11. 9. 2026

ID: 121615

Firmy čekají na rok 2027, první povinnosti podle CRA ale přichází už teď v září. Dopadají i na produkty, které už jsou na trhu

Evropské nařízení o kybernetické odolnosti (CRA) nabývá plné účinnosti až v prosinci 2027, jeho část však začíná platit už 11. září 2026. Od tohoto data musí výrobci softwaru i hardwaru, který se připojuje k síti, hlásit do 24 hodin aktivně zneužívané zranitelnosti a závažné incidenty. Podle odborníků z advokátní kanceláře ROWAN LEGAL se tato povinnost vztahuje i na produkty uvedené na trh v minulosti a firmy ji musí plnit bez ohledu na to, v jaké fázi schvalování je navazující český zákon.

Evropské nařízení o požadavcích na kybernetickou bezpečnost produktů s digitálními prvky (Cyber Resilience Act, CRA) vstoupilo v platnost v prosinci 2024. Jeho hlavní část začne platit až v prosinci 2027, ale povinnost hlásit zranitelnosti a bezpečnostní incidenty přichází už 11. září 2026. Řada firem přitom o nařízení zatím ani neví.

„Pokud firmy o CRA vůbec ví, často vnímají jako podstatný termín prosinec 2027. Povinnosti účinné od 11. září 2026 jsou přitom také podstatné a vyžadují nastavení procesů. Bez nastaveného procesu, určených odpovědností a vyzkoušeného přístupu do systému, přes který se zranitelnosti a incidenty ohlašují se lhůta 24 hodin pro prvotní hlášení dá těžko dodržet,“ říká **Jan Tomíšek, partner ROWAN LEGAL a odborník na IT právo**.

Jan Tomíšek

Podle průzkumu OpenSSF a Linux Foundation z června 2026 CRA nezná 66 % dotázaných. Agentura EU pro kybernetickou bezpečnost ENISA zároveň řadí zvládání bezpečnostních incidentů mezi slabší schopnosti malých a středních podniků.

Často přehlížený je také časový záběr nařízení. Většina požadavků CRA se na produkty uvedené na trh před 11. prosincem 2027 nevztahuje (resp. vztahuje se na ně pouze tehdy, pokud projdou podstatnou změnou). Povinnost hlášení je ale výjimkou a dopadá i na produkty, které jsou již na trhu, pokud spadají do působnosti nařízení. *„Právě to manažery často překvapuje nejvíc. Nestačí zavést nový proces pro produkty, které teprve vzniknou. Firma musí vědět, co všechno má v tuto chvíli na evropském trhu, jak zjistí zneužívané zranitelnosti těchto produktů a jak je bude komunikovat úřadům, případně zákazníkům,“* doplňuje **Michaela Holíková, associate ROWAN LEGAL a odbornice na IT právo**.

Michaela Holíková

Výrobcem podle CRA není jen ten, kdo produkt přímo vyvinul. Je jím i firma, která pod svou značkou nabízí software vyvinutý na zakázku někým jiným. CRA se tak netýká jen technologických společností, ale například i bank, pojišťoven nebo výrobců, kteří dodávají chytrá zařízení s přidruženou aplikací.

Samotné hlášení není omezené na jednu čtyřiadvacetihodinovou lhůtu. Do 24 hodin od chvíle, kdy se výrobce o aktivně zneužívané zranitelnosti nebo závažném incidentu dozví, musí odeslat první oznámení. Do 72 hodin následuje podrobnější oznámení a u zranitelností poté závěrečná zpráva do 14 dnů od dostupnosti nápravného opatření; u závažných incidentů do jednoho měsíce. Hlášení probíhá prostřednictvím centrální platformy provozované agenturou ENISA. Pokud náprava vyžaduje součinnost uživatelů, musí je výrobce bez zbytečného odkladu informovat o zranitelnosti či incidentu a o nápravných opatřeních, které může uživatel podniknout.

Za porušení těchto povinností mohou hrozit pokuty až 10 milionů eur nebo 2 % celosvětového ročního obratu, v Česku je však zatím nemá kdo vymáhat. Dozor nad plněním CRA v Česku má upravit samostatný zákon o požadavcích na kybernetickou bezpečnost výrobků s digitálními prvky, který připravilo Ministerstvo průmyslu a obchodu. Ten je momentálně v meziresortním připomínkovém řízení. To však neznamená, že by se povinnost hlášení jakkoli odkládala.

„Evropská povinnost hlásit zranitelnosti a incidenty začne platit 11. září bez ohledu na to, v jaké fázi bude český zákon. Přestože za její porušení aktuálně nehrozí pokuty, pořád je zde riziko povinnosti k náhradě škody, např. pokud firma řádně neinformuje své zákazníky o zranitelnosti, kterou pak útočník aktivně zneužije,“ uzavírá **Jan Tomíšek**. Firmy by si proto měly co nejdříve zmapovat produkty s digitálními prvky, které mají na trhu EU, určit odpovědné osoby a jejich zastupitelnost a ověřit si přístup do systému pro hlášení. Stejně důležité je nastavit, jak se budou o zranitelnostech dozvídat od zákazníků, bezpečnostních výzkumníků nebo dodavatelů a jak budou v případě potřeby komunikovat se zákazníky.

Další články:

- JUDr. Aneta Průšová, Ph.D., posiluje pražský tým CEE Attorneys na pozici Senior Associate
- EET 2.0 je na světě: od ledna 2027 budou podnikatelé evidovat i platby kartou a QR kódem
- Co dělat, když do firmy přijde policie nebo AI způsobí škodu? Advokátní kancelář Chrenek, Toman, Kotrba spouští praktický právní institut
- Firmy čekají na rok 2027, první povinnosti podle CRA ale přichází už teď v září. Dopadají i na produkty, které už jsou na trhu
- Karin Pomaizlová posiluje IP tým Brichta & Partners jako Senior Counsel

- Aliance Horizons rozšiřuje svoji působnost do Slovinska a Bosny a Hercegoviny
- Heureka v přelomovém sporu s Googlem vysoudila před prvostupňovým soudem přes 400 milionů korun. Zastupovala ji advokátní kancelář ROWAN LEGAL
- V prvním pololetí zaznamenala skupina HAVEL & PARTNERS tržby 815 milionů korun
- Změny v AML legislativě: co přinese nová evropská a česká úprava
- JUDr. Lucia Šoralová posílila tým bpv BRAUN PARTNERS
- Katrin Vydržel novou advokátkou Aegis Law