



Akt o kybernetické odolnosti (CRA) Deloitte Cyber Regulatory Compliance

Pro společnosti prodávající **produkty s digitálními prvky v EU** přináší nařízení CRA **nové povinnosti** týkající se řízení kybernetických rizik, detekce a řešení zranitelností, zabezpečení dodavatelského řetězce a hlášení incidentů. Týká se to široké škály produktů, včetně:



IoT
zařízení



Síťové komponenty



Cloudové služby



Specializované
průmyslové systémy

S příchodem nařízení CRA jsou podniky povinny splňovat **přísnější bezpečnostní standardy a opatření** a nedodržení těchto požadavků může vést k vážným důsledkům.

CRA je **nařízení** Evropské unie s cílem zajistit, aby **produkty s digitálními prvky** – jako je software, chytrá zařízení a připojené produkty – byly bezpečné již od návrhu a ve výchozím nastavení. Vztahuje se na **dovozce, výrobce a distributory** působící na trhu EU.

Koho se CRA týká?

- › **Výrobci softwaru a hardwaru**
- › **Dovozci a distributoři** uvádějící digitální produkty na trh EU
- › **Organizace integrující digitální produkty** do svých podnikových procesů

Rizika spojená s nedodržením CRA

- › Pokuty až do výše **15 milionů EUR** nebo **2,5 % z celosvětového ročního obratu**
- › **Stažení produktů** z trhu nebo jejich zákaz
- › **Poškození reputace** a právní odpovědnost

Základní požadavky



Security by Design

Zavádění bezpečnostních prvků v každé fázi vývoje



Řízení zranitelností

Průběžné monitorování, testování a patchování



Transparentnost

Srozumitelné pokyny pro použití, údržbu a zmírnění rizik, úplná dokumentace



Vulnerability & Incident Reporting

Oznamování zranitelností a jejich zneužití CSIRT týmům a agentuře ENISA



Conformity Assessment (posouzení shody)

Některé vysoce rizikové produkty vyžadují posouzení třetí stranou

Milníky

Září 2026 – Začínají platit požadavky na hlášení zranitelností a incidentů

Prosinec 2027 – Plná implementace CRA, všechny produkty musí splňovat požadavky

S ohledem na tyto termíny je nezbytné začít s přípravou co nejdříve, aby bylo možné **zavést příslušné procesy a potřebná bezpečnostní opatření**.

Náš tým odborníků na **kybernetickou bezpečnost, dodržování předpisů, právo a řízení rizik** vám pomůže splnit všechny požadavky nařízení CRA.



Analýza produktového portfolia

Posoudíme vaše produktové portfolio s cílem identifikovat produkty regulované CRA



Posouzení shody a dokumentace

Podpoříme vás při zpracování technické dokumentace a přípravě na posouzení shody (conformity assessment)



Připravenost na CRA & gap analýza

Porovnáme současný stav ve vaší společnosti s požadavky nařízení CRA



Řízení zranitelností a aktualizací

Pomůžeme vám efektivně spravovat bezpečnostní aktualizace a oznamování zranitelností



Nápravná opatření

Navrheme jasné a prioritizované kroky k odstranění nedostatků



Bezpečnost dodavatelského řetězce a třetích stran

Posoudíme a zavedeme bezpečnostní standardy napříč vašimi dodavateli a partnery



Podpora při implementaci

Provedeme vás aplikací principů bezpečnosti již od návrhu a ve výchozím nastavení (security by design, security by default)



Odborné poradenství & metodologie

Poskytneme průběžnou odbornou podporu během celého procesu zajištění souladu s nařízením CRA

Kontaktujte nás

Jakub Höll, Director
jholl@deloittece.com



Marek Fišer, Manager
mfisher@deloittece.com

