27. 8. 2026

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Cyber Resilience Act: od září 2026 budete muset hlásit incidenty i zranitelnosti. Jste na to připraveni?

Chytré hodinky, domácí router, mobilní aplikace, dětská chůvička, bezpečnostní kamera nebo software ve výrobní lince. Všechny tyto produkty mají jedno společné: pracují s digitálními prvky a mohou se stát vstupní branou pro kybernetický útok. Právě proto budou jejich výrobci, dovozci a distributoři nově povinni plnit konkrétní povinnosti dle nového nařízení Cyber Resilience Act („CRA“). CRA je už platné, ale jednotlivé povinnosti z něj nastupují postupně. A jedna z prvních povinností, hlášení incidentů a zranitelností, začíná platit už za necelý měsíc, od 11. září 2026.

Koho se CRA týká?

CRA dopadá především na **výrobce, dovozce a distributory** produktů s digitálními prvky, které jsou uváděny na trh EU. Nezáleží přitom nutně na tom, zda společnost sídlí v EU. Rozhodující je, zda se její produkt dostává na evropský trh.

Co vše se podle CRA rozumí produktem a na co dopadá?

Produktem s digitálním prvkem jsou typicky chytrá zařízení, síťové prvky, bezpečnostní kamery, nositelná elektronika nebo senzory. „**Produktem s digitálními prvky**“ ale není jen hardware. **CRA pod tento pojem zahrnuje i software.** Nařízení tedy dopadá i na operační systémy, mobilní aplikace, firmware nebo samostatný software ke stažení.

CRA ale zdaleka neplatí pro veškerý software, aplikace nebo zdrojový kód:

- **Webové aplikace, progresivní webové aplikace nebo i webové stránky**, které jsou přístupné pouze skrze webový prohlížeč, typicky nebudou CRA podléhat. Výjimkou jsou případy, kdy webová stránka podporuje funkcionalitu produktu s digitálními prvky (např. pokud je provoz digitálního produktu možný pouze po získání tokenu nebo přihlašovacích údajů z webového autentifikačního portálu).
- **SaaS řešení třetích stran** zakomponovaná do produktu s digitálními elementy budou považována za součást produktu s digitálními vlastnostmi. Pokud ale budou do produktu integrovány způsobem, který ovlivňuje jeho bezpečnost, měla by tato řešení být ošetřena podobně jako komponenty 3. stran.
- **Free and open-source software** nespadá pod CRA, pokud není monetizován (např. účtováním ceny, monetizací jiných služeb či zpracováním osobních údajů).

Podobně ani každý elektronický výrobek automaticky nespadá pod CRA. Do působnosti nařízení se produkt dostane jen, pokud má přímé či nepřímé datové připojení k jinému zařízení nebo síti. Rozhodující tedy je, zda produkt zpracovává, ukládá nebo přenáší digitální data a zda má relevantní datové propojení. Mimo působnost nařízení tak zůstanou zařízení, která pouze lokálně vykonávají jednoduchou funkci a nepřenášejí žádná digitální data. Typickým příkladem je jednoduchá elektronická hračka, která pouze přehrává předem uložené zvuky a nemá žádné datové

připojení, nebo myčka nádobí s vestavěným firmwarem řídícím mycí cykly, avšak bez možnosti připojení k jiným zařízením nebo sítím.

CRA se dále nevztahuje na produkty již pokryté zvláštní sektorovou legislativou (vybrané zdravotnické prostředky, motorová vozidla, některé výrobky v civilním letectví) ani na produkty vyvíjené výhradně pro obranu či národní bezpečnost.

Co CRA v praxi mění?

Největší změna spočívá v tom, že kybernetická bezpečnost se stane součástí základních požadavků na produkt. Výrobce nebude moci produkt jednoduše uvést na trh a řešit zranitelnosti až dodatečně. Už před uvedením na trh bude muset posoudit kybernetická rizika, zohlednit je při návrhu a vývoji produktu, připravit technickou dokumentaci a zajistit, že produkt splňuje příslušné bezpečnostní požadavky.

V praxi to znamená například, že domácí router by neměl být dodáván s univerzálním heslem typu „admin/admin“, bezpečnostní kamera by měla umožňovat bezpečné aktualizace, mobilní aplikace by neměla zpracovávat více dat než skutečně potřebuje, a výrobce průmyslového zařízení by měl vědět, jaké softwarové komponenty ve svém produktu používá.

Co začíná platit už 11. září 2026?

Většina požadavků CRA čeká společnosti až od 11. prosince 2027. Reportovací povinnosti ale nastupují s předstihem a týkají se i produktů, které jsou na trhu už dnes. Od **11. září 2026** budou výrobci muset hlásit:

- aktivně zneužívané zranitelnosti – tedy ty, u nichž existuje důkaz, že byly aktivně zneužity, a
- závažné incidenty s dopadem na bezpečnost produktu.

V praxi může jít například o situaci, kdy výrobce zjistí, že útočníci aktivně zneužívají chybu ve firmwaru routeru nebo že zranitelnost v aplikaci umožňuje neoprávněný přístup k účtům uživatelů. Naopak zranitelnost zjištěná například při etickém testování bez důkazu o zneužití může být oznámena dobrovolně, ale sama o sobě nemusí spadat pod povinné hlášení.

Oznámení bude probíhat ve velmi krátkých lhůtách:

Krok	Lhůta
Včasné varování	24 hodin
Oznámení o zranitelnosti / incidentu	72 hodin
Závěrečná zpráva	14 dní (zranitelnost) / 1 měsíc (incident)

Povinnost provést hlášení se vždy váže k okamžiku, kdy se **výrobce o zranitelnosti nebo incidentu dozví** – lhůty běží od tohoto okamžiku, nikoli od vzniku samotné zranitelnosti či incidentu. CRA přitom nestanoví, jakým způsobem se má výrobce o problému dozvědět, ani mu neukládá povinnost aktivně monitorovat konkrétní zdroje informací.

V praxi se tak může výrobce o incidentu nebo zranitelnosti dozvědět například od zákazníka, který nahlásí neobvyklé chování produktu, z reportu kyberbezpečnostní organizace popisující zneužité

zranitelnosti, z upozornění od úřadu NÚKIB, od etických hackerů nebo prostřednictvím interního monitoringu.

Komu a jak hlášení provést?

Výrobce bude oznámení podávat prostřednictvím **jednotné platformy pro podávání zpráv**, kterou má podle nařízení zřídit agentura ENISA (Evropská agentura pro bezpečnost sítí a informací). Skrze platformu bude oznámení podáno souběžně dvěma adresátům: národnímu CSIRT[1] týmu a agentuře ENISA. Systém je tedy navržen tak, aby výrobce podal jedno oznámení a to bylo distribuováno všem relevantním orgánům v EU, kde je dotčený produkt dostupný.

Příslušný koordinátor, tedy CSIRT tým, kterému výrobce prostřednictvím platformy hlásí, se určí podle hlavní provozovny výrobce. Podle nařízení se hlavní provozovna nachází tam, kde **výrobce nejčastěji rozhoduje o kybernetické bezpečnosti svých produktů**; nelze-li provozovnu takto určit, rozhoduje počet zaměstnanců. Pokud výrobce v EU provozovnu vůbec nemá, uplatní se náhradní kritéria dle místa působení zplnomocněného zástupce, usazení dovozce, distributora či největšího počtu uživatelů.

CSIRT tým a ENISA však nejsou jedinými adresáty, které bude muset výrobce o problému informovat. Jakmile se výrobce o aktivně zneužívané zranitelnosti nebo závažném incidentu dozví, musí o tom **informovat i zasažené uživatele produktu** (případně dokonce všechny uživatele). Uživatelům musí současně doporučit opatření, která mohou přijmout ke zmírnění dopadu. Pokud výrobce uživatele neinformuje, mohou tuto informaci poskytnout přímo příslušné CSIRT týmy, považují-li to za nezbytné ke zmírnění rizika.

Co když je původ zranitelnosti v komponentě třetí strany?

Produkty s digitálními prvky se často skládají z řady komponent, softwarových knihoven nebo modulů, které nevyrábí sám výrobce finálního produktu. Pokud se aktivně zneužívaná zranitelnost nachází v takové integrované komponentě, **hlásit ji musí výrobce finálního produktu, bez ohledu na to, že chybu sám nezpůsobil**. Je-li daná komponenta na trh dodávána i samostatně, vztahuje se ohlašovací povinnost i na výrobce této komponenty.

Stále ale platí, že ohlašovací povinnost vzniká, jen když je zranitelnost v konkrétním produktu skutečně zneužívaná. Pokud výrobce ví o zranitelnosti v komponentě, ale ta se v jeho produktu prakticky zneužít nedá, nejde o aktivně zneužívanou zranitelnost ve smyslu CRA a povinné hlášení se neuplatní (lze ji ale nahlásit dobrovolně). Výrobce je nicméně vždy povinen o zjištěné zranitelnosti informovat toho, kdo danou komponentu vyrábí nebo udržuje, aby ji mohl opravit.

Proč CRA nepodcenit?

Nesplnění požadavků může znamenat nejen regulatorní riziko, ale i omezení prodeje produktu, který nesplňuje požadavky CRA. Při neplnění **reportingových povinností se výrobce vystavuje riziku pokuty** až 15 milionů eur nebo 2,5 % celosvětového ročního obratu podniku podle toho, která částka je vyšší.

Co je tedy potřeba mít do září hotové?

- **Revidovat nebo vytvořit politiky hlášení** tak, aby pokryly nové povinnosti.
- **Nastavit eskalační matici povinností**, aby byla každá informace o potenciálním incidentu nebo zranitelnosti řádně zpracována, bylo jasné, kdo incidenty a zranitelnosti vyhodnocuje,

schvaluje jejich kvalifikaci, kdo komunikuje s úřady a uživateli a kdo připravuje technická řešení.
- **Zmapovat portfolio produktů** a určit, které z nich jsou „produktem s digitálními prvky“.
- **Projít smluvní vztahy s dodavateli** a určit, kdo je povinen informovat koho, pokud se zranitelnost objeví v dodavatelském řetězci.

Mgr. Bc. Lenka Michalcová,
advokátka

Mgr. Kateřina Tesařová,
koncipientka

PricewaterhouseCoopers Legal s.r.o., advokátní kancelář
PwC Legal

City Green Court
Hvězdova 1734/2c
140 00 Praha 4

Tel.: +420 251 151 111
Fax: +420 251 156 111

Svobody 91/20
602 00 Brno

Tel.: +420 542 520 111
Fax: +420 542 214 796

e-mail: info@pwc.cz

---

[1] Tým pro reakce na počítačové bezpečnostní incidenty.

Další články:

- Výklad některých otázek týkajících se valných hromad obchodních korporací ve světle aktuální judikatury
- Ban, omezení zpeněžení či zablokování účtu? Jaká máte práva vůči platformě? Ochrana streamerů a dalších tvůrců ve světle DSA
- Povaha sjezdů

- Zaplatit za logo nestačí. Jaká práva skutečně získáváte?
- Výslech advokáta účastníka řízení coby důkazní prostředek
- Rozhodnutí Nejvyššího soudu ke změně klíče pro stanovení příspěvků na správu domu a pozemku, k samotnému stanovení příspěvků a k rozúčtování nákladů na služby
- Byznys a paragrafy, díl 41.: Záruka za jakost v kupní smlouvě
- Dvacet let vlastní cestou. Arthur Braun o svobodě, číslech a lidském elementu advokacie
- Komu náleží vlastnické právo k náhradní veřejné komunikaci postavené investorem?
- AML rizika u luxusních nákupů
- Recentní judikatura Nejvyššího soudu k důvodům neplatnosti usnesení valné hromady