Oznamování incidentů podle CRA: rychlý průvodce

Pro výrobce produktů s digitálními prvky · orientační otázky, lhůty a první kroky

Nejprve ověřte působnost

Pokud vyrábíte produkt s digitálními prvky a uvádíte jej na trh EU, mohou určité události vyvolat oznamovací povinnosti podle článku 14 CRA. Tento průvodce pomáhá připravit tým na reakci. Zda se CRA vztahuje na váš produkt a roli, je nutné posoudit podle konkrétních okolností.

Může se oznamovací postup vztahovat i na vás?

Ověřte svou roli výrobce, zda má produkt digitální prvky a zda je uváděn na trh EU. Tento průvodce se týká oznamovacích povinností výrobců podle článku 14; nenahrazuje úplné posouzení působnosti CRA.

Které události mohou podléhat oznámení?

Aktivně zneužívaná zranitelnost Zranitelnost je skutečně zneužívána při útoku a ovlivňuje bezpečnost produktu s digitálními prvky. Ne každá nově zjištěná zranitelnost splňuje tuto podmínku.	Závažný bezpečnostní incident Závažný incident má dopad na bezpečnost produktu s digitálními prvky. Ne každý IT incident ve firmě automaticky podléhá oznamovací povinnosti podle CRA.

Lhůty začínají běžet okamžikem, kdy se výrobce o oznamované události dozví.

24 hodin	72 hodin	Závěrečná zpráva
Včasné varování co nejdříve, nejpozději do 24 hodin.	Oznámení s dalšími informacemi a prvotním posouzením, nejpozději do 72 hodin.	Zranitelnost: nejpozději do 14 dnů po zpřístupnění nápravného opatření. Závažný incident: do jednoho měsíce od oznámení ve lhůtě 72 hodin.

Kam výrobci podávají oznámení?

Výrobci podávají jedno oznámení prostřednictvím platformy CRA Single Reporting Platform (SRP). Oznámení je určeno týmu CSIRT v zemi hlavního sídla výrobce; informace se zpravidla zpřístupní také agentuře ENISA. Přijímající tým CSIRT je sdílí s dotčenými týmy CSIRT v dalších členských státech.

Připravte se před incidentem

Malá, jasně definovaná sada podkladů ušetří v první hodině cenný čas:

• Určete vedoucího incidentu a jeho zástupce; stanovte, jak je zastihnout mimo pracovní dobu.	• Udržujte aktuální přehled produktů, variant, verzí softwaru a trhů EU.
• Zaveďte interní kanál pro bezpečnostní zjištění a hlášení incidentů.	• Seznamte kontakty na bezpečnost produktů, vývoj, právo/compliance a komunikaci.
• Připravte společný záznam událostí pro časové údaje, rozhodnutí a odpovědné osoby.	• Předem dohodněte postup omezení dopadu, nápravy a komunikace aktualizace.

První kroky při události

Rychle zorganizujte reakci, uchovejte důkazy a aktivně sledujte lhůty.

Prvních 60 minut

01	Zaznamenejte, kdy se organizace o události dozvěděla: datum, čas, časové pásmo, zdroj a první příjemce informace.
02	Aktivujte základní tým a určete jednu osobu odpovědnou za oznamování.
03	Proveďte prvotní klasifikaci: aktivně zneužívaná zranitelnost, závažný incident, nebo zatím nejasná situace. Pokud si nejste jisti, bez prodlení věc eskalujte.
04	Zaznamenejte produkt, dotčené verze, možný dopad, známky útoku a dosud provedené kroky. Uchovejte důkazy.
05	Zapište lhůty 24 a 72 hodin do kalendáře; připravte oznámení v SRP a stanovte odpovědnost za následnou závěrečnou zprávu.

Rychlý záznam incidentu

Číslo případu _____	Produkt / dotčené verze _____
První zjištění (datum, čas, pásmo) _____	Předpokládaný typ události _____
Odpovědná osoba / zástupce _____	Dotčené trhy / zákazníci _____
Známý dopad a dostupné důkazy _____	Okamžité opatření / další aktualizace _____

Působnost a omezení

Oznamovací povinnosti podle článku 14 CRA se od 11. září 2026 vztahují na výrobce v působnosti nařízení. Konkrétní posouzení závisí na produktu, roli, události a použitelných výjimkách. Tento bezplatný praktický průvodce poskytuje obecné informace; nejde o právní poradenství ani úplný postup pro soulad s předpisy nebo reakci na incident. Oznámení nepodává a nezaručuje soulad.

Zdroj: nařízení (EU) 2024/2847, článek 14. Ověřte aktuální právní stav a konkrétní okolnosti svého případu.