



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

Usmernenie k nahlasovacím povinnostiam podľa článku 14 aktu o kybernetickej odolnosti (CRA)

Tento dokument poskytuje výrobcovi produktov s digitálnymi prvkami metodické usmernenie k plneniu nahlasovacích povinností podľa článku 14 nariadenia (EÚ) 2024/2847 (CRA), a to z pohľadu Národného bezpečnostného úradu (NBÚ) a jeho národnej jednotky pre riešenie kybernetických bezpečnostných incidentov SK-CERT.

nbu.gov.sk · sk-cert.sk · cra.nbu.gov.sk
Verzia 1.0 – september 2026

TLP:CLEAR

Zrieknutie sa zodpovednosti

Toto usmernenie má výrobcom produktov s digitálnymi prvkami poskytnúť orientáciu, pokiaľ ide o ich nahlasovacie povinnosti podľa článku 14 CRA.

Usmernenie nepredstavuje právne poradenstvo, ani oficiálny výklad regulačných požiadaviek a nemožno ho považovať za a nepredstavuje schválenie konkrétneho postupu alebo riešenia ani akceptáciu rizík. Žiadnu jeho časť nemožno vykladať ako potvrdenie, že konkrétny postup, súbor opatrení alebo rozhodnutie spĺňa právne, regulačné či dohľadové požiadavky vyplývajúce okrem iného z práva EÚ, národnej legislatívy, usmernení alebo politík. Uvedené príklady a odporúčané postupy majú ilustratívny charakter a nenahrádzajú vlastné riadiace a kontrolné procesy výrobcu ani nezávislé odborné poradenstvo. Za svoje rozhodnutia, plnenie povinností a riadenie rizík zodpovedá výlučne príslušný hospodársky subjekt.

Toto usmernenie nemožno použiť ako dôkaz súladu s právnymi predpismi, ako schválenie zo strany orgánu verejnej moci ani ako doklad náležitej starostlivosti a nemožno sa naň odvolávať ako na obhajobu, ospravedlnenie či poľahčujúcu okolnosť v žiadnom regulačnom, kontrolnom, vyšetrovacom ani sankčnom konaní.

Ak nie je výslovne uvedené inak alebo z kontextu nevyplýva inak, pojmy použité v tomto usmernení, ktoré sa zároveň vyskytujú v texte CRA, majú rovnaký význam ako v CRA.

NBÚ si vyhradzuje právo toto usmernenie kedykoľvek a podľa potreby aktualizovať.

Akt o kybernetickej odolnosti (CRA)

Čo je CRA?

Akt o kybernetickej odolnosti (Cyber Resilience Act, CRA; nariadenie (EÚ) 2024/2847) nadobudlo platnosť 10. decembra 2024. Zavádza povinné kybernetickobezpečnostné požiadavky pre všetok pripojený hardvér a softvér uvádzaný na trh EÚ. Cieľom je zabezpečiť, aby digitálne produkty boli navrhované, vyvíjané a vyrábané s ohľadom na bezpečnosť a aby výrobcovia niesli zodpovednosť za riešenie zraniteľností počas celého životného cyklu produktu.

Na dosiahnutie tohto cieľa sa preto CRA zameriava najmä na:

- presadzovanie bezpečnostných štandardov už vo fáze návrhu produktu a podporenie princípu „bezpečnosti už od návrhu“ (security by design);
- zavedenie povinnosti v oblasti riadenia zraniteľností počas celej životnosti produktu;
- zvýšenie transparentnosti voči používateľom, pokiaľ ide o bezpečnostné aktualizácie a obdobie podpory;
- prispievanie k harmonizovaného a odolného jednotného digitálneho trhu EÚ.

Zavádzanie CRA prebieha postupne od decembra 2024 do decembra 2027, aby výrobcovia mali dostatok času prispôbiť sa novým požiadavkám. Nahlasovacie povinnosti podľa článku 14 CRA sa však uplatňujú skôr – od 11. septembra 2026 – keď subjekty, ktorých produkty patria do pôsobnosti CRA, musia začať hlásiť aktívne zneužívané zraniteľnosti a závažné incidenty ovplyvňujúce bezpečnosť produktu.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti).

Rozsah pôsobnosti CRA

CRA sa vzťahuje na širokú škálu produktov s digitálnymi prvkami (PDE) dodávaných na trh EÚ. Do jeho pôsobnosti patria výrobcovia, dovozcovia a distribútori hardvérového a softvérového tovaru, ktorý sa priamo alebo nepriamo pripája k sieti, a to s určitými výnimkami.

Definícia PDE

„Softvérový alebo hardvérový produkt a jeho riešenia spracovania údajov na diaľku vrátane softvérových alebo hardvérových komponentov, ktoré sa uvádzajú na trh samostatne.“

Prakticky ide o akýkoľvek softvérový alebo hardvérový produkt, ktorý sa dokáže pripojiť k zariadeniu alebo sieti. Ak produkt obsahuje čip, vykonáva kód a na fungovanie využíva dátové pripojenie (napr. Wi-Fi, Bluetooth alebo fyzické sieťové pripojenie), pravdepodobne patrí do pôsobnosti CRA.

Do pôsobnosti CRA patria napríklad: notebooky, smartfóny, inteligentné domáce spotrebiče, prvky priemyselného IoT, operačné systémy, samostatné mobilné aplikácie a cloudové služby, bez ktorých produkt nemôže plniť svoju funkciu.

Mimo pôsobnosti CRA naopak zostávajú: nepripojené zariadenia (napr. jednoduchá kalkulačka) a produkty upravené osobitnou odvetvovou legislatívou, ako sú napríklad zdravotnícke pomôcky alebo motorové vozidlá.

CRA rozdeľuje produkty do troch rizikových kategórií (default, dôležitá a kritická). Tieto kategórie ovplyvňujú spôsob posudzovania zhody pred uvedením produktu na trh, avšak nahlasovacie povinnosti uvedené v tomto dokumente sa vzťahujú na produkty vo všetkých troch kategóriách rovnako.

Upozornenie

Pre offline produkty a niektoré vylúčené odvetvia platia konkrétne výnimky. Posúdenie, či sa na konkrétny produkt výnimka vzťahuje, je vždy vecou vlastného právneho a technického posúdenia výrobcu.

Povinné nahlasovanie

Pred úplným nadobudnutím účinnosti CRA koncom roka 2027, keď musí byť každý relevantný produkt v plnom súlade so všetkými požiadavkami (napr. označenie CE, posúdenie rizík), nastupujú kľúčové nahlasovacie povinnosti skôr – už 11. septembra 2026. Aj keď produkty ešte nemusia spĺňať všetky pravidlá bezpečného návrhu, výrobcovia produktov patriacich do pôsobnosti CRA majú od tohto dátumu zákonnú povinnosť podľa článku 14 nahlasovať závažné bezpečnostné udalosti týkajúce sa ich produktov.

Čo sa nahlasuje?

Aktívne zneužívané zraniteľnosti

To znamená, ak existujú spoľahlivé dôkazy, že škodlivý subjekt zraniteľnosť v produkte s digitálnymi prvkami aktívne zneužíva.

Závažné incidenty

To znamená, akýkoľvek incident, ktorý negatívne ovplyvňuje alebo môže ovplyvniť bezpečnostné funkcie produktu, napríklad ochranu údajov alebo integritu systému.

Ak dôjde k aktívne zneužívanej zraniteľnosti alebo závažnému incidentu v integrovanom komponente tretej strany, podať príslušné hlásenia je povinný výrobca finálneho produktu, hneď ako sa dozvie, že je jeho konkrétny produkt tým dotknutý.

Lehoty na nahlasovanie

Výrobcovia hlásia aktívne zneužívanú zraniteľnosť alebo závažný incident príslušnej národnej jednotke CSIRT – určenej podľa miesta svojho hlavného usadenia v EÚ – a Agentúre Európskej únie pre kybernetickú bezpečnosť (ENISA).

1. Včasné varovanie (Early Warning)

Do 24 hodín od okamihu, keď sa výrobca dozvie o aktívne zneužívanej zraniteľnosti alebo o závažnom incidente. V prípade aktívne zneužívanej zraniteľnosti začína táto lehota plynúť okamihom, keď existujú spoľahlivé dôkazy, že škodlivý subjekt zraniteľnosť aktívne zneužíva. Ide o počiatočné hlásenie, ktoré opisuje podozrenie na škodlivý úmysel a dotknuté členské štáty; úplné technické podrobnosti sa v tejto fáze nevyžadujú a podanie včasného varovania sa nesmie odkladať kvôli čakaniu na podrobnú analýzu.

2. Podrobné hlásenie (72-hodinové hlásenie)

Do 72 hodín od okamihu, keď sa výrobca o zneužití zraniteľnosti alebo o závažnom incidente dozvie. Ide o podrobnejšie hlásenie obsahujúce počiatočné posúdenie závažnosti, povahy udalosti a prípadných zmierňujúcich opatrení. Po podaní včasného varovania je potrebné podrobné hlásenie podať najneskôr do 48 hodín od jeho podania.

3. Záverečná správa (Final Report)

V prípade aktívne zneužívanej zraniteľnosti sa podáva do 14 dní od sprístupnenia nápravného alebo zmierňujúceho opatrenia. V prípade závažného incidentu sa podáva najneskôr do jedného mesiaca od podania podrobného hlásenia. Záverečná správa obsahuje úplnú technickú analýzu, opis príčin a prijaté nápravné opatrenia.

Úplný výpočet informácií, ktoré musí výrobca v jednotlivých fázach uviesť, upravuje priamo článok 14 CRA.

Národný CSIRT ako koordinujúci CSIRT

Hneď ako výrobca podá hlásenie, dostane ho súčasne ENISA a národný CSIRT krajiny, v ktorej má výrobca svoje hlavné miesto podnikateľskej činnosti. Pre výrobcov usadených na území Slovenskej republiky je touto národnou jednotkou SK-CERT, ktorý v takom prípade vystupuje ako koordinujúci CSIRT a plní dve kľúčové funkcie:

- overuje, že osoba podávajúca hlásenie je oprávneným zástupcom výrobcu;
- šíri hlásenie ďalším národným CSIRTom v členských štátoch, v ktorých bol podľa údajov výrobcu jeho produkt uvedený na trh

Koordinujúci CSIRT je ďalej oprávnený od výrobcu po podaní hlásenia vyžiadať si priebežné správy, aby získal ďalšie technické podrobnosti alebo aktuálny stav prebiehajúceho šetrenia.

Odložené šírenie hlásení zo strany CSIRT

Podľa rámca pre nahlasovanie podľa CRA má CSIRT právomoc dočasne odložiť šírenie podaného hlásenia o aktívne zneužívanej zraniteľnosti alebo závažnom incidente ďalším národným CSIRT.

CSIRT môže šírenie hlásenia (alebo jeho časti) odložiť v prípadoch, keď kybernetickobezpečnostné riziká spojené s jeho šírením prevažujú nad bezpečnostným prínosom, a keď okrem iného štandardné postupy zdieľania informácií nezaručujú dostatočnú úroveň ich zabezpečenia.

Odklad je vždy časovo obmedzený a vzťahuje sa len na konkrétne situácie, napríklad:

- do 72 hodín sa očakáva sprístupnenie účinnej opravy;
- existuje vysoké riziko, že zdieľanie informácie umožní rýchle vytvorenie exploitu;
- prebieha proces koordinovaného zverejňovania zraniteľnosti (CVD).

Ak CSIRT odklad uplatní, bezodkladne o tomto rozhodnutí, jeho odôvodnení a predpokladanom termíne následného šírenia informuje agentúru ENISA.

Delegované nariadenie Komisie (EÚ) 2026/881 z 11. decembra 2025, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 určením podmienok uplatňovania dôvodov súvisiacich s kybernetickou bezpečnosťou v súvislosti s odloženým rozosielením oznámení

Spôsob nahlasovania na Slovensku – JISKB namiesto priameho prihlásenia do SRP ENISA

Na úrovni celej EÚ zriaďuje ENISA podľa článku 16 CRA centralizovanú Jednotnú oznamovaciu platformu (Single Reporting Platform - SRP), prostredníctvom ktorej sa hlásenia podľa článku 14 CRA spravidla podávajú a odkiaľ sú automaticky zdieľané s príslušným národným CSIRT aj s agentúrou ENISA.

NBÚ na príjem hlásení na národnej úrovni využíva vlastný informačný systém – Jednotný informačný systém kybernetickej bezpečnosti (JISKB), dostupný na adrese <https://jiskb.nbu.gov.sk/>. Výrobcovia preto pri podávaní hlásení podľa článku 14 CRA voči SK-CERT nepristupujú priamo do platformy SRP spravovanej agentúrou ENISA, ale využívajú JISKB, resp. jeho verejné nahlasovacie formuláre:

- subjekty, ktoré majú do JISKB pridelený prístup (napr. prevádzkovatelia základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti), podávajú hlásenie priamo cez JISKB;
- ostatné nahlasujúce subjekty, ktoré prístup do JISKB pridelený nemajú, využijú verejný formulár „Nahlásenie incidentu“ na adrese <https://jiskb.nbu.gov.sk/public-report/incident>. SK-CERT tento kanál výslovne označuje ako určený aj na nahlasovanie závažného incidentu podľa CRA.

SK-CERT ako koordinujúci CSIRT následne zabezpečuje, aby sa relevantné informácie z takto prijatého hlásenia dostali k agentúre ENISA a prípadne ďalším dotknutým národným CSIRT v súlade s požiadavkami CRA. Výrobca, ktorý nahlasuje prostredníctvom JISKB, sa teda sám do platformy SRP neprihlasuje, ani si na nej nezakladá samostatný účet.

Čo robiť, ak JISKB nie je dostupný

Zaslanie e-mailu SK-CERT samo osebe nepredstavuje formálne hlásenie podľa článku 14 CRA.

Ak JISKB nie je výnimočne dostupný, možno aktívne zneužívanú zraniteľnosť alebo závažný incident v krajnom prípade nahlásiť e-mailom na adresu incident@nbn.gov.sk, pričom SK-CERT odporúča využiť šifrovanie PGP (SK-CERT PGP Key ID: 0xCF7496BD1A1A0ACD; odtlačok kľúča: D66E 619A E83A 8802 51A6 5AC7 CF74 96BD 1A1A 0ACD). Aktuálny PGP kľúč je na stiahnutie na webe sk-cert.sk.

Hneď ako je JISKB opäť dostupný, je potrebné formálne hlásenie (včasné varovanie aj podrobné hlásenie) podať aj cez tento systém, aby bola splnená zákonná nahlasovacia povinnosť – len hlásenie podané cez JISKB sa považuje za splnenie zákonnej povinnosti nahlásiť aktívne zneužívanú zraniteľnosť a závažný incident.

Legacy produkty (legacy products)

Produkty s digitálnymi prvkami uvedené na trh pred 11. decembrom 2027 sú spravidla oslobodené od požiadaviek CRA na návrh produktu, nie však od nahlasovacích povinností. Ak sú takéto produkty aktuálne dostupné na trhu EÚ, patria – bez ohľadu na to, kedy boli prvýkrát uvedené na trh alebo vyrobené – na účely hlásenia do pôsobnosti CRA.

Nahlasovacia povinnosť sa pritom vzťahuje len na novozistené aktívne zneužívané zraniteľnosti a závažné incidenty. Výrobcovia nemusia hlásiť aktívne zneužívané zraniteľnosti a závažné incidenty, o ktorých sa dozvedeli už pred 11. septembrom 2026.

Ďalšie informácie a často kladené otázky

Európska komisia vedie prehľad často kladených otázok, ktorý sa venuje zložitejším otázkam implementácie CRA, vrátane technických scenárov a regulačného výkladu.

Doplňujúce praktické usmernenie pre výrobcov, vývojárov a podniky všetkých veľkostí k plneniu povinností podľa CRA poskytuje aj priebežne aktualizovaná metodická podpora Európskej komisie k implementácii CRA.

K otázkam týkajúcim sa platformy SRP a hlásenia jej prostredníctvom vedie agentúra ENISA vlastný prehľad často kladených otázok.

Priebežne aktualizované informácie o CRA v prostredí Slovenskej republiky, vrátane metodických usmernení NBÚ, nájdete na webovej stránke cra.nbn.gov.sk. Aktuálne kontaktné údaje na SK-CERT sú uvedené na sk-cert.sk (sekcia O nás – Kontakty).

NBÚ neposkytuje súčinnosť pri určovaní rozsahu pôsobnosti konkrétneho produktu ani všeobecné regulačné posúdenie.

Nahlasovacia povinnosť opísaná v tomto dokumente predstavuje len jednu z povinností stanovených článkom 14 CRA. Výrobcovia sú povinní vykonať vlastné zodpovedajúce právne a technické posúdenie, aby zabezpečili súlad so všetkými požiadavkami CRA a súvisiacich predpisov.

