vstúpil do platnosti 10. decembra 2024, povinnosti nabiehajú postupne do decembra 2027
- *Dopĺňa (nenahrádza) smernicu NIS2, ktorá sa týka bezpečnosti organizácií a služieb*



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

- Rastúci počet pripojených ('smart') zariadení a softvéru s prístupom do siete
- Časté bezpečnostné zraniteľnosti v produktoch, ktoré výrobcovia dlho neopravovali
- Doteraz chýbala jednotná európska povinnosť 'bezpečnosti už v návrhu' pre väčšinu digitálnych produktov
- Cieľ: znížiť riziko rozsiahlych kybernetických incidentov spôsobených zraniteľnými zariadeniami a softvérom naprieč EÚ

NA KOHO SA CRA PRIAMO VZŤAHUJE

Výrobcovia

uvádzajú produkt s
digitálnymi prvkami
na trh EÚ pod vlastným
menom/značkou

Dovozcovia

uvádzajú na trh EÚ
produkty vyrobené
mimo EÚ

Distribútori

dodávajú produkty na trh
EÚ v rámci
dodávateľského reťazca

Splnomocnení zástupcovia

zastupujú výrobcov
usadených mimo EÚ



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

PREČO SA CRA TÝKA AJ VÁS, HOCI NIE STE VÝROBCA

- Ako orgán verejnej správy ste spravidla v úlohe odberateľa a používateľa produktov, nie výrobcu
- CRA preto neukladá orgánom verejnej správy priame povinnosti výrobcu
- Osobitná situácia: softvér vyvinutý výhradne pre internú potrebu organizácie a neuvádzaný na trh spravidla pod CRA nespadá
- *Ak by ste produkt začali poskytovať iným subjektom alebo verejnosti, môžete sa dostať do postavenia výrobcu — v prípade pochybností odporúčame konzultáciu*



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

VAŠA HLAVNÁ ROLA: VEREJNÝ OBSTARÁVATEĽ

- Nakupujete produkty s digitálnymi prvkami (počítače, sieťové zariadenia, IoT, softvér, aplikácie) prostredníctvom verejného obstarávania
- Od plného uplatňovania CRA (11. 12. 2027) budú musieť byť takéto produkty pri uvedení na trh v súlade s CRA
- Vaša úloha: pri príprave a vyhodnocovaní zákaziek zohľadniť, že dodávaný produkt musí (alebo bude musieť) spĺňať požiadavky CRA
- Ide o novú 'kvalitatívnu' dimenziu obstarávania — podobne ako napríklad požiadavky na energetickú efektívnosť

KĽÚČOVÉ TERMÍNY CRA

10. 12. 2024



Nariadenie
vstúpilo do
platnosti

11. 6. 2026



Rámec pre
notifikáciu
autorizovaných
osôb posudzovania
zhody (kap. IV)

11. 9. 2026



Povinnosť hlásiť
aktívne zneužívané
zraniteľnosti a
závažné incidenty
(čl. 14)

11. 12. 2027



Plné uplatňovanie CRA
— bezpečnostné
požiadavky,
posudzovanie zhody, CE
označenie



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

ZÁKLADNÉ POVINNOSTI VÝROBCOV (V SKRATKE)

- 'Bezpečnosť už v návrhu' (security by design) a bezpečné predvolené nastavenia
- Riadenie zraniteľností počas celej doby podpory produktu, vrátane evidencie komponentov (SBOM)
- Bezodkladné odstraňovanie zistených zraniteľností a poskytovanie bezpečnostných aktualizácií
- Hlásenie aktívne zneužívaných zraniteľností a závažných incidentov národnému CSIRT — v lehotách 24 hodín / 72 hodín / 14 dní
- Poskytovanie zrozumiteľných informácií a pokynov používateľovi



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

ZÁKLADNÉ BEZPEČNOSTNÉ POŽIADAVKY (PRÍLOHA I)

ČASŤ I — Vlastnosti produktu

- Bez známych zneužíteľných zraniteľností pri uvedení na trh
- Bezpečné predvolené nastavenia
- Ochrana pred neoprávneným prístupom
- Ochrana dôvernosti a integrity dát
- Mechanizmus na bezpečné aktualizácie

ČASŤ II — Riadenie zraniteľností

- Identifikácia a evidencia zraniteľností a komponentov (SBOM)
- Bezodkladné odstraňovanie zraniteľností
- Pravidelné testovanie bezpečnosti produktu
- Zverejňovanie informácií o opravených zraniteľnostiach
- Bezpečná distribúcia aktualizácií

CE OZNAČENIE A VYHLÁSENIE O ZHODE

- CE označenie = viditeľné potvrdenie, že výrobca deklaruje súlad produktu s požiadavkami CRA
- Vyhlásenie o zhode (EU Declaration of Conformity) — dokument, ktorý má produkt sprevádzať
- Od 11. 12. 2027 nebude možné uviesť na trh EÚ produkt s digitálnymi prvkami spadajúci pod CRA bez CE označenia podľa tohto nariadenia
- *Pri obstarávaní: CE označenie a vyhlásenie o zhode budú jedným zo signálov, že dodávateľ berie požiadavky CRA vážne — nie však jediným*

KLASIFIKÁCIA PRODUKTOV (ZJEDNODUŠENE)

Bežné produkty	Väčšina produktov s digitálnymi prvkami. Výrobca si spravidla sám posúdi zhodu (samohodnotenie).
Dôležité produkty (príloha III)	Napr. niektoré operačné systémy, firewally, správčovské nástroje. Vyžadujú harmonizovanú normu alebo posúdenie autorizovanou osobou.
Kritické produkty (príloha IV)	Napr. vybrané hardvérové bezpečnostné moduly a čipové karty. Vyžadujú povinnú certifikáciu treťou stranou.



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

ČO TO ZNAMENÁ PRE VEREJNÉ OBSTARÁVANIE — PREHĽAD

- CRA nezavádza nový samostatný 'kybernetický' postup obstarávania — premieta sa do existujúcich pravidiel verejného obstarávania
- Relevantné najmä pri nákupe hardvéru s pripojením do siete, softvéru, aplikácií a IoT zariadení
- Dotýka sa technických špecifikácií, podmienok účasti, hodnotiacich kritérií aj zmluvných podmienok
- *Nasledujúce odporúčania vychádzajú zo všeobecných zásad CRA — nejde o záväznú metodiku*

Na čo sa pýtať dodávateľa

- Spadá ponúkaný produkt pod CRA? (má digitálny prvok a pripojenie do siete alebo zariadenia?)
- Do ktorej kategórie patrí — bežný, dôležitý alebo kritický produkt?
- Aké je deklarované 'obdobie podpory' (support period) a spôsob poskytovania bezpečnostných aktualizácií?
- Má produkt CE označenie a vyhlásenie o zhode podľa CRA (od relevantného termínu)?
- Existuje k produktu SBOM alebo iný zoznam komponentov?



HODNOTIACE KRITÉRIÁ A ZMLUVNÉ PODMIENKY

- Zvážiť dĺžku obdobia podpory a záväzok poskytovať bezpečnostné aktualizácie ako súčasť hodnotenia — nielen cenu
- Zaviesť zmluvnú povinnosť dodávateľa informovať obstarávateľa o závažných zraniteľnostiach či incidentoch týkajúcich sa dodaného produktu
- Zohľadniť náklady na celý životný cyklus produktu (TCO), nielen obstarávaciu cenu
- Vyhradiť si právo požadovať dokumentáciu k zhode s CRA, napr. vyhlásenie o zhode

- CRA zavádza pojem 'obdobie podpory' (support period) — obdobie, počas ktorého výrobca poskytuje bezpečnostné aktualizácie
- Dĺžka obdobia podpory sa líši produkt od produktu — dôležité poznať ju vopred pri plánovaní obstarávania
- Dôsledok pre verejnú správu: dlhšie obdobie podpory môže znamenať nižšie riziko aj nižšie budúce náklady na výmenu či opravu
- Odporúčanie: zahrnúť informáciu o období podpory do technickej dokumentácie k zákazke

RIZIKÁ NESPRÁVNE NASTAVENÉHO OBSTARÁVANIA

- Nákup produktu bez jasne deklarovanej podpory — riziko nezápлатovaných zraniteľností po nábehu plných povinností CRA
- Chýbajúca zmluvná povinnosť hlásiť incidenty — neskoré zistenie bezpečnostného problému
- Podceňovanie životného cyklu produktu — vyššie dlhodobé náklady na výmenu alebo opravu
- Ignorovanie klasifikácie produktu — riziko obstarania produktu, ktorý nespĺňa požadovanú úroveň zhody

ČO ROBIŤ UŽ TERAZ — KONKRÉTNE KROKY

- 1 Zmapovať, aké produkty s digitálnymi prvkami vaša organizácia nakupuje a používa
- 2 Zaradiť pripravované obstarávania IT/OT produktov do plánu s dostatočným predstihom pred termínmi CRA
- 3 Doplniť do technických špecifikácií otázky na súlad s CRA, obdobie podpory a aktualizácie
- 4 Preškoliť zodpovedné osoby (obstarávanie, IT, právne oddelenie) v základoch CRA
- 5 Sledovať usmernenia NBÚ a Európskej komisie k CRA



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

- NBÚ je určeným orgánom trhového dohľadu pre CRA na Slovensku
- Dohliada na dodržiavanie požiadaviek CRA výrobcami, dovozcami a distribútormi na slovenskom trhu
- Poskytuje metodickú podporu a informácie aj orgánom verejnej správy
- Priebežne aktualizuje informačný web venovaný CRA
 - www.cra.nbu.gov.sk



ZHRNUTIE — KLÍČOVÉ ODKAZY

CRA prichádza — postupne, s jasnou časovou osou do decembra 2027

Netýka sa vás priamo ako výrobcu, ale ovplyvní, čo a ako budete obstarávať

Netreba sa báť — existuje dostatok času na prípravu a metodická podpora zo strany NBÚ

Malé kroky už dnes (otázky do tendrov, zmapovanie nákupov) vám ušetria problémy neskôr



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

KDE NÁJSŤ POMOC A INFORMÁCIE

- Informačný web NBÚ k CRA: cra.nbu.gov.sk
- Oficiálny text nariadenia (EÚ) 2024/2847 a jeho prílohy
- Usmernenia a odpovede na časté otázky Európskej komisie k CRA
- SK CERT - informácie k nahlasovaniu zraniteľností a incidentov



ĎAKUJEM ZA POZORNOSŤ

Priestor na otázky a diskusiu.

Ďalšie informácie: cra.nbu.gov.sk