Cybrela

Cyber Resilience Act

Bezpečnost produktu přestává být obchodním rozhodnutím a stává se podmínkou pro jeho prodej v EU. E-book pro výrobce, dovozce a distributory produktů s digitálními prvky.

NAŘÍZENÍ
(EU) 2024/2847

PLNÁ ÚČINNOST
od 11. 12. 2027

Cyber Resilience Act

Kolektiv autorů

Vydala Cybrela s.r.o.
Rybná 682/14, 110 00 Praha 1-Staré Město
+ 420 724 587 588
www.cybrela.com

Počet stran 60
1. vydání, Praha 2026
Vytiskla společnost ON tisk, s.r.o.

ISBN 978-80-11-09276-4 (pdf)
ISBN 978-80-11-09275-7 (brožováno)

OBSAH

Co v e-booku najdete

Desítky stran nařízení CRA převedených do jazyka, se kterým se dá pracovat. Od rolí a kategorií produktů přes bezpečnostní požadavky, dokumentaci a označení CE až po lhůty pro hlášení a dohled nad trhem.

E-book nenahrazuje posouzení konkrétní situace vaší organizace ani odbornou či právní konzultaci. Uvedené informace slouží pouze pro obecné informativní účely.

Nařízení CRA přináší regulaci produktů s digitálními prvky

Nařízení o kybernetické odolnosti, zkráceně CRA, je nařízení Evropského parlamentu a Rady (EU) 2024/2847. Poprvé zavádí **plošné kybernetické požadavky** na produkty s digitálními prvky, které se prodávají na evropském trhu.

CRA dopadá na **produkty s digitálními prvky**, tedy na hardware i software, který se propojuje s jiným zařízením nebo se sítí. Definice je záměrně široká a pokrývá koncová zařízení, samostatný software i komponenty dodávané na trh zvlášť.

Povinnosti **nese ten, kdo produkt uvádí nebo dodává na trh EU**. CRA rozlišuje výrobce, dovozce a distributora a každému přiřazuje jinou míru odpovědnosti. Rozhoduje přitom to, co s produktem fakticky děláte, ne jak se vaše firma označuje. Dovozce nebo distributor se stává výrobcem se všemi jeho povinnostmi ve chvíli, kdy produkt uvede na trh pod vlastní značkou nebo ho podstatně změní.

Naplno se CRA začne uplatňovat od 11. prosince 2027
Oznamovací povinnosti výrobců začínají dříve – **od 11. září 2026**. Přípravu dokumentace a procesů je rozumné začít výrazně s předstihem.

Proč byste přípravu na CRA neměli odkládat?

- **Shodu potvrzujete sami**. U většiny produktů nikdo předem nekontroluje, jestli je vaše dokumentace v pořádku. Zjistí se to až při kontrole, která může přijít kdykoli po celou dobu životního cyklu produktu.
- **Dokumentaci nelze dohnat zpětně**. Technická dokumentace popisuje návrh, vývoj a posouzení rizik. Pokud vzniká až měsíc před uvedením na trh, nepopisuje realitu a při kontrole je to znát.
- **Sankce jsou nastavené vysoko**. Za porušení základních požadavků a oznamovacích povinností hrozí pokuta až 15 mil. EUR nebo 2,5 % celosvětového ročního obratu, podle toho, která částka je vyšší.

až 15 mil. €
nejvyšší pokuta za porušení požadavků CRA

11. 9. 2026
začínají platit oznamovací povinnosti dle CRA

11. 12. 2027
plná účinnost nařízení, nečeká se na český zákon

→ Než dojde na samotné požadavky, musí si každá organizace zodpovědět dvě úvodní otázky: spadá konkrétní **produkt do působnosti CRA** a jakou **roli v dodavatelském řetězci** zastává.

01

Na koho se CRA vztahuje a v jaké roli

Nařízení má velmi širokou působnost. Nejdříve si ověřte, jestli váš produkt spadá pod CRA, jestli ho z něj nevyjímá jiný předpis a jakou máte roli. Rozsah povinností se odvíjí od toho, co s produktem reálně děláte, ne od toho, jak se označujete.

Cybrela

1.1 Co je „produkt s digitálními prvky“

Působnost CRA stojí na pojmu „produkt s digitálními prvky“. Jde o jakýkoli hardware nebo software, který se přímo nebo nepřímo, logicky nebo fyzicky propojuje s jiným zařízením nebo se sítí.

Definice je záměrně velmi široká. Pod CRA spadají **koncové produkty** jako notebooky, routery, chytré žárovky nebo chytré hračky, ale i **samostatný software** – mobilní aplikace, firmware, operační systémy. Součástí produktu jsou i řešení pro zpracování dat na dálku, bez kterých by produkt nemohl plnit některou ze svých funkcí.

Produkt s digitálními prvky
HW nebo SW, který se dokáže propojit s jiným zařízením nebo se sítí. Nezáleží na tom, jestli je propojení přímé, nebo přes něco dalšího, ani jestli je propojení logické, nebo fyzické. Rozhoduje zamýšlený účel produktu a to, jak se dá rozumně očekávat, že se bude používat.

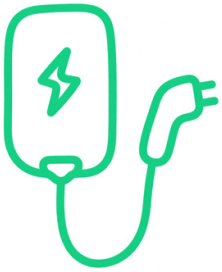
Jako produkt s digitálními prvky se posuzuje nejen hotový výrobek, ale i **komponenta dodávaná na trh samostatně**. Softwarová knihovna nebo hardwarový modul určený k zabudování do jiných systémů je podle CRA samostatný produkt s digitálními prvky. Komponenta zabudovaná do výrobku se posuzuje v rámci tohoto výrobku, komponenta prodávaná zvlášť pak stojí samostatně.

Pokud v e-booku uvádíme zkráceně „produkt“, vždy tím myslíme produkt s digitálními prvky.

1.2 Příklady produktů s digitálními prvky

CRA se netýká jen produktů, u kterých byste zabezpečení čekali. Spadá pod něj skoro všechno, co se připojí k síti nebo k jinému zařízení, od tiskárny přes chůvičku až po vlaky. Tohle je jen minimální výčet.

TISKÁRNA



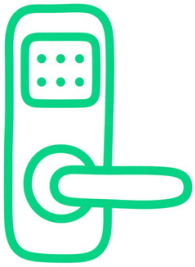
NABÍJEČKA ELEKTROMOBILU

NOTEBOOK

WI-FI ROUTER

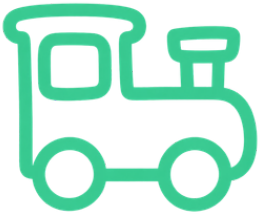
ROBOTICKÝ VYSAVAČ

CHŮVIČKA S KAMEROU



VIDEOZVONEK

CHYTRÉ HODINKY



VLAK

1.3 Produkty, u kterých se CRA nepoužije

Existují produkty, které už pokrývá jiná specifická unijní úprava. Pokud produkt spadá do některé z následujících kategorií, řídí se dál vlastní unijní úpravou, ne CRA.

- Zdravotnické prostředky – nařízení (EU) 2017/745.
- Diagnostické zdravotnické prostředky in vitro – nařízení (EU) 2017/746.
- Produkty pod nařízením (EU) 2019/2144 – schvalování typu motorových vozidel z hlediska bezpečnosti.
- Produkty certifikované podle nařízení (EU) 2018/1139 – civilní letectví.
- Námořní výstroj podle směrnice 2014/90/EU.
- Produkty, u kterých už stejná nebo některá rizika řeší jiná unijní pravidla, a to ve stejné nebo vyšší úrovni ochrany. **Kterých produktů se to bude týkat, upřesní Komise.**
- Náhradní díly dodávané na trh jako totožná náhrada komponenty a vyrobené podle stejných specifikací jako komponenta, kterou nahrazují.
- Produkty vyvinuté nebo upravené výlučně pro účely národní bezpečnosti nebo obrany a produkty speciálně určené ke zpracování utajovaných informací.

Pokud produkt do žádné z těchto kategorií nepatří a zároveň splňuje definici produktu s digitálními prvky, je velmi pravděpodobné, že **do působnosti CRA spadá**.

1.4 Tři role: výrobce, dovozce, distributor

CRA rozlišuje roli **výrobce**, **dovozce** a **distributora** produktu s digitálními prvky a každému subjektu přiřazuje jinou míru odpovědnosti. Role nezávisí na tom, jak se společnost sama označuje, ale na tom, co fakticky s produktem dělá.

Role	Popis role
Výrobce	**Vyvíjí nebo vyrábí produkt** (či si ho nechá vyrobit) a uvádí ho na trh pod svým jménem nebo ochrannou známkou. Nese hlavní tíhu povinností a odpovídá za shodu po celou dobu podpory.
Dovozce	Subjekt v EU, který **uvádí na evropský trh produkt** od výrobce mimo EU. Ověřuje, že výrobce splnil své povinnosti, než produkt uvede na trh.
Distributor	**Dodává produkt na trh, aniž by byl výrobcem či dovozcem**. Typicky je to velkoobchod nebo e-shop. Ověřuje náležitosti produktu a splnění povinností dovozce a výrobce.

Pozor na změnu role. Dovozce i distributor se stávají výrobcem (a přebírají jeho povinnosti), pokud produkt uvádějí pod vlastní značkou nebo provedou podstatnou změnu, která ovlivní soulad s CRA nebo změní zamýšlený účel produktu. Běžná údržba či drobná aktualizace podstatnou změnou není.

1.5 Jak roli poznat a pozor na výjimky

Kdo produkt s digitálními prvky vyvíjí nebo vyrábí, je výrobce. Kdo dováží na trh produkt od výrobce mimo EU, je dovozce. Kdo produkt jen zpřístupňuje dál, aniž by měnil jeho vlastnosti, je distributor. I tady ale platí výjimky. Dovozce nebo distributor se mohou stát výrobcem a přebrat stejné povinnosti ve dvou situacích.

- **Uvedou produkt na trh pod vlastním jménem nebo ochrannou známkou** (například: internetový obchod prodává router vyrobený jinou společností pod svou vlastní značkou).
- **Provedou u produktu podstatnou změnu a změněný produkt dodají na trh.**

Podstatná změna je taková změna produktu po jeho uvedení na trh, která **ovlivní soulad s požadavky CRA** nebo vede ke změně účelu, pro který byl produkt vyroben. Běžná údržba, oprava nebo drobná aktualizace, která nemění zamýšlený účel ani úroveň rizika, podstatnou změnou zpravidla není.

Uvádíte produkt pod vlastním jménem nebo provádíte podstatnou změnu?	Výrobce
Dovážíte na unijní trh produkt od výrobce mimo EU?	Dovozce
Distribuujete hotový, **nezměněný** produkt dál?	Distributor

1.6 Jak ověřit, jestli spadáte pod CRA

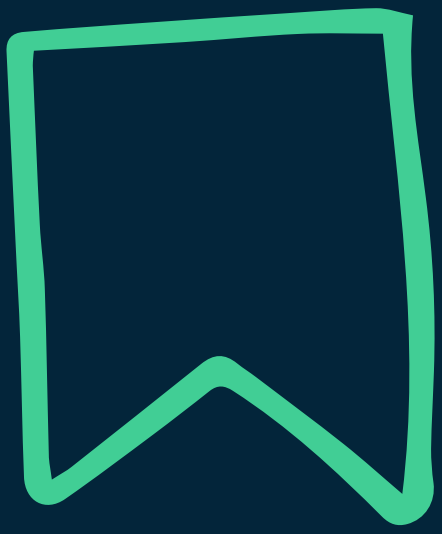
Pro ověření, jestli se vás nařízení CRA týká, si zodpovězte tři základní otázky, které nejdříve posoudí aplikovatelnost a pak vaši roli.

1. **Má váš produkt digitální prvek?**
   Vyrábíte, dovážíte nebo distribuujete HW či SW, který se přímo či nepřímo propojuje s jiným zařízením nebo sítí? Může jít i o komponentu jiného produktu uváděnou na trh samostatně.

2. **Vztahuje se na produkt jiná unijní úprava?**
   Pokud se na produkt s digitálními prvky vztahuje jiná úprava vyjímající ho z působnosti CRA (viz kapitola 1.3), uplatňuje se specifická právní úprava. Pokud ne, řídí se CRA.

3. **Jakou máte ve vztahu k produktu roli?**
   Podle toho, co s produktem reálně děláte, jste výrobce, dovozce nebo distributor a tomu odpovídá rozsah vašich povinností.

Pro ověření dopadu CRA a určení své role se neptejte „co jsme zač“, ale „co s produktem reálně děláme“. Roli posuzujte pro každý produkt a každou obchodní praktiku zvlášť.



Shrnutí kapitoly

- **CRA dopadá na produkty s digitálními prvky** – hardware i software, který se propojuje s jiným zařízením nebo se sítí.
- Definice je široká záměrně, ale **některé produkty vyjímá jiná unijní úprava**. Ověřte si to dřív, než začnete řešit požadavky.
- **Role (výrobce / dovozce / distributor) určuje rozsah povinností** a plyne z toho, co s produktem reálně děláte, ne z názvu nebo typu společnosti.
- Uvedení produktu pod vlastní značkou nebo podstatná změna produktu vás mohou z dovozce nebo distributora **změnit na výrobce produktu**.

02

Klasifikace produktu a postup posuzování shody

Základní požadavky na kybernetickou bezpečnost platí pro všechny produkty stejně. Kategorie rozhodují o tom, jak náročné bude splnění požadavků CRA prokázat: jestli si vystačíte sami, nebo budete muset zapojit třetí stranu. Zhruba 90 % produktů patří do nejmírnější kategorie.

2.1 Kategorie produktů

CRA rozděluje produkty s digitálními prvky do čtyř kategorií podle **kybernetického rizika a významu funkce**, kterou produkt plní.

Kategorie	Příklady produktů
Důležité produkty třídy I čl. 7 a příloha III CRA	Správci hesel, internetové prohlížeče, VPN, antivirový software, systémy správy identit, operační systémy, směrovače a modemy pro připojení k internetu nebo chytré domácí zámky a bezpečnostní kamery.
Důležité produkty třídy II čl. 7 a příloha III CRA	Hypervizory a systémy runtime kontejnerů, firewally, systémy detekce a prevence narušení (IDS/IPS) a mikroprocesory i mikrořadiče odolné proti neoprávněné manipulaci.
Kritické produkty čl. 8 a příloha IV CRA	Hardwarová zařízení s bezpečnostními schránkami, brány inteligentních měřicích systémů (smart meter gateways) a čipové karty či obdobná zařízení včetně zabezpečených prvků.
Ostatní (obecné) produkty	Všechno, co není vyjmenované v přílohách III a IV CRA. Typicky jsou to běžné aplikace, kancelářské nástroje nebo jednoduchá IoT zařízení. Podle odhadů Komise jde přibližně o 90 % produktů na trhu.

2.2 Podle čeho se produkt zařazuje

Zařazení se neodvíjí od toho, kolik funkcí produkt nabízí ani jaké komponenty obsahuje. Rozhoduje jeho **klíčová funkčnost**, tedy hlavní vlastnosti a technické schopnosti, bez kterých by produkt nemohl plnit svůj zamýšlený účel. U hraničních případů se řiďte následujícími pravidly.

Jeden produkt, jedna klíčová funkčnost

Produkt má pro účely posuzování shody jednu klíčovou funkčnost, ne několik. Kategorie se nesčítají a produkt neprochází nejpřísnější cestou za každou funkci, kterou umí. Pokud produkt odpovídá dvěma kategoriím, vyberte tu přesnější, i kdyby patřila do vyšší třídy. Volbu si zapište i s odůvodněním.

Doplňkové funkce zařazení nemění

Operační systém, který obsahuje i kalkulačku nebo jednoduchý grafický editor, zůstává operačním systémem.

Zabudovaná komponenta produkt do vyšší kategorie nepřesune

Zpravodajská aplikace s vestavěným prohlížečem se nestává prohlížečem. Smartphone s operačním systémem i správcem hesel není ani operačním systémem, ani správcem hesel. Pro zařazení se komponenty nepočítají, pro bezpečnost produktu ale ano: výrobce musí posoudit produkt jako celek, tedy i se zabudovanými komponentami.

Co tvrdíte, musí odpovídat realitě

Klíčovou funkčnost nelze popsat účelově tak, aby produkt unikl přísnějšímu režimu. Rozhodující bude vždy zamýšlený účel produktu a jeho předvídatelné použití.

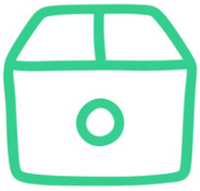
Zařazení produktu do kategorie nezakládejte na tom, jak produkt prodáváte, ale na tom, **jaký je jeho účel a jak se bude používat**.

2.3 Cesta ke shodě podle kategorie produktu

CRA stanoví, jakými postupy můžete shodu prokázat. Liší se hlavně tím, jak moc do nich vstupuje nezávislá třetí strana. Kategorie produktu tedy určuje, jak lze prokázat, že **produkt požadavky CRA splňuje**.

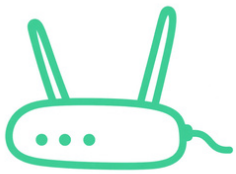
Oznámený subjekt

Oznámený subjekt je osoba nebo instituce, která **kontroluje shodu**. Zjednodušeně jsou to auditoři, kteří podle konkrétních postupů určí, jestli je produkt skutečně v souladu s požadavky CRA.



Ostatní (obecné) produkty

Vystačíte si sami. Shodu posoudíte interní kontrolou, bez oznámeného subjektu. Sami pak popíšete, jak jste požadavky splnili. Je to nejjednodušší a nejlevnější cesta. Přísnější postup si můžete zvolit dobrovolně.



Důležité produkty třídy I

U těchto produktů můžete provádět interní kontrolu, ale jen v případě, že už máte kybernetickou bezpečnost certifikovanou podle jiných evropských norem nebo regulací. Takové případy budou zatím spíš výjimečné. Častěji se na produkt použijí následující moduly posuzování shody:

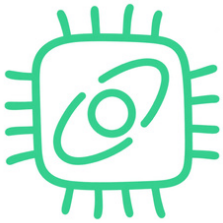
- **Modul B** – EU přezkoušení typu
- **Modul C** – shoda s typem na základě interního řízení výroby
- **Modul H** – komplexní zabezpečování kvality

2.3 Cesta ke shodě podle kategorie produktu

Důležité produkty třídy II

Interní kontrola u těchto produktů nestačí, a to ani při plném uplatnění norem. Nabízejí se tři postupy.

- **Modul B+C**
- **Modul H**
- **Evropská certifikace**



Kritické produkty

Platí stejné tři cesty jako u důležitých produktů třídy II. Komise navíc může aktem v přenesené pravomoci stanovit povinnost získat evropský certifikát, jakmile je pro danou kategorii schéma přijaté a dostupné.

- **Modul B+C**
- **Modul H**
- **Evropská certifikace**

Evropská certifikace

Systém posouzení shody, kdy si místo modulu pořídíte evropský certifikát kybernetické bezpečnosti na úrovni záruky alespoň „významná“. Pro čipové karty a zabezpečené prvky je takové schéma, EUCC, dnes k dispozici.

2.4 Moduly posuzování shody

Modul B – EU přezkoušení typu

- Výrobce předloží vybranému oznámenému subjektu technickou dokumentaci, analýzu rizik a vzorek produktu. Oznámený subjekt produkt přezkouší a otestuje.
- Pokud produkt splňuje základní požadavky CRA, oznámený subjekt vystaví certifikát o EU přezkoušení typu. Ten slouží jako oficiální doklad, že tento konkrétní konstrukční typ prošel nezávislou kontrolou.
- Modul B sám o sobě nestačí. Musí být vždy doplněn modulem C.

Modul C – shoda s typem na základě interního řízení výroby

- Modul C navazuje na modul B. Jeho cílem je zajistit, aby každý vyrobený kus odpovídal schválenému typu z certifikátu.
- Výrobce přijímá nezbytná opatření při výrobě, kontroluje shodu jednotlivých produktů, umisťuje označení CE a vypracovává prohlášení o shodě, které uchovává 10 let nebo po dobu podpory produktu.
- Kombinace modulů B+C tedy znamená: nezávislá kontrola typu a výrobcem řízená kontrola sériové výroby.

Modul H – komplexní zabezpečování kvality

- U modulu H se neposuzuje jen konkrétní typ produktu. Oznámený subjekt audituje celý systém kvality výrobce, tedy návrh, vývoj, výrobu, kontrolu i postupy řešení zranitelností.
- Po schválení systému kvality může výrobce zaručit shodu pro celou kategorii svých produktů. Zároveň ale podléhá průběžným dohledovým auditům.
- Modul H je náročnější na zavedení, ale nabízí větší flexibilitu pro společnosti se širším portfoliem produktů nebo častými aktualizacemi.

2.5 Jak určit kategorii produktu

Abyste správně určili kategorii, vycházejte z funkčního popisu produktu, tedy ze zamýšleného účelu, hlavních funkcí a rozhraní.

1. **Je produkt uvedený v přílohách III nebo IV CRA?**
   Pokud ano, jde o kritický produkt nebo o důležitý produkt třídy I nebo třídy II. Samoposouzení v žádné z těchto kategorií zpravidla nestačí. Posouzení souladu budete muset řešit se zapojením třetí strany.

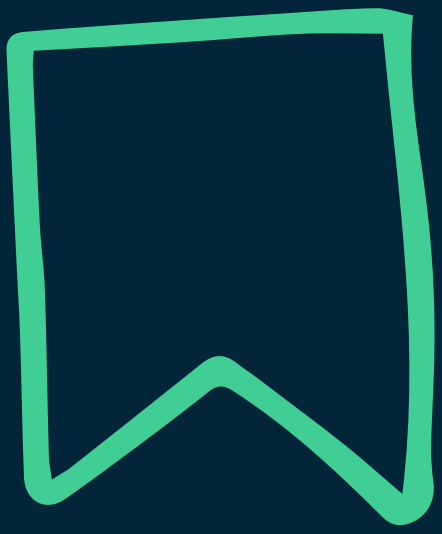
2. **Nespadá produkt ani do jedné z příloh?**
   Pak jde o ostatní (obecný) produkt a posouzení toho, zda jste v souladu s CRA, si můžete provést sami.

Klasifikaci proveďte znovu **vždy, když se změní funkčnost produktu** nebo jeho zamýšlený účel, dojde k podstatné změně nebo se změní legislativa.

2.6 Záznam o zařazení

Závěr o zařazení do kategorie si vždy zapište, **i když je negativní**. Doložený závěr, proč produkt do kategorie nespadá, má stejnou hodnotu jako závěr pozitivní. Do záznamu patří:

- Identifikace a verze produktu.
- Datum posouzení a odpovědná osoba.
- Určená klíčová funkčnost.
- Výsledná kategorie.
- Kategorie, které jste zvažovali a vyloučili, včetně důvodu.
- Přípustné postupy posuzování shody, které z výsledku plynou.



Shrnutí kapitoly

- Základní požadavky na kybernetickou bezpečnost platí pro všechny produkty stejně. Kategorie rozhodují o tom, jak náročné bude jejich splnění prokázat.

- CRA rozlišuje ostatní (obecné) produkty, důležité produkty třídy I a II a kritické produkty. Odhadem 90 % trhu tvoří obecné produkty, u kterých si výrobce při posouzení shody vystačí sám.

- Pro zařazení do kategorie rozhoduje klíčová funkčnost, ne doplňkové funkce ani zabudované komponenty. Podrobný popis kategorií najdete v prováděcím nařízení (EU) 2025/2392.

- U obecných produktů stačí provést samoposouzení.
  U důležitých produktů tříd I a II a u kritických produktů se požadavky stupňují a posouzení shody musí provádět třetí strana.

03

Základní kyberbezpečnostní požadavky CRA

Co musí produkt splňovat z hlediska kybernetické bezpečnosti bez ohledu na kategorii, do které patří? Základní požadavky stanovuje příloha I CRA a dělí je na dvě části. Část I se týká vlastností produktu, tedy toho, jak je produkt navržený, vyvinutý a vyrobený. Část II se týká řízení zranitelností, tedy toho, jak výrobce bezpečnost produktu řídí po celou dobu, po kterou se očekává jeho používání.

Cybrela

3.1 Bezpečnost podle rizika, ne podle šablony

CRA vychází z principu proporcionality. Výrobce má zvolit bezpečnostní opatření **podle skutečných rizik produktu**, ne podle jednotné šablony pro všechny produkty.

Jinou úroveň ochrany bude vyžadovat jednoduché zařízení, které komunikuje v izolované lokální síti, a jinou zařízení dostupné z internetu, s administračním rozhraním a přístupem k citlivým datům.

Součástí požadavků technické dokumentace je proto **posouzení kybernetických bezpečnostních rizik**, které zohledňuje zamýšlený účel produktu, jeho rozumně předvídatelné použití, podmínky používání a očekávanou dobu, po kterou se produkt bude používat.

Posouzení rizik nemá být formální dokument navíc. **Má ovlivnit samotný návrh produktu** – architekturu, oddělení jednotlivých funkcí, omezení oprávnění nebo zabezpečení komunikačních rozhraní.

Bezpečnostní riziko se neřeší až po dokončení vývoje, ale je jedním ze vstupů, podle kterých se produkt navrhuje.

3.2 Bezpečnost jako výchozí nastavení

Princip „security by default“ znamená, že **produkt má být bezpečný už ve výchozím nastavení**. Základní zabezpečení nemá záviset na tom, že si zákazník po zakoupení produktu provede bezpečnostní konfiguraci sám. Výrobce má potřebná opatření nastavit předem – například zapnout automatickou instalaci bezpečnostních aktualizací.

Výrobce **nemůže přenést odpovědnost za bezpečnost produktu na zákazníka** prostřednictvím pokynů typu „po instalaci si změňte heslo a vypněte tuto službu“.

Pokud šlo produkt navrhnout bezpečněji už ve výchozím nastavení, nestačí se spolehnout na to, že si zákazník přečte návod.

3.3 Vlastnosti produktu podle přílohy I části I

Část I přílohy I určuje, jaké **technické požadavky** musí produkt splňovat. Míra jejich naplnění se odvíjí od rizik a charakteru konkrétního produktu. Výrobce se však musí vypořádat se všemi následujícími oblastmi:

- **Řízení přístupu a autentizace**
- **Odolnost a dostupnost**
- **Důvěrnost a integrita dat**
- **Omezení dopadu incidentu**
- **Minimalizace útočné plochy**
- **Záznam a monitorování**

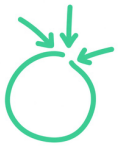
3.4 Technické požadavky na produkt

Řízení přístupu a autentizace

Produkt musí rozlišovat oprávněné a neoprávněné uživatele. Jednotlivým účtům nebo procesům má přidělovat pouze oprávnění, která skutečně potřebují.

Důvěrnost a integrita dat

Citlivá data musí být chráněna při uložení i přenosu, například pomocí šifrování. Produkt musí zároveň zabraňovat neoprávněným změnám dat, konfigurace nebo softwaru.



Minimalizace útočné plochy

Síťové služby, porty a rozhraní mají být omezeny pouze na ty, které produkt skutečně potřebuje ke svému fungování. Pokud jsou všechny služby aktivní už ve výchozím nastavení, zbytečně se rozšiřuje prostor, který může útočník využít.

Odolnost a dostupnost

Ochrana základních funkcí produktu, včetně omezení dopadu útoků typu odepření služby (DoS), a to i na jiná zařízení a sítě, se kterými je produkt propojen.

Omezení dopadu incidentu

Výrobce má zavést opatření, jako je oddělení procesů nebo izolace funkcí, aby kompromitace jedné části produktu automaticky nevedla k převzetí celého produktu.

Záznam a monitorování

Zaznamenávání bezpečnostně významných interních událostí v rozsahu odpovídajícím riziku produktu. Uživatel musí mít možnost monitorování vypnout.

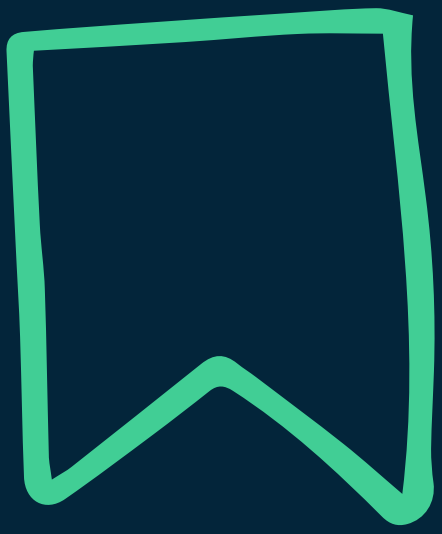
3.5 Řízení zranitelností

Odpovědnost za bezpečnost produktu nekončí jeho uvedením na trh. Část II přílohy I CRA ukládá výrobci povinnosti, které trvají po celou dobu podpory produktu. Výrobce musí produkt podporovat nejméně **5 let od jeho uvedení na trh**. Podpora může trvat kratší dobu, pokud je kratší také očekávaná doba používání produktu. Výrobce musí zejména:

- **Identifikovat a dokumentovat zranitelnosti** a komponenty produktu, mimo jiné prostřednictvím SBOM, tedy softwarového kusovníku.
- Neprodleně **řešit a odstraňovat zranitelnosti**, provádět odpovídající bezpečnostní testování a zveřejňovat informace o opravených zranitelnostech.
- Zavést **politiku koordinovaného zveřejňování zranitelností** (CVD) a zveřejnit jasný kontakt, na který mohou uživatelé nebo bezpečnostní výzkumníci zranitelnost nahlásit.
- **Distribuovat bezpečnostní aktualizace** zabezpečeným způsobem, typicky s využitím digitálního podpisu a ověření integrity, a poskytovat je bezplatně, pokud se strany nedohodnou jinak.

Další povinnosti výrobce po uvedení produktu na trh najdete podrobněji rozepsané v kapitole 5.1.

Základní požadavky CRA je užitečné vnímat jako celek. Výrobce nejprve **identifikuje rizika** a podle nich produkt navrhne. Během vývoje zavede odpovídající **bezpečnostní mechanismy** a po uvedení produktu na trh sleduje zranitelnosti a poskytuje aktualizace.



Shrnutí kapitoly

- CRA staví základní kyberbezpečnostní požadavky na dvou pilířích podle přílohy I: vlastnostech produktu podle části I a řízení zranitelností podle části II. Každý produkt musí splňovat požadavky obou částí.
- Klíčovým principem je proporcionalita. Výrobce nejprve posoudí skutečná rizika produktu a podle nich volí bezpečnostní opatření, která promítne už do samotného návrhu.
- Produkt má být bezpečný už ve výchozím nastavení, včetně automatických bezpečnostních aktualizací zapnutých jako výchozí volba.
- Požadavky na vlastnosti produktu podle části I zahrnují řízení přístupu, ochranu dat, omezení útočné plochy, odolnost a dostupnost, omezení dopadu incidentu a monitorování.

04

Prokazování shody – technická dokumentace, EU prohlášení o shodě a označení CE

Shodu prokazujete technickou dokumentací, EU prohlášením o shodě a označením CE. Pořadí není libovolné, každý krok stojí na předchozím. Kapitola ukazuje, co mají obsahovat a jak dlouho si je musíte uchovat.

Cybrela

4.1 Na čem stojí prokázání shody

Prokázání shody je způsob, jakým výrobce **doloží, že produkt s digitálními prvky splňuje požadavky CRA**. Celý systém stojí na třech vzájemně provázaných pilířích.

Technická dokumentace

Popisuje produkt, jeho návrh a vývoj, posouzení kybernetických rizik, použité komponenty včetně SBOM a hlavně to, jak jsou naplněné jednotlivé požadavky CRA na vlastnosti produktu i na zacházení se zranitelnostmi. Zůstává u výrobce a nikde se nezveřejňuje. Musí ale být k dispozici orgánu dozoru, a to i roky poté, co produkt uvedete na trh.

EU prohlášení o shodě

Krátký formální dokument, kterým výrobce na vlastní odpovědnost prohlašuje, že produkt požadavky CRA splňuje.

Označení CE

Viditelný symbol, který se umisťuje na produkt a potvrzuje, že produkt prošel předepsaným postupem posouzení shody.

Pořadí v rámci prokázání shody není libovolné. Nejprve vzniká technická dokumentace, na jejím základě výrobce vypracuje EU prohlášení o shodě a teprve poté smí na produkt s digitálními prvky umístit označení CE. Bez prvního kroku nelze platně provést druhý ani třetí.

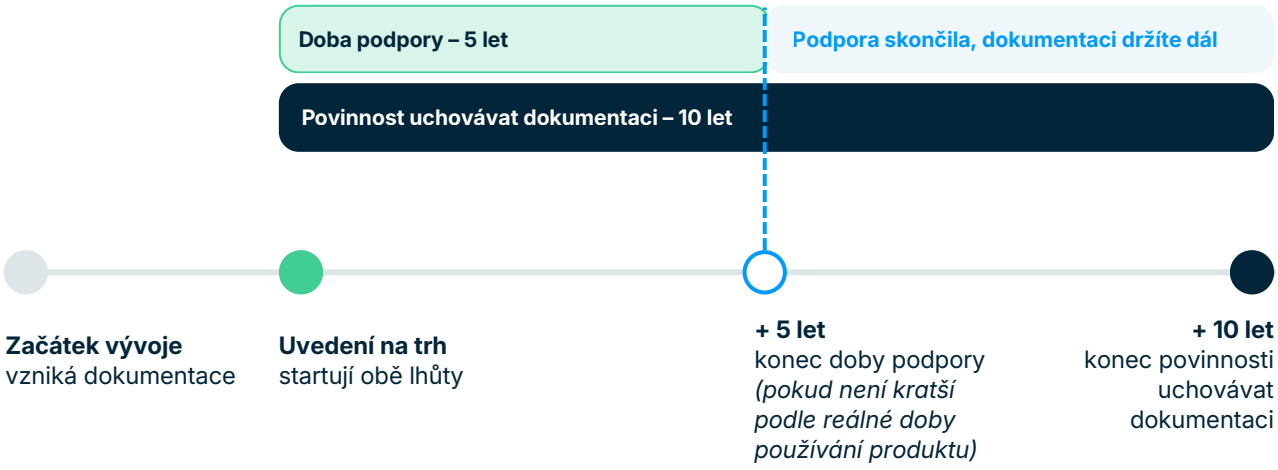
4.2 Technická dokumentace

Technická dokumentace dokazuje, jak produkt i procesy kolem něj **splňují základní požadavky na kybernetickou bezpečnost** z přílohy I nařízení CRA. Musí obsahovat všechny relevantní údaje o tom, jakými prostředky jste shody dosáhli.

Dokumentaci vypracujete **před uvedením produktu na trh** a průběžně ji aktualizujete, nejméně však po celou dobu podpory. Shoda se totiž v čase mění: vydáte novou verzi, vyměníte knihovnu, upravíte způsob distribuce aktualizací.

Technickou dokumentaci musíte uchovávat **nejméně 10 let** od uvedení produktu na trh, nebo po dobu podpory, podle toho, které období je delší.

Technickou dokumentaci a korespondenci k posuzování shody připravujete **v úředním jazyce státu, ve kterém sídlí oznámený subjekt**, nebo v jazyce, který tento subjekt přijímá. Pokud shodu posuzujete sami, oznámený subjekt do procesu nevstupuje.



4.3 Co musí dokumentace obsahovat

Náležitosti technické dokumentace stanoví **příloha VII nařízení CRA**.

- **Všeobecný popis produktu**, jeho zamýšlený účel, verze softwaru ovlivňující shodu a u hardwaru také fotografie nebo nákresy a informace a pokyny pro uživatele.
- **Popis návrhu, vývoje a výroby produktu i postupů, kterými řešíte zranitelnosti.** Patří sem architektura systému, softwarový kusovník (SBOM), politika koordinovaného zveřejňování zranitelností, kontaktní adresa pro hlášení a popis toho, jak bezpečně distribuujete aktualizace.
- **Seznam použitých harmonizovaných norem, společných specifikací nebo certifikačních schémat**. Pokud jste žádné nepoužili, popis řešení, kterými jste požadavky splnili.
- **Posouzení kybernetických bezpečnostních rizik.**
- **Informace zohledněné při stanovení doby podpory.**
- **Protokoly o provedených zkouškách.**
- **Kopie EU prohlášení o shodě.**

Na odůvodněnou žádost orgánu dozoru nad trhem mu navíc poskytnete softwarový kusovník (SBOM).

Mikropodniky a malé podniky mohou technickou dokumentaci poskytnout ve **zjednodušeném formátu**, který stanoví Komise prováděcím aktem. Menší společnost tedy nemusí vypracovávat stejně objemný spis jako velký výrobce. Obsahové jádro ale zůstává stejné.

4.4 EU prohlášení o shodě

EU prohlášení o shodě je formální dokument, kterým jako výrobce potvrzujete, že produkt splňuje příslušné požadavky na kybernetickou bezpečnost podle nařízení CRA. Jeho vypracováním **přebíráte odpovědnost za soulad produktu s požadavky**.

Prohlášení musí být dostupné v jazycích požadovaných státem, **kde se produkt uvádí na trh**. Pokud tedy produkt prodáváte do několika zemí EU, řešíte jazykové verze, ne jednu univerzální.

Pokud se na produkt vztahuje více právních aktů EU vyžadujících prohlášení o shodě, **vypracuje se jedno společné prohlášení** odkazující na všechny tyto předpisy.

Výrobce může k produktu přiložit buď **úplné, nebo zjednodušené EU prohlášení o shodě**.

Zjednodušené prohlášení musí obsahovat **přesnou internetovou adresu**, kde je dostupné úplné znění.

4.5 Co musí EU prohlášení o shodě obsahovat

Náležitosti EU prohlášení o shodě stanoví **příloha V nařízení CRA**.

- **Identifikace produktu umožňující jeho zpětné vysledování.** U softwaru to znamená přesné určení verze, u hardwaru typicky typ, model nebo sériové číslo. Smyslem je, aby bylo kdykoli jasné, ke které konkrétní podobě produktu se prohlášení vztahuje.
- **Jméno a adresa výrobce** nebo jeho zplnomocněného zástupce.
- **Konstatování, že se prohlášení vydává na výhradní odpovědnost výrobce** a že je produkt ve shodě s příslušnými harmonizačními předpisy EU.
- **Odkazy na použité harmonizované normy, společné specifikace nebo certifikace.**
- **Název a číslo oznámeného subjektu a vydaný certifikát** (pokud byl zapojen).
- **Datum vydání, podpis a funkce podepisující osoby.**

4.6 Označení CE

Jde o **viditelný symbol**, kterým výrobce stvrzuje, že produkt a procesy kolem něj splňují základní požadavky CRA i další předpisy EU, které se na produkt vztahují. Pravidla pro jeho podobu a umisťování se řídí obecnými zásadami nařízení (ES) č. 765/2008.

- Označení musíte umístit **dřív, než produkt uvedete na trh**. Obvyklá minimální výška značky je 5 mm. U produktů podle CRA ale může být i menší, pokud zůstane označení CE viditelné a čitelné.
- Pokud se na produkt vztahují i jiné předpisy EU, které označení CE vyžadují, jedno označení pokrývá shodu se všemi. **Nedává se na produkt vícekrát**.
- Za označením může následovat piktogram nebo **jiná značka upozorňující na zvláštní kybernetické bezpečnostní riziko** nebo na konkrétní způsob použití. Jak přesně budou vypadat, teprve stanoví Komise prováděcím aktem.

Typ produktu	Kam umístit označení CE
Hardware	Viditelně, čitelně a nesmazatelně přímo na produkt, nebo když to nejde, tak na obal a na EU prohlášení o shodě přiložené k produktu.
Software	Na EU prohlášení o shodě, nebo na web doprovázející produkt – snadno a přímo přístupné spotřebiteli.

4.7 Proces prokázání shody

Postup prokázání shody probíhá v logickém sledu událostí a kroků.

1. **Vypracujete technickou dokumentaci**
   Technická dokumentace vzniká průběžně s vývojem produktu a drží všechny důkazy o tom, jak produkt plní požadavky CRA. Na dokumentaci stojí všechny další kroky.

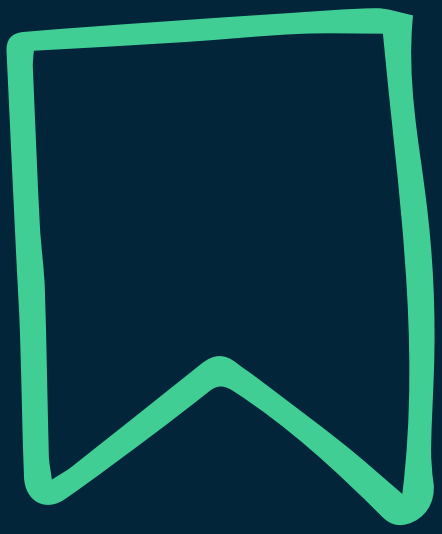
2. **Provedete posouzení shody**
   Buď vlastními silami, nebo s někým dalším. Rozhoduje kategorie produktu: interní kontrola, oznámený subjekt, evropská certifikace.

3. **Vypracujete EU prohlášení o shodě**
   Formálním dokumentem potvrzujete, že produkt požadavky nařízení CRA splňuje. Podpisem za to ručíte.

4. **Umístíte označení CE**
   Na produkt ho smíte umístit až ve chvíli, kdy máte technickou dokumentaci a EU prohlášení o shodě. Nejpozději však před uvedením na trh.

5. **Uchováváte a aktualizujete**
   Dokumentaci i prohlášení o shodě uchováváte 10 let od uvedení na trh, případně déle, pokud produkt tak dlouho podporujete.

V praxi se vyplatí vést technickou dokumentaci jako živý dokument **od začátku vývoje**, nikoli až těsně před uvedením na trh, a aktualizovat ji při každé podstatné změně produktu i při řešení zranitelností.



Shrnutí kapitoly

- Prokázání shody je **způsob, jakým výrobce doloží, že produkt s digitálními prvky splňuje požadavky CRA**. Systém prokazování shody stojí na třech pilířích – technická dokumentace, EU prohlášení o shodě a označení CE.
- Postup posouzení shody se **liší podle kategorie produktu**. Rozhoduje o tom, jestli si vystačíte sami, nebo do procesu vstoupí oznámený subjekt.
- **Technická dokumentace** je důkazním základem. Veďte ji jako živý dokument od začátku vývoje.
- **EU prohlášení o shodě** je závazek výrobce, že produkt splňuje požadavky na kybernetickou bezpečnost. Není to formalita.
- **Označení CE** se umisťuje na produkt až jako poslední krok, před uvedením na trh.

05

Povinnosti po uvedení produktu na trh

Uvedením na trh povinnosti nekončí. Po celou dobu podpory musíte hledat a odstraňovat zranitelnosti, vydávat aktualizace a informovat uživatele. Kapitola shrnuje, co čeká výrobce a v čem jsou povinnosti dovozce a distributora mírnější, a co má dělat správce open source softwaru.

Cybrela

5.1 Povinnosti výrobce

Výrobce má nejširší okruh povinností. **Po celou dobu podpory** musí evidovat, testovat a odstraňovat zranitelnosti produktu i jeho komponent. Příloha I část II nařízení CRA stanoví konkrétně, co všechno musí zajistit.

- **Identifikovat a dokumentovat zranitelnosti** a komponenty, zejména prostřednictvím softwarového kusovníku ve strojově čitelném formátu.
- Neprodleně **řešit a odstraňovat zranitelnosti**, nejčastěji bezpečnostními aktualizacemi. Tam, kde je to technicky možné, odděleně od funkčních aktualizací.
- Pravidelně a účinně testovat a **přezkoumávat bezpečnost** produktu.
- Po vydání opravy zveřejnit informace o opravených zranitelnostech, tedy jejich **popis, dopad, závažnost a způsob odstranění**.
- Zavést a prosazovat politiku koordinovaného zveřejňování zranitelností.
- **Usnadnit sdílení informací** o zranitelnostech, mimo jiné zveřejněním kontaktní adresy pro jejich hlášení.
- Zajistit bezpečnou distribuci aktualizací, automaticky tam, kde je to možné.

Zranitelnost

Zranitelnost je podle CRA slabina, snížená odolnost nebo chyba produktu s digitálními prvky, kterou lze zneužít v rámci kybernetické hrozby.

5.2 Zranitelnosti v převzatých komponentách

Zranitelnost se může nacházet i v komponentě, kterou jste do produktu začlenili, včetně softwaru s otevřeným zdrojovým kódem. Odpovědnost tím nepřechází na dodavatele komponenty. Zůstává na vás. **Zranitelnost musíte v první řadě vyřešit ve svém produktu** a oznámit ji tomu, kdo komponentu vyvíjí nebo udržuje.

Pokud sami zranitelnost v komponentě opravíte, **poskytnete vývojáři** komponenty příslušný kód nebo dokumentaci, ideálně ve strojově čitelném formátu.

5.3 Bezpečnostní aktualizace

Jakmile je bezpečnostní aktualizace produktu k dispozici, **musí být sdílena neprodleně a zpravidla bezplatně**. Spolu s ní jde k uživatelům poradní zpráva s informacemi, které potřebují vědět. Aktualizace musí zůstat dostupné nejméně 10 let po vydání, nebo po zbytek doby podpory, pokud je delší.

V situacích, kdy výrobce vydá podstatně změněnou verzi produktu, může bezpečnostní aktualizace zajišťovat jen u této poslední verze. Podmínkou je, že uživatelé starších verzí k ní budou mít **bezplatný přístup**.

5.4 Doba podpory

Součástí odpovědnosti výrobce je také **určit dobu podpory a informovat o ní uživatele**. Stanovuje se už při uvádění produktu na trh a musí odpovídat tomu, jak dlouho se produkt bude reálně používat.

- Minimální doba podpory je zpravidla **5 let**. U produktů s kratší životností odpovídá doba podpory tomu, jak dlouho se bude produkt reálně používat.
- Doba podpory se stanoví **podle očekávané doby používání**, povahy produktu a přiměřených očekávání uživatelů.
- Měsíc a rok, kdy končí doba podpory, **musí být uvedeny** v době nákupu.
- Výrobce může vést veřejné softwarové **archivy starších verzí**, ale pak musí jasně informovat o rizicích nepodporovaného softwaru.

Pokud zjistíte, že produkt nebo procesy kolem něj nejsou v souladu s požadavky CRA, **musíte bezodkladně přijmout nápravná opatření**. Podle konkrétní situace může jít o:

- uvedení produktu do souladu,
- stažení produktu z trhu,
- stažení produktu od uživatelů.

5.5 Povinnosti dovozce a distributora

Dovozce ani distributor nemají stejnou odpovědnost jako výrobce. Po uvedení produktu na trh ale i na ně několik povinností dopadá. Zejména když se objeví zranitelnost nebo pochybnost o splnění požadavků CRA.

- Jakmile se dozví o zranitelnosti produktu, musí bez zbytečného odkladu **informovat výrobce**.
- Pokud produkt představuje významné kybernetické bezpečnostní riziko, neprodleně **informují orgány dozoru nad trhem** ve státech, kde byl produkt uveden nebo dodán na trh.
- Pokud zjistí, že produkt požadavky nesplňuje, musí zajistit nápravu, **zastavit jeho dodávání na trh**, případně ho vzít zpět od uživatelů.
- Pokud výrobce ukončil činnost a nemůže plnit své povinnosti, informují o tom orgány dozoru i uživatele.

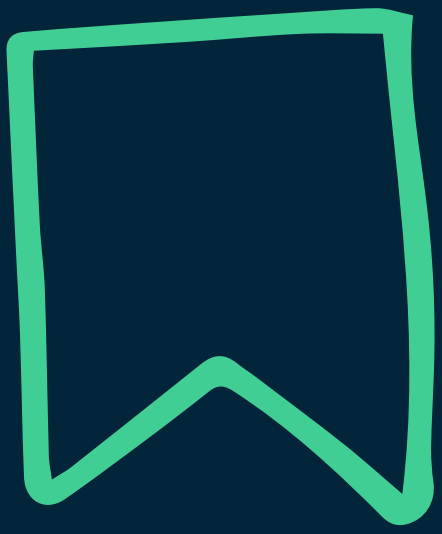
Pozor na změnu role. Jakmile dovozce nebo distributor uvede produkt na trh pod vlastním jménem či ochrannou známkou nebo provede podstatnou změnu produktu, **stává se výrobcem** a přebírá celý rozsah povinností.

5.6 Povinnosti správce open source softwaru

Správce softwaru s otevřeným zdrojovým kódem **neodpovídá za konkrétní produkt** uváděný na trh, ale za procesy, které podporují bezpečný vývoj open source projektů. Jeho povinnosti jsou proto výrazně užší než povinnosti výrobce.

- Musí **zavést a dokumentovat politiku kybernetické bezpečnosti**, která podporuje bezpečný vývoj a řešení zranitelností.
- Podporuje dobrovolné hlášení zranitelností vývojáři a **sdílí informace** v rámci komunity.
- Na žádost **spolupracuje s orgány dozoru** nad trhem při zmírňování rizik.

Oznamovací povinnosti se na správce open source softwaru vztahují jen **v omezeném rozsahu**. Uplatní se do té míry, do jaké je zapojen do vývoje produktu, případně pokud incident zasáhne systémy pro vývoj, které sám poskytuje.



Shrnutí kapitoly

- **Uvedením produktu na trh povinnosti nekončí**. Po celou dobu podpory musí výrobce zranitelnosti hledat, řešit a informovat o nich uživatele.
- Zranitelnost v cizí komponentě je vaše zranitelnost. **Musíte ji vyřešit ve svém produktu** a zároveň ji oznámit tomu, kdo komponentu vyvíjí nebo udržuje.
- Doba podpory je **nejméně 5 let** (pokud není doba používání produktu kratší) a stanovuje se už při uvedení produktu na trh. Uživatel musí znát měsíc a rok jejího konce v době nákupu.
- Dovozce a distributor mají užší povinnosti, **hlavně informační**. Uvedením produktu pod vlastní značkou nebo jeho podstatnou změnou se ale stávají výrobcem se vším, co k tomu patří.
- Bezpečnostní aktualizace výrobce šíří **neprodleně a zpravidla bezplatně**, spolu s poradní zprávou.

06

Oznamování zranitelností a hlášení incidentů

Oznamovací povinnosti platí už od 11. září 2026, tedy podstatně dřív než většina ostatních požadavků nařízení. Kapitola vysvětluje, co se hlásí a co ne, kdo oznámení podává, komu míří a jaké lhůty platí.
Na včasné varování máte 24 hodin.

Cybrela

6.1 Kdy oznamovací povinnost vzniká

Oznamovací povinnosti podle CRA **platí od 11. září 2026**, tedy podstatně dřív než většina ostatních požadavků nařízení.

Nemusíte mít sice hotovou technickou dokumentaci ani prohlášení o shodě, ale musíte mít **funkční proces hlášení**. To znamená vědět, kdo hlášení podává, kdo o něm rozhoduje a co se stane v pátek večer, když do vaší schránky pro hlášení zranitelností přijde zpráva o aktivním zneužití zranitelnosti.

Klíčem k pochopení oznamovacích povinností je **správně rozeznat, o jakou situaci vlastně jde**. CRA pracuje se třemi situacemi, které mají odlišné důsledky pro to, jestli oznamovací povinnost vůbec vzniká.

Běžná zranitelnost	BEZ POVINNOSTI HLÁSIT
Aktivně zneužívaná zranitelnost	POVINNOST HLÁSIT
Závažný incident	POVINNOST HLÁSIT

6.2 Co se (ne)musí hlásit

Běžná zranitelnost

Byla objevena, ale není aktivně zneužívána útočníkem ani škodlivým kódem. Typicky ji objeví sám výrobce, bezpečnostní pracovník, případně přijde hlášení přes koordinované zveřejňování. Povinnost okamžitého hlášení v tomto případě **nevzniká**. Kdokoli ji může **dobrovolně oznámit** týmu CSIRT nebo agentuře ENISA.

BEZ POVINNOSTI HLÁSIT

Aktivně zneužívaná zranitelnost

Existují spolehlivé důkazy, že zranitelnost někdo zneužil bez svolení vlastníka produktu nebo systému. Za spolehlivý důkaz se považují například záznamy v bezpečnostních logech, potvrzení od postiženého uživatele, informace od CERT či CSIRT nebo veřejně dostupný exploit, který byl aktivně používán. Nerozhoduje závažnost vyjádřená skóre CVSS, ale to, zda probíhá aktivní zneužití.

POVINNOST HLÁSIT

Závažný incident

Jde o incident, který negativně ovlivnil nebo může ovlivnit schopnost produktu chránit **dostupnost, autenticitu, integritu nebo důvěrnost citlivých či důležitých dat nebo funkcí produktu**. Spadá sem i situace, kdy dojde k zavlečení či spuštění škodlivého kódu v produktu nebo v síti uživatele. Typicky ransomware šířící se zranitelností, DDoS útok, který vyřadil základní funkce produktu, neautorizovaný přístup, zranitelnost umožňující únik dat nebo zapojení produktu do botnetu.

POVINNOST HLÁSIT

6.3 Kdo má oznamovací povinnost

Oznamovací povinnost se týká dvou ze tří uvedených situací: **aktivně zneužívané zranitelnosti** a **závažného incidentu** s dopadem na bezpečnost produktu. Rozsah oznamovacích povinností se liší podle role.

Výrobce má povinnost oznamovat aktivně zneužívané zranitelnosti i povinnost hlásit závažné incidenty.	Plná povinnost
Dovozce a distributor mají stejnou povinnost, pokud na trh uvádí produkt pod vlastním jménem či ochrannou známkou, případně pokud produkt podstatně upraví. Typickým příkladem je prodej elektroniky pod vlastní privátní značkou.	Plná povinnost
Ostatní dovozci a distributoři informují o zranitelnosti výrobce a také orgány dozoru, pokud mají důvod se domnívat, že produkt představuje významné kybernetické bezpečnostní riziko.	Informační
Správce open source softwaru má oznamovací povinnost v rozsahu, v jakém je do vývoje produktu zapojen.	Mírnější režim

6.4 Lhůty a proces hlášení

Hlášení probíhá prostřednictvím **jednotné oznamovací platformy**, kterou provozuje agentura ENISA. Odtud míří současně dvěma adresátům: **agentuře ENISA** a **týmu CSIRT** určenému jako koordinátor v členském státě, kde má výrobce hlavní provozovnu.

Pro výrobce se sídlem v České republice plní roli koordinátora vládní CERT, který je součástí NÚKIB.

Oznámení aktivně zneužívaných zranitelností a závažných incidentů probíhá ve třech fázích.

1

Včasné varování – do 24 hodin

Lhůta běží od chvíle, kdy se o aktivně zneužívané zranitelnosti nebo závažném incidentu dozvíte. Včasné varování obsahuje jen základní informace, jeho smyslem je hlavně rychlost, ne úplnost. Nikdo v této fázi nečeká hotovou analýzu.

2

Oznámení – do 72 hodin

Oznámení u zranitelnosti obsahuje obecné informace o její povaze, dostupná nápravná opatření, dále opatření, která mohou přijmout uživatelé, posouzení citlivosti oznamovaných informací a případně první vyhodnocení. U incidentu zahrnuje obecnou povahu incidentu, prvotní posouzení a přijatá zmírňující opatření.

3

Závěrečná zpráva – do 14 dnů nebo 1 měsíce

Lhůta je 14 dnů u zranitelnosti a 1 měsíc u incidentu, podrobnosti najdete v další podkapitole.

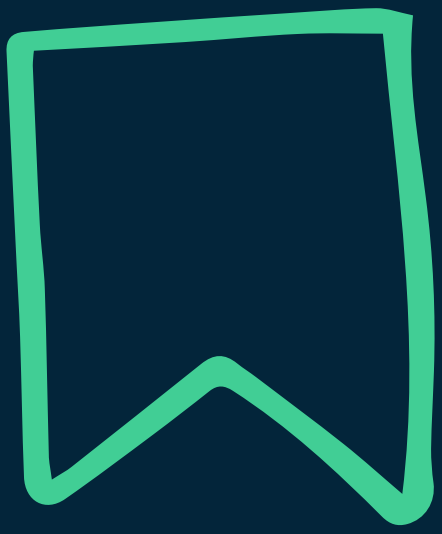
6.5 Závěrečná zpráva

Lhůta i obsah se liší podle toho, zda se oznamuje aktivně zneužívaná zranitelnost nebo závažný incident.

- U zneužívané zranitelnosti **do 14 dnů** od chvíle, kdy je k dispozici nápravné nebo zmírňující opatření. Obsahuje popis zranitelnosti včetně závažnosti a dopadu, informace o útočníkovi nebo škodlivém softwaru (pokud jsou známy) a detaily bezpečnostních aktualizací či nápravných opatření.
- U incidentu **do 1 měsíce** od oznámení, které musí proběhnout ve lhůtě do 72 hodin. Obsahuje podrobný popis incidentu včetně závažnosti a dopadu, druh hrozby nebo základní příčinu a probíhající zmírňující opatření.

Nezapomeňte na uživatele. Vedle hlášení regulátorovi musíte bez zbytečného odkladu **informovat i dotčené uživatele** produktu a doporučit jim, jak mohou riziko zmírnit.

Nad rámec povinného hlášení umožňuje CRA **dobrovolné oznámení zranitelností a incidentů** komukoli, tedy nejen výrobcům, dovozcům a distributorům, ale i uživatelům nebo bezpečnostním pracovníkům.



Shrnutí kapitoly

- Oznamovací povinnosti platí **od 11. září 2026**, tedy podstatně dřív než většina ostatních požadavků nařízení CRA.
- Hlásí se **aktivně zneužívaná zranitelnost** u produktu a **závažný incident** s dopadem na bezpečnost produktu. Běžná zranitelnost, kterou nikdo nezneužívá, se hlásit nemusí.
- Povinnost oznamovat zranitelnosti a hlásit incidenty **dopadá hlavně na výrobce**. Dovozce nebo distributor ji přebírá, pokud produkt uvede na trh pod vlastním jménem či ochrannou známkou nebo ho podstatně upraví.
- Lhůty běží ve třech krocích: **včasné varování do 24 hodin**, oznámení do 72 hodin, závěrečná zpráva do 14 dnů od dostupnosti nápravného opatření u zranitelnosti a do 1 měsíce od oznámení u incidentu.

07

Kontrola, nápravná opatření a sankce

Shodu u většiny produktů potvrzujete sami, na vlastní odpovědnost. Kontrola ale může přijít kdykoli po celou dobu životního cyklu produktu. Kapitola popisuje, co orgán dozoru zkoumá, jak postupuje při nálezu a kde jsou horní hranice pokut.

Cybrela

7.1 Kdo vás může kontrolovat

V každém členském státě působí orgán dozoru nad trhem, který kontroluje, jestli váš produkt odpovídá požadavkům CRA.

- Může si vyžádat **přístup k datům a k veškeré dokumentaci** potřebné k posouzení shody, včetně interních podkladů o vývoji a řešení zranitelností.
- Může požadovat informace, kontrolovat produkty a u produktů s významným rizikem **nařizovat nápravná opatření**.
- Při dohledu nad plněním oznamovacích povinností **spolupracuje s týmy CSIRT** a agenturou ENISA.

7.2 Co se kontroluje

Kontrola se neomezuje na dokumentaci. Orgán obvykle posuzuje tři věci najednou.

Dokumentace

EU prohlášení o shodě a technická dokumentace.

Procesy

Zejména způsob, jakým řešíte zranitelnosti.

Produkt

Samotný produkt a jak se chová v praxi.

7.3 Co se stane, když něco nesedí

Postup je zpravidla odstupňovaný. Nejdříve **přijde výzva k nápravě**, teprve potom přísnější opatření nebo sankce. Konkrétní scénář se liší podle povahy problému.

a) Produkt představuje vážné riziko
Orgán produkt posoudí, a pokud najde problém, vyzve vás k nápravě nebo ke stažení produktu z trhu v přiměřené lhůtě. Pokud nezareagujete, může sám omezit nebo zakázat dodávání produktu na trh. Dokonce může nařídit jeho stažení od uživatelů, tedy zpětně získat kusy, které se už dostaly ke koncovým zákazníkům.

b) Jde jen o formální chybu
Typicky chybějící označení CE, chybějící nebo nesprávné EU prohlášení o shodě nebo neúplná technická dokumentace. I tady vás orgán nejdříve vyzve k nápravě. Pokud problém přetrvá, může omezit nebo zakázat dodávání produktu na trh.

c) Produkt vyhovuje, ale je rizikový
Orgán může řešit i produkt, který formálně splňuje CRA, pokud ohrožuje zdraví, bezpečnost nebo důležité služby.

Pokud se nesoulad týká více států, řeší se na úrovni EU. Orgány mohou rovněž provádět koordinované kontroly napříč státy, včetně kontrolních nákupů, kdy orgán koupí produkt jako běžný zákazník.

7.4 Jaké hrozí sankce a za co

Sankce jsou odstupňované podle závažnosti a vždy platí, že **vyšší bere** – uplatní se ta z obou hodnot, která je vyšší. Při stanovení výše sankce se navíc přihlíží k závažnosti porušení, opakování a velikosti společnosti.

Čeho se porušení týká	Horní hranice sankce
Porušení základních požadavků z přílohy I a povinností podle článků 13 a 14 (povinnosti výrobců a oznamovací povinnost).	**15 mil. EUR nebo 2,5 % celosvětového ročního obratu**
Porušení dalších povinností, například posouzení shody nebo dokumentace.	**10 mil. EUR nebo 2 % obratu**
Poskytnutí nesprávných, neúplných nebo zavádějících informací oznámenému subjektu či orgánu dozoru na jejich žádost.	**5 mil. EUR nebo 1 % obratu**
Produkt dlouhodobě není v souladu s požadavky CRA a například představuje významnou kybernetickou hrozbu.	**Stažení produktu z trhu**

- **Mikropodnikům a malým podnikům** se neukládá pokuta za nedodržení 24hodinové lhůty pro včasné varování.
- **Správcům softwaru s otevřeným zdrojovým kódem** se správní pokuty podle CRA neukládají. Jejich režim stojí na spolupráci a nápravných opatřeních.

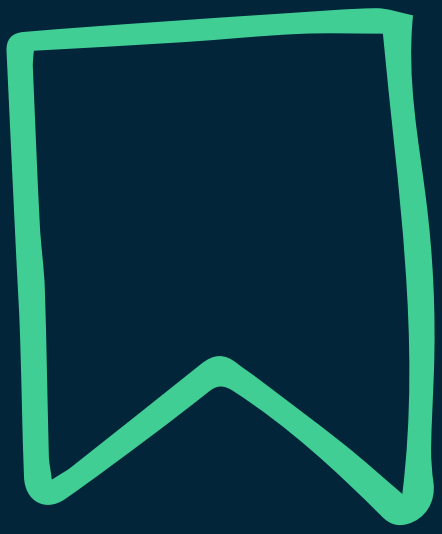
7.5 Jaká máte při kontrole práva

Dohled není jednosměrný. Než orgán nařídí nápravné opatření, máte právo se ke zjištěním vyjádřit v přiměřené lhůtě, která nesmí být kratší než 10 pracovních dnů. Tato lhůta plyne z obecných pravidel dozoru nad trhem podle nařízení (EU) 2019/1020, která se na produkty podle CRA použijí.

Výjimkou jsou situace, kdy **naléhavost rizika vyžaduje okamžitý zásah**.

Tehdy dostanete příležitost vyjádřit se dodatečně a orgán své rozhodnutí okamžitě přezkoumá. Proti rozhodnutí orgánu dozoru existuje opravný prostředek podle národního práva.

V praxi se vyplatí s orgánem **aktivně spolupracovat** a doložit přijatá opatření. Řízení se tak může uzavřít už ve fázi, kdy stačí zjednat nápravu.



Shrnutí kapitoly

- Kontrola může přijít kdykoli **po celou dobu životního cyklu produktu**.
- Nápravná opatření jsou odstupňovaná: od výzvy přes omezení či **zákaz dodávání na trh** až po **stažení od uživatelů**. Před nápravným opatřením máte právo se vyjádřit ve lhůtě, která nesmí být kratší než 10 pracovních dnů.
- Pokuty jdou **až do 15 mil. EUR nebo 2,5 % celosvětového ročního obratu**, podle toho, co je vyšší. Nejvyšší sazba hrozí za porušení základních požadavků z přílohy I a za porušení povinností výrobce, včetně oznamovací povinnosti.

Související pojmy

Vysvětlení hlavních pojmů CRA jsou zjednodušená a slouží k základní orientaci. Závazné jsou definice v článku 3 nařízení (EU) 2024/2847.

Aktivně zneužívaná zranitelnost
Zranitelnost, u které existují spolehlivé důkazy, že ji někdo zneužil bez svolení vlastníka systému. Rozhoduje probíhající zneužití, ne skóre CVSS. Podléhá povinnému hlášení.

Bezpečnostní aktualizace
Oprava, která odstraňuje nebo zmírňuje zranitelnost produktu. Šíří se neprodleně a zpravidla bezplatně, spolu s poradní zprávou.

CVSS
Mezinárodně používaná stupnice závažnosti zranitelností. Pro oznamovací povinnost podle CRA není rozhodující, vysoké skóre samo o sobě povinnost hlásit nezakládá.

Distributor
Subjekt v dodavatelském řetězci jiný než výrobce a dovozce, který produkt dodává na trh, aniž by měnil jeho vlastnosti. Typicky velkoobchod nebo e-shop.

Doba podpory
Období, po které musí výrobce řešit zranitelnosti produktu. Trvá nejméně 5 let, kratší může být jen tehdy, když se počítá s kratším používáním produktu.

Dovozce
Subjekt usazený v EU, který na unijní trh uvádí produkt nesoucí jméno nebo značku výrobce mimo EU.

Důležitý produkt
Produkt uvedený v příloze III nařízení, rozdělený do třídy I a přísnější třídy II. Zařazení určuje, jestli si posouzení shody můžete udělat sami.

ENISA
Agentura Evropské unie pro kybernetickou bezpečnost. Provozuje jednotnou oznamovací platformu a přijímá hlášení souběžně s národním koordinátorem.

EU prohlášení o shodě
Formální dokument, kterým výrobce na svou výhradní odpovědnost stvrzuje, že produkt splňuje požadavky CRA. Náležitosti stanoví příloha V.

Klíčová funkčnost
Hlavní vlastnosti a technické schopnosti produktu, bez kterých by nemohl plnit svůj zamýšlený účel.

Komponenta
Software nebo hardware určený k zabudování do jiného systému. Komponenta zabudovaná do výrobku se posuzuje v rámci tohoto výrobku, komponenta prodávaná zvlášť je samostatný produkt s digitálními prvky.

Modul posuzování shody
Postup, kterým se ověřuje splnění požadavků. Modul A je interní kontrola bez třetí strany, moduly B+C znamenají přezkoušení typu oznámeným subjektem, modul H audit celého systému. Které moduly smíte použít, určuje kategorie produktu.

Orgán dozoru nad trhem
Národní orgán, který kontroluje, jestli produkty na trhu odpovídají požadavkům CRA. Může si vyžádat dokumentaci, nařídit nápravná opatření i omezit dodávání produktu.

Související pojmy

Vysvětlení hlavních pojmů CRA jsou zjednodušená a slouží k základní orientaci. Závazné jsou definice v článku 3 nařízení (EU) 2024/2847.

Označení CE
Viditelný symbol, kterým výrobce stvrzuje shodu produktu s CRA i s dalšími předpisy EU. Umisťuje se až jako poslední krok, před uvedením produktu na trh.

Oznámený subjekt
Nezávislý subjekt posuzování shody určený členským státem. Zjednodušeně akreditovaná zkušebna nebo auditor, který vstupuje do procesu u rizikovějších kategorií produktů.

Podstatná změna
Změna produktu po jeho uvedení na trh, která naruší jeho soulad se základními požadavky nebo změní zamýšlený účel.

Poradní zpráva
Sdělení, které jde k uživatelům spolu s bezpečnostní aktualizací. Obsahuje informace, které uživatelé potřebují vědět, včetně opatření, jež mají přijmout.

Posouzení shody
Postup, kterým ověříte, že produkt a vaše procesy splňují požadavky z přílohy I. Rozsah zapojení nezávislé třetí strany určuje kategorie produktu.

Produkt s digitálními prvky
Hardware nebo software, který se dokáže propojit s jiným zařízením nebo se sítí. Součástí produktu jsou i řešení pro zpracování dat na dálku, bez kterých by produkt nemohl plnit některou ze svých funkcí.

Prokazování shody
Doložení splnění požadavků navenek. Stojí na třech výstupech: technické dokumentaci, EU prohlášení o shodě a označení CE.

Softwarový kusovník (SBOM)
Formální záznam o komponentách obsažených v produktu a o vztazích mezi nimi. Vede se ve strojově čitelném formátu a na odůvodněnou žádost ho poskytnete orgánu dozoru nad trhem.

Technická dokumentace
Soubor podkladů dokládající, jak produkt i procesy kolem něj splňují požadavky CRA. Vzniká před uvedením na trh, průběžně se aktualizuje a uchovává se nejméně 10 let.

Uvedení na trh a dodání na trh
Uvedení na trh je první dodání produktu na unijní trh. Dodání na trh je každé následující předání k distribuci nebo použití, ať už za úplatu, nebo bezplatně.

Výrobce
Ten, kdo produkt vyvíjí nebo vyrábí, případně si ho nechá vyrobit, a nabízí ho pod svým jménem nebo ochrannou známkou. Nese nejširší okruh povinností.

Závažný incident
Incident, který negativně ovlivnil nebo může ovlivnit schopnost produktu chránit dostupnost, autenticitu, integritu nebo důvěrnost citlivých či důležitých dat nebo funkcí. Podléhá povinnému hlášení.

Zranitelnost
Slabina, snížená odolnost nebo chyba produktu, kterou lze zneužít v rámci kybernetické hrozby.

Cybrela

Chcete připravit na splnění požadavků CRA?

Posoudíme, jestli CRA dopadá na vaše produkty, pomůžeme vám určit roli i kategorii produktu, nastavit proces hlášení a připravit dokumentaci k prokázání shody, která obstojí při kontrole. Kontaktujte náš tým.

Tobiáš Trnka

Konzultant informační bezpečnosti Cybrela
a odborný garant e-booku Cyber Resilience Act

E-MAIL
info@cybrela.com

VÍCE NA
www.cybrela.com

Cybrela

Vaši konzultanti informační bezpečnosti