TISKOVÁ ZPRÁVA

Výrobci softwaru, aplikací i chytrých zařízení mají nově jen 24 hodin na nahlášení útoku

Praha, 23. září 2026 – Od 11. září se začala uplatňovat jedna z prvních praktických povinností evropského nařízení Cyber Resilience Act (CRA). Výrobci softwaru, aplikací i chytrých zařízení musí do 24 hodin podat prvotní oznámení o aktivně zneužívaných zranitelnostech a závažných incidentech majících dopad na bezpečnost produktu, jakmile se o nich dozvědí. Ačkoliv většina požadavků nařízení se na firmy plně uplatní až v prosinci 2027, první ostrý test přišel právě teď, upozorňuje Tomáš Kubíček, partner BDO a vedoucí týmu kybernetické bezpečnosti.

Cyber Resilience Act (CRA) je evropské nařízení, které nastavuje bezpečnostní požadavky pro takřka všechny produkty s digitálními prvky, od mobilních aplikací přes routery až po průmyslová IoT zařízení. Naprostá většina jeho požadavků, jako je bezpečný vývoj produktu nebo dokumentace zranitelností, začne platit až 11. prosince 2027. Oznamovací povinnosti podle CRA se však uplatňují už od 11. září 2026.

Do 24 hodin musí výrobce podat první varování o aktivně zneužívané zranitelnosti nebo závažném incidentu. U incidentu zároveň uvede, zda má podezření, že byl způsoben protiprávním nebo škodlivým jednáním. Do 72 hodin následuje podrobnější oznámení s popisem zranitelnosti či incidentu, prvotním posouzením a přijatými nápravnými nebo zmírňujícími opatřeními. U aktivně zneužívané zranitelnosti musí být závěrečná zpráva podána nejpozději do 14 dnů od chvíle, kdy je k dispozici nápravné nebo zmírňující opatření. U závažného incidentu se závěrečná zpráva podává do jednoho měsíce od podání 72hodinového oznámení.

„Ne každá nově objevená chyba znamená povinnost hlášení,“ říká Tomáš Kubíček z BDO. *„CRA za aktivně zneužívanou zranitelnost považuje jen takovou, u které existují spolehlivé důkazy, že ji útočník skutečně využil bez souhlasu vlastníka systému. Přesto jde o povinnost, kterou firmy nesmí podcenit, protože lhůty jsou extrémně krátké a týkají se i produktů, které už dávno prodávají.“*

Systém pro hlášení se skládal na poslední chvíli

Praxe posledních týdnů ukazuje, že ani na evropské úrovni to nebylo hladké. *„Jednotnou platformu pro hlášení, kterou pro CRA zřizuje agentura ENISA, měly firmy k dispozici až v samotný den, kdy povinnost začala platit,“* upozorňuje Tomáš Kubíček. Seznam národních CSIRT týmů, které mají hlášení jako koordinátoři přijímat, ENISA zveřejnila krátce před spuštěním nové povinnosti.

Platforma navíc ve své první verzi neumožňuje automatizované odesílání hlášení přímo z firemních systémů, takže je firmy musí zadávat ručně prostřednictvím webového formuláře. Její rozhraní je zatím pouze v angličtině a dobrovolná hlášení podle článku 15 budou dostupná až v další fázi.

V Česku je jako koordinátor pro hlášení podle CRA určen Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), tedy stejný úřad, který od loňského listopadu dohlíží i na nový zákon o

kybernetické bezpečnosti. Ten transponoval evropskou směrnici NIS2 a nově pod regulaci dostal řádově tisíce dalších českých organizací, podle NÚKIB do února 2026 ohlásilo regulovanou službu přes 4 800 subjektů. Povinnosti podle CRA se tak pro mnohé podniky přidávají k pravidlům, která si teprve začínají osvojovat.

Povinnost se týká i produktů, které jsou na trhu roky

Firmy podle Tomáše Kubíčka často mylně předpokládají, že se oznamovací povinnost týká jen nových produktů. Podle nařízení se ale vztahuje i na produkty s digitálními prvky, které byly na unijní trh uvedeny před plnou použitelností CRA. *„Firmy by si měly udělat pořádek v tom, co všechno v jejich portfoliu spadá pod definici produktu s digitálními prvky, včetně mobilních aplikací, cloudových služeb nebo autentizačních systémů, které k produktu patří,“* dodává.

Regulace zároveň počítá s citelnými sankcemi. Za porušení některých klíčových povinností, včetně oznamovacích povinností, může firmám hrozit pokuta až 15 milionů eur nebo 2,5 procenta celosvětového obratu za předchozí finanční rok, podle toho, která částka je vyšší, byť plné vymáhání této sazby se má rozběhnout až s koncem roku 2027.

Firmy musí mít předem jasno, kdo o hlášení rozhodne

Dvacet čtyři hodin je podle Tomáše Kubíčka doba, ve které se nedá improvizovat. *„Firmy by měly mít nastavený proces ještě předtím, než k incidentu dojde: kdo zranitelnost nebo incident jako první zaznamená, kdo posoudí jeho závažnost a kdo bude mít pravomoc hlášení odeslat. Když se tyto role řeší až v okamžiku útoku, čas na samotné hlášení se tím jen zkracuje,“* vysvětluje Tomáš Kubíček z BDO.

Firmy, které chtějí být připravené, by si měly nechat zmapovat, zda a v jakém rozsahu na ně CRA dopadá, najít mezery v jejich současné připravenosti a nastavit procesy a dokumentaci tak, aby zvládly nové požadavky v běžném provozu. ENISA navíc v platformě rozlišuje primárního a sekundárního zástupce, takže firmy by měly mít předem určeny alespoň dvě osoby, které mohou hlášení podat.

O společnosti BDO

BDO je poradenská společnost poskytující auditorské, daňové, právní, účetní, znalecké a poradenské služby. Na českém trhu působí již přes 30 let. S více než 600 odborníky a dlouholetou praxí se řadí k předním společnostem s tímto zaměřením v České republice, kde také opakovaně vyhrála titul Největší poradenská firma roku. Kanceláře má v Praze, Brně, Ostravě, Plzni, Českých Budějovicích, Pardubicích, Jindřichově Hradci a Domažlicích.

BDO je v České republice zastoupena společnostmi BDO Audit s.r.o., BDO Czech Republic s.r.o., BDO Consulting s.r.o., BDO Legal s.r.o., advokátní kancelář, BDO Valuation, s.r.o., BDO Fund Administration

TISKOVÁ ZPRÁVA

a.s., BDO Euro-Trend s.r.o. a BDO EURO-Trend Audit, a.s. Společnost je součástí mezinárodní sítě BDO, která celosvětově tvoří jednu z největších sítí auditorských a poradenských skupin. Zaměstnává více než 119 tisíc odborníků a působí ve 166 zemích, v nichž provozuje více než 1 800 kanceláří.

Kontakt:
Jan Kuliš, EPIC Public relations
E-mail: jan.kulis@epicpr.cz
Tel.: +420 731 920 874
Web: www.epicpr.cz