

## Často kladené otázky týkajúce sa aktu o kybernetickej odolnosti

Akt o kybernetickej odolnosti ([nariadenie \(EÚ\) 2024/2847](#)) stanovuje pravidlá pre uvádzanie produktov s digitálnymi prvkami na trh s cieľom zabezpečiť ich kybernetickú bezpečnosť, základné požiadavky kybernetickej bezpečnosti pri navrhovaní, vývoji a výrobe, ako aj procesy riešenia zraniteľnosti, povinnosti hospodárskych subjektov v súvislosti s týmito produktmi a pravidlá týkajúce sa dohľadu nad trhom a presadzovania práva.

Tento predbežný súbor technických často kladených otázok (FAQ), ktorý bol uverejnený približne dva roky pred nadobudnutím účinnosti aktu o kybernetickej odolnosti (CRA), má pomôcť zainteresovaným stranám pri vykonávaní CRA. Často kladené otázky nemajú za cieľ vyčerpávajúco pokryť rozsah pôsobnosti CRA, ale skôr reagovať na opakujúce sa otázky, ktoré služby Komisie zhromaždili od nadobudnutia účinnosti CRA. Ide o „živý dokument“, ktorý bude v prípade potreby aktualizovaný.

Tento dokument pripravili služby Komisie a nemal by sa považovať za reprezentatívny pre oficiálne stanovisko Európskej komisie. Odpovede na často kladené otázky v žiadnom prípade nerozširujú práva a povinnosti vyplývajúce z platných právnych predpisov ani nezavádzajú žiadne dodatočné požiadavky. Vyjadrené názory nie sú záväzné a nemôžu predurčovať žiadne budúce opatrenia, ktoré Európska komisia môže prijať, vrátane potenciálnych stanovísk pred Súdnym dvorom Európskej únie, ktorý je kompetentný na autoritatívne výklad práva Únie.

Komisia tiež prijala usmernenia v súlade s článkom 26 CRA.

| FAQ Verzia | Dátum      | Zmeny                                                       |
|------------|------------|-------------------------------------------------------------|
| 1.0        | 03/12/2025 | Nové                                                        |
| 1.1        | 17/12/2025 | Upozornenie o autorských právach; drobné formátovacie chyby |
| 1.2        | 16/01/2026 | Drobná oprava v bode 6.2                                    |
| 1.3        | 01/07/2026 | Vypustenie pododdielu 4.6                                   |
| 1.4        | 04/09/2026 | Pridanie FAQ 5.5                                            |

© European Union, 2025



Politika opätovného použitia dokumentov Európskej komisie sa vykonáva na základe rozhodnutia Komisie 2011/833/EÚ z 12. decembra 2011 o opätovnom používaní dokumentov Komisie (Ú. v. EÚ L 330, 14.12.2011, s. 39). Pokiaľ nie je uvedené inak, opätovné použitie tohto dokumentu je autorizované na základe licencie Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>). To znamená, že opätovné použitie je autorizované za podmienky, že sa uvedie príslušný zdroj a všetky zmeny.

Zdroj: © European Union, 2025.

Originálny dokument: FAQs on the Cyber Resilience Act.

Preklad do slovenského jazyka: Národný bezpečnostný úrad, 2026.

Dokument je založený na diele © European Union, ktoré je licencované pod licenciou Creative Commons Attribution 4.0 International (CC BY 4.0).

Tento dokument predstavuje slovenský preklad/adaptáciu originálneho dokumentu. Preklad vyhotovil Národný bezpečnostný úrad. Európska únia, a Komisia tento preklad nevytvorila, neschválila ani neendordzuje.

Originál: <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions>

Licencia: <https://creativecommons.org/licenses/by/4.0/>

## Obsah

|                                                                                                                                    |    |
|------------------------------------------------------------------------------------------------------------------------------------|----|
| 1 Rozsah pôsobnosti .....                                                                                                          | 7  |
| 1.1 Kedy spadá produkt s digitálnymi prvkami do pôsobnosti aktu o kybernetickej odolnosti? .....                                   | 7  |
| 1.2 Čo je produkt s digitálnymi prvkami? Sú samostatné softvérové alebo firmvérové produkty produktmi s digitálnymi prvkami? ..... | 7  |
| 1.3 Čo je priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti? .....                            | 8  |
| 1.4 Vzťahuje sa CRA na produkty s digitálnymi prvkami, ktoré boli uvedené na trh pred 11. decembrom 2027? .....                    | 10 |
| 1.5 Vzťahuje sa CRA na produkty, ktoré sú určené výlučne na vlastné použitie? .....                                                | 11 |
| 1.6 Môžu výrobcovia uvádzať na trh verzie softvéru, ktoré nie sú súladné, na testovanie? .....                                     | 11 |
| 1.7 Môžu výrobcovia udržiavať verejne prístupné archívy softvéru? .....                                                            | 12 |
| 1.8 Sú produkty určené na použitie na účely národnej bezpečnosti alebo obrany vylúčené z CRA? .....                                | 12 |
| 1.9 Existujú produkty s digitálnymi prvkami, na ktoré sa vzťahujú iné právne predpisy Únie a ktoré sú vyňaté z CRA? .....          | 12 |
| 2 Vzájomné pôsobenie s inými právnymi predpismi .....                                                                              | 14 |
| 2.1 Nariadenie (EÚ) 2018/1139 o spoločných pravidlách v oblasti civilného letectva .....                                           | 14 |
| 2.1.1 Vzťahuje sa CRA aj na produkty, ktoré patria do pôsobnosti nariadenia (EÚ) 2018/1139? .....                                  | 14 |
| 2.2 Smernica (EÚ) 2014/90 o námornom zariadení .....                                                                               | 14 |
| 2.2.1 Sú produkty, ktoré patria do pôsobnosti smernice (EÚ) 2014/90, tiež zahrnuté v CRA? .....                                    | 14 |
| 2.3 Smernica o zodpovednosti za produkty (EÚ) 2024/2853 .....                                                                      | 15 |
| 2.3.1 Aký je vzájomný vzťah medzi CRA a smernicou o zodpovednosti za produkty? .....                                               | 15 |
| 2.4 Nariadenie o strojových zariadeniach (nariadenie (EÚ) 2023/1230) .....                                                         | 15 |
| 2.4.1 Aký je vzťah medzi CRA a nariadením o strojových zariadeniach? .....                                                         | 15 |
| 2.4.2 Mal by produkt spĺňať požiadavky CRA aj MR v oblasti kybernetickej bezpečnosti? .....                                        | 17 |
| 2.4.3 Mal by výrobca zabezpečiť posudzovanie zhody produktu prostredníctvom postupov stanovených v CRA aj MR? .....                | 17 |
| 2.5 Nariadenie o všeobecnej bezpečnosti produktov (EÚ) 2023/988 .....                                                              | 17 |

|                                                                                                                                                                          |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 2.5.1 Aká je vzájomná súvislosť medzi CRA a nariadením o všeobecnej bezpečnosti produktov.....                                                                           | 17 |
| 2.5.2 Musí produkt s digitálnymi prvkami spĺňať požiadavky CRA aj GPSR? .....                                                                                            | 18 |
| 2.6 Smernica o rádiových zariadeniach 2014/53/EÚ a delegované nariadenie Komisie (EÚ) 2022/30 .....                                                                      | 18 |
| 2.6.1 Aký je vzťah medzi CRA a smernicou o rádiových zariadeniach? .....                                                                                                 | 18 |
| 2.7 Nariadenie o európskom priestore pre zdravotné údaje (nariadenie (EÚ) 2025/327) .                                                                                    | 19 |
| 2.7.1 Aký je vzťah medzi CRA a nariadením o európskom priestore pre zdravotné údaje .....                                                                                | 19 |
| 2.7.2 Mal by produkt spĺňať požiadavky CRA aj nariadenia EHDS? .....                                                                                                     | 19 |
| 2.7.3 Mal by výrobca zabezpečiť posudzovanie zhody produktu prostredníctvom postupov stanovených v nariadení CRA aj v nariadení EHDS? .....                              | 19 |
| 2.7.4 Mal by výrobca vypracovať samostatné EÚ vyhlásenia o zhode podľa jednotlivých právnych aktov Únie?.....                                                            | 20 |
| 2.8 Všeobecné nariadenie o ochrane údajov (nariadenie (EÚ) 2016/679) .....                                                                                               | 20 |
| 2.8.1 Aký je vzťah medzi CRA a nariadením o všeobecnej ochrane údajov?.....                                                                                              | 20 |
| 2.9 Akt o údajoch (nariadenie (EÚ) 2023/2854).....                                                                                                                       | 21 |
| 2.9.1 Aká je vzájomná súvislosť medzi CRA a aktom o údajoch? .....                                                                                                       | 21 |
| 2.9.2 Ako požiadavky na produkty s digitálnymi prvkami podľa CRA zohľadňujú povinnosti sprístupňovať údaje používateľom alebo tretím stranám podľa aktu o údajoch? ..... | 21 |
| 2.9.3 Mal by výrobca prepracovať svoje produkty, aby vyhovovali požiadavkám DA a CRA? .....                                                                              | 22 |
| 3 Dôležité a kritické produkty .....                                                                                                                                     | 23 |
| 3.1 Určenie, či je produkt s digitálnymi prvkami dôležitým alebo kritickým produktom?..                                                                                  | 23 |
| 3.2 Stáva sa produkt dôležitým alebo kritickým, ak sa dôležitý alebo kritický produkt s digitálnymi prvkami integruje do iného produktu s digitálnymi prvkami? .....     | 23 |
| 3.3 Ovplyvňuje klasifikácia produktu ako dôležitého alebo s kritického posudzovanie rizika výrobcom? .....                                                               | 23 |
| 3.4 Znamená prítomnosť viacerých funkcií, že produkt nemá základnú funkcionality dôležitého alebo kritického produktu?.....                                              | 24 |
| 4 Povinnosti výrobcu.....                                                                                                                                                | 26 |
| 4.1 Prístup založený na riziku a posudzovanie rizika .....                                                                                                               | 26 |
| 4.1.1 Čo CRA vyžaduje od posúdenia kybernetickobezpečnostných rizík výrobcu?.....                                                                                        | 26 |
| 4.1.2 Vyžaduje CRA konkrétnu metodiku posudzovania rizika? .....                                                                                                         | 27 |

|                                                                                                                                                                                                                              |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.1.3 Musí výrobca implementovať všetky základné požiadavky? .....                                                                                                                                                           | 27 |
| 4.1.4 Čo je zamýšľaný účel a odôvodnene predvídateľné použitie a aký vplyv majú na posúdenie kybernetickobezpečnostného rizika?.....                                                                                         | 28 |
| 4.1.5 Čo je odôvodnene predvídateľné nesprávne použitie a aký vplyv má na posúdenie kybernetickobezpečnostného rizika? .....                                                                                                 | 30 |
| 4.1.6 Aký vplyv má predpokladaná dĺžka používania produktu na posúdenie kybernetickobezpečnostného rizika výrobcu?.....                                                                                                      | 31 |
| 4.1.7 Aký je vzťah medzi harmonizovanými normami a posúdením kybernetickobezpečnostného rizika výrobcu?.....                                                                                                                 | 31 |
| 4.1.8 Čo musí výrobca zahrnúť do technickej dokumentácie, ktorá má byť k dispozícii orgánom dohľadu nad trhom, pokiaľ ide o posúdenie kybernetickobezpečnostného rizika? .....                                               | 32 |
| 4.2 Základné požiadavky týkajúce sa produktov (príloha I, časť I) .....                                                                                                                                                      | 33 |
| 4.2.1 Aké technické opatrenia musí výrobca zaviesť? .....                                                                                                                                                                    | 33 |
| 4.2.2 Ako môže výrobca zabezpečiť, aby produkt neobsahoval žiadnu zraniteľnosť? ....                                                                                                                                         | 34 |
| 4.2.3 Ako by mali výrobcovia postupovať v prípade známych zneužívateľných zraniteľností, ktoré je možné zneužiť a ktoré boli zistené po uvedení produktu na trh, ale predtým, ako sa dostal k konečnému používateľovi? ..... | 35 |
| 4.2.4 Ako funguje požiadavka zabezpečenia na úrovni štandardného nastavenia (secure by default)? .....                                                                                                                       | 35 |
| 4.2.5 Kedy je produkt „vyrobený na mieru“? Aká dokumentácia sa v týchto prípadoch vyžaduje? .....                                                                                                                            | 36 |
| 4.3 Povinnosti v oblasti riešenia zraniteľností (príloha I, časť II) .....                                                                                                                                                   | 37 |
| 4.3.1 Sú výrobcovia povinní aplikovať záplaty na všetky zraniteľnosti, ktoré boli zistené počas obdobia podpory? .....                                                                                                       | 37 |
| 4.3.2 Musí výrobca riešiť a odstraňovať zraniteľnosti vo všetkých verziách softvérového produktu?.....                                                                                                                       | 38 |
| 4.3.3 Je výrobca zodpovedný za inštaláciu bezpečnostných aktualizácií používateľmi produktu?.....                                                                                                                            | 39 |
| 4.3.4 Musí výrobca stiahnuť produkt z trhu, ak nedokáže odstrániť zraniteľnosť?.....                                                                                                                                         | 40 |
| 4.3.5 Ako by mali výrobcovia zabezpečiť oddelenie aktualizácií bezpečnosti a funkcionáľit, najmä ak aktualizácie slúžia obom účelom? .....                                                                                   | 41 |
| 4.3.6 Ako by sa mali riešiť a odstraňovať zraniteľnosti v integrovaných komponentoch? .....                                                                                                                                  | 42 |

|                                                                                                                                                                                           |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.3.7 Aký vplyv má koniec obdobia podpory integrovanej súčasti na súlad produktu s CRA? .....                                                                                             | 43 |
| 4.4 Požiadavky na náležitú starostlivosť pri integrácii komponentov.....                                                                                                                  | 44 |
| 4.4.1 Čo CRA predpisuje pri integrácii komponentov? .....                                                                                                                                 | 44 |
| 4.4.2 Aká je primeraná úroveň náležitej starostlivosti? .....                                                                                                                             | 45 |
| 4.4.3 Aby výrobca konal s náležitou starostlivosťou, mal by integrovať iba komponenty, ktoré nesú označenie CE? .....                                                                     | 46 |
| 4.4.4 Ako by mali výrobcovia vykonávať náležitú starostlivosť v súvislosti s komponentmi s otvoreným zdrojovým kódom, na ktoré sa CRA nevzťahuje? .....                                   | 46 |
| 4.5 Obdobie podpory.....                                                                                                                                                                  | 47 |
| 4.5.1 Aké kritéria by mal výrobca zohľadniť pri určení obdobia podpory produktu? .....                                                                                                    | 47 |
| 4.5.2 Existuje minimálne obdobie podpory? .....                                                                                                                                           | 48 |
| 4.5.3 Môže výrobca pokračovať v predaji produktov bez obdobia podpory? .....                                                                                                              | 49 |
| 5 Povinnosti hlásenia výrobcov.....                                                                                                                                                       | 50 |
| 5.1 Ako sa môže výrobca dozvedieť o aktívne zneužívanej zraniteľnosti alebo závažnom incidente? .....                                                                                     | 50 |
| 5.2 Musí výrobca urobiť hlásenie o zraniteľnostiach typu zero-day? .....                                                                                                                  | 51 |
| 5.3 Musí výrobca vykonávať hlásenie aktívne zneužívaných zraniteľností alebo závažných incidentov týkajúcich sa produktov, ktoré boli uvedené na trh pred začatím uplatňovania CRA? ..... | 51 |
| 5.4 Ak je aktívne zneužívaná zraniteľnosť obsiahnutá v komponente tretej strany, sú všetci výrobcovia, ktorí túto komponentu integrujú, povinní hlásiť to? .....                          | 52 |
| 5.5 Podliehajú správcovia softvéru s otvoreným zdrojovým kódom nahlasovacím povinnostiam podľa CRA? .....                                                                                 | 53 |
| 6 Posudzovanie zhody.....                                                                                                                                                                 | 54 |
| 6.1 Čo je modul A? Ako funguje? Aké činnosti posudzovania zhody sa očakávajú pri samohodnotení? .....                                                                                     | 54 |
| 6.2 Čo je modul B+C? Ako funguje? .....                                                                                                                                                   | 55 |
| 6.3 Čo je modul H? Ako funguje? .....                                                                                                                                                     | 56 |
| 6.4 Sú výrobcovia povinní zabezpečiť zhodu „existujúcich“ typov produktov? .....                                                                                                          | 57 |
| 6.5 Akú metodiku hodnotenia by mal výrobca použiť? .....                                                                                                                                  | 58 |
| 6.6 Čo je technická dokumentácia? .....                                                                                                                                                   | 58 |
| 6.7 Čo je označenie CE? .....                                                                                                                                                             | 58 |
| 6.8 Čo je vyhlásenie o zhode? .....                                                                                                                                                       | 59 |

|                                                                                                                                                                         |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 6.9 Čo sú notifikované osoby? .....                                                                                                                                     | 59 |
| 6.10 Kedy budú pripravené harmonizované normy na podporu súladu s CRA? .....                                                                                            | 60 |
| 7 Prechodné obdobie.....                                                                                                                                                | 61 |
| 7.1 Kedy sa začne CRA uplatňovať? .....                                                                                                                                 | 61 |
| 7.2 Výrobca vyvinie produkt predtým, ako sa začne uplatňovať CRA. Môže pokračovať vo výrobe produktov identických s týmto produktom aj po začatí uplatňovania CRA?..... | 61 |
| 7.3 Môže výrobca uvádzať na trh produkty s digitálnymi prvkami vyvinutými počas prechodného obdobia, ktoré obsahujú komponenty, ktoré nemajú označenie CE? .....        | 62 |
| 7.4 Môže výrobca integrovať komponenty, ktoré sú dôležitými alebo kritickými produktmi s digitálnymi prvkami, ktoré nespĺňajú harmonizované normy? .....                | 62 |
| 7.5 Sú distribútori povinní zabezpečiť súlad produktov s digitálnymi prvkami, ktoré boli uvedené na trh pred 11. decembrom 2027?.....                                   | 63 |

# 1 Rozsah pôsobnosti

## 1.1 Kedy spadá produkt s digitálnymi prvkami do pôsobnosti aktu o kybernetickej odolnosti?

Akt CRA sa vzťahuje na *produkty s digitálnymi prvkami, ktoré sú dostupné na trhu a ktorých zamýšľaný účel alebo odôvodnené predpokladané použitie zahŕňa priame alebo nepriame logické alebo fyzické pripojenie k zariadeniu alebo sieti*“ (článok 2 ods. 1), s výnimkou produktov s digitálnymi prvkami, ktoré sú vyňaté z jeho pôsobnosti, ako je uvedené v článku 2 ods. 2, ods. 3 a ods. 4.

Tri kumulatívne prvky pomáhajú pochopiť, či sa na produkt s digitálnymi prvkami vzťahuje CRA:

- či spĺňa definíciu produktu s digitálnymi prvkami (pozri tiež 1.2 *Čo je produkt s digitálnymi prvkami? Sú samostatné softvérové alebo firmvérové produkty produktmi s digitálnymi prvkami?*);
- či je dostupný na trhu;
- či jeho zamýšľaný účel alebo odôvodnené predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti (pozri tiež 1.3 *Čo je priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti?* a 4.1.4 *Čo je zamýšľaný účel a odôvodnené predvídateľné použitie a ako ovplyvňujú posudzovanie kybernetickobezpečnostného rizika?*).

## 1.2 Čo je produkt s digitálnymi prvkami? Sú samostatné softvérové alebo firmvérové produkty produktmi s digitálnymi prvkami?

Produkt s digitálnymi prvkami je definovaný ako *„softvérový alebo hardvérový produkt a jeho riešenia spracovania údajov na diaľku, vrátane softvérových alebo hardvérových komponentov, ktoré sa uvádzajú na trh samostatne“* (článok 3 ods. 1).

Spracovanie údajov na diaľku sa vymedzuje ako *„spracovanie údajov na diaľku, pre ktoré je softvér navrhnutý a vyvinutý výrobcom alebo na zodpovednosť výrobcu a ktorého neexistencia by bránila produktu s digitálnymi prvkami plniť jednu z jeho funkcií“* (článok 3 ods. 2).

Softvér je definovaný ako *„časť elektronického informačného systému, ktorý pozostáva z počítačového kódu“* (článok 3 ods. 4).

Hardvér je definovaný ako *„fyzický elektronický informačný systém alebo jeho časti so schopnosťou spracúvať, uchovávať alebo prenášať digitálne údaje“* (článok 3 ods. 5).

Elektronický informačný systém je definovaný ako *„systém vrátane elektrických alebo elektronických zariadení, ktorý je schopný spracúvať, uchovávať alebo prenášať digitálne údaje“* (článok 3 ods. 7).

- samostatný softvér, ktorý je možné stiahnuť a nainštalovať do zariadenia, napr. mobilná aplikácia, ktorú je možné stiahnuť prostredníctvom obchodu s aplikáciami, alebo program, ktorý je možné stiahnuť prostredníctvom webovej stránky;
- softvér určený na integráciu do elektronického informačného systému, ak je uvádzaný na trh samostatne, napr. firmvér alebo softvér určený na zabudovanie do hardvérových zariadení;
- softvér, ktorý sa uvádza na trh spolu s hardvérovým produktom, bez ohľadu na to, či je vopred nainštalovaný v hardvéri, napr. ovládače potrebné na správne fungovanie tlačiarne, operačný systém v notebooku alebo nástroje používané na navrhovanie a programovanie FPGA;
- Rôzne typy hardvéru, ako napríklad základné komponenty (napr. integrované obvody, základné dosky, senzory); spotrebné zariadenia (napr. smartfóny, notebooky, inteligentné chladničky); komplexné zariadenia (napr. priemyselné zariadenia IoT, stroje).

Produkt s digitálnymi prvkami zahŕňa aj riešenia spracovania údajov na diaľku.

Ako sa uvádza v odôvodnení 12, webové stránky, ktoré nepodporujú funkcionality produktu s digitálnymi prvkami, nie sú samy osebe produktmi s digitálnymi prvkami. Webové stránky, ktoré poskytujú podporu funkcionality produktu s digitálnymi prvkami, môžu spadať do pôsobnosti CRA v rozsahu, v akom spĺňajú definíciu spracovania údajov na diaľku (článok 3 ods. 2).

Podobne služby, ako napríklad samostatný softvér ako služba (SaaS) alebo iné cloudové riešenia navrhnuté a vyvinuté mimo zodpovednosti výrobcu produktu s digitálnymi prvkami, nie sú samy osebe produktmi s digitálnymi prvkami. Ak však takéto služby spĺňajú definíciu spracúvania údajov na diaľku, spadajú do pôsobnosti CRA.

Pojem spracovanie údajov na diaľku bude súčasťou samostatných usmernení.

### 1.3 Čo je priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti?

Fyzické pripojenie je definované ako „*je spojenie medzi elektronickými informačnými systémami alebo komponentmi realizované s použitím fyzických prostriedkov vrátane elektrických, optických alebo mechanických rozhraní, vodičov alebo rádiových vĺn*“ (článok 3 ods. 9).

Logické pripojenie je definované ako „*virtuálna forma dátového spojenia realizovaná prostredníctvom softvérového rozhrania*“ (článok 3 ods. 8).

Nepriame pripojenie je definované ako „*pripojenie k zariadeniu alebo sieti, ktoré sa nevykonáva priamo, ale skôr ako súčasť väčšieho systému, ktorý je priamo pripojiteľný k takémuto zariadeniu alebo sieti*“ (článok 3 ods. 10).

*Za určitých podmienok môžu všetky produkty s digitálnymi prvkami integrované vo väčšom elektronickom informačnom systéme alebo pripojené k takému systému slúžiť ako vektor útoku škodlivých subjektov. V dôsledku toho aj hardvér a softvér považovaný za menej kritický môže uľahčiť počiatočné ohrozenie zariadenia alebo siete, ktoré umožní škodlivým subjektom získať privilegovaný prístup do systému alebo sa pohybovať laterálne naprieč systémami. Výrobcovia by preto mali zabezpečiť, aby všetky produkty s digitálnymi prvkami boli navrhnuté a vyvíjané v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení. Táto povinnosť sa týka produktov, ktoré možno pripojiť fyzicky cez hardvérové rozhranie, ako aj produktov, ktoré sa pripájajú logicky, napríklad pomocou sieťových zásuviek, dátovodov, súborov, aplikačných programovacích rozhraní alebo iných druhov softvérového rozhrania. Keďže kybernetické hrozby môžu šíriť rôzne produkty s digitálnymi prvkami pred dosiahnutím určitého cieľa, napríklad zrežaním viacerých zneužití zraniteľnosti, výrobcovia by mali zaistiť kybernetickú bezpečnosť aj pre produkty s digitálnymi prvkami, ktoré sú k iným zariadeniam alebo sieťam pripojené iba nepriamo (odôvodnenie 9).*

Fyzické pripojenie môže byť priame, napríklad keď sa produkt s digitálnymi prvkami pripája prostredníctvom kábla USB (napr. tlačiareň pripájaná k prenosnému počítaču); prostredníctvom ethernetového kábla (napr. pripojenie počítača k smerovaču); prostredníctvom optického kábla (napr. pripojenie optického smerovača k sieti poskytovateľa internetových služieb) alebo medeného kábla (napr. priemyselná zbernica, ako je PROFIBUS, pripájajúca senzor k programovateľnému logickému kontroléru); prostredníctvom rádiových vĺn, napríklad prostredníctvom Wi-Fi (napr. terminál v mieste predaja (POS), ktorý sa pripája k sieti obchodu), Bluetooth (napr. Bluetooth slúchadlá pripojené k smartfónu), technológia komunikácie v blízkosti (napr. dverový zámok pripojený k NFC tagu).

Logické pripojenie môže byť priame, napríklad keď produkt s digitálnymi prvkami iniciuje alebo spravuje komunikáciu s inými zariadeniami alebo sieťami (napr. prehliadač, ktorý nadviaže HTTPS reláciu na prístup k webovej stránke, alebo e-mailový klient, ktorý iniciuje výmenu IMAP alebo SMTP); alebo môže byť nepriame, keď produkt s digitálnymi prvkami sám neiniciuje komunikáciu, ale beží na hostiteľskom systéme, ktorý to robí (napr. offline textový editor alebo kalkulačka, ktoré sú nepriamo pripojené prostredníctvom operačného systému).

Produkty s digitálnymi prvkami môžu mať súčasne viac ako jednu formu dátového pripojenia k iným zariadeniam alebo sieťam.

Na druhej strane, produkt s digitálnymi prvkami nemá priame ani nepriame dátové pripojenie, ak jeho zamýšľaný účel alebo odôvodnene predvídateľné použitie nezahŕňa takéto pripojenie k iným zariadeniam alebo sieťam. Medzi produkty, ktoré nespádajú do pôsobnosti CRA, patria napríklad:

- umývačka riadu s integrovaným firmvérom, ktorý je určený na riadenie cyklu umývania riadu, ale bez možnosti pripojenia k iným zariadeniam alebo sieťam;
- základná kalkulačka s integrovaným firmvérom vykonávajúcim aritmetické operácie, ale bez možnosti pripojenia k iným zariadeniam alebo sieťam;

- elektronická hračka s integrovaným firmvérom, ktorá prehráva vopred nahraté svetelné a zvukové efekty, ale nemá schopnosť pripojiť sa k iným zariadeniam alebo sieťam;
- kávovar s integrovaným firmvérom, ktorý nastavuje čas prípravy alebo silu kávy prostredníctvom panela pre riadenie, ale bez možnosti pripojenia k iným zariadeniam alebo sieťam
- elektrická zubná kefka s bezdrôtovou nabíjacou stanicou, ale bez možnosti pripojenia k iným zariadeniam alebo sieťam.<sup>1</sup>

## 1.4 Vzťahuje sa CRA na produkty s digitálnymi prvkami, ktoré boli uvedené na trh pred 11. decembrom 2027?

*„Na produkty s digitálnymi prvkami, ktoré boli uvedené na trh pred 11. decembrom 2027 sa vzťahujú požiadavky stanovené v tomto nariadení len vtedy, ak sú tieto produkty od uvedeného dátumu predmetom podstatnej úpravy“ (článok 69 ods. 2).*

*„Odchylne od odseku 2 tohto článku sa povinnosti stanovené v článku 14 uplatňujú na všetky produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti tohto nariadenia a boli uvedené na trh pred 11. decembrom 2027“ (článok 69 ods. 3).*

CRA sa vzťahuje na produkty uvedené na trh pred 11. decembrom 2027 len v prípade, ak sú tieto produkty po tomto dátume podstatne upravené. Pozri tiež 7.1 *Kedy sa CRA začne uplatňovať?*

Napríklad výrobca uvedie na trh inteligentný televízor v polovici roka 2027. Výrobca nie je povinný dodržiavať CRA pre tento produkt s digitálnymi prvkami. V roku 2028 vydá aktualizáciu softvéru, ktorá sa nepovažuje za podstatnú úpravu, s cieľom opraviť chybu, ktorá spôsobuje zlyhanie aplikácií bežiacich na televízore po určitom čase používania. Výrobca nie je povinný uviesť inteligentný televízor do zhody s CRA, pretože by to nebola podstatná úprava.

V roku 2029 výrobca vydá aktualizáciu softvéru, ktorá sa považuje za podstatnú úpravu, napríklad preto, že mení pôvodné zamýšľané funkcie tým, že umožňuje inteligentnému televízoru riadenie inteligentných domáckych systémov. V takom prípade je výrobca povinný uviesť inteligentný televízor do súladu s CRA.

Pozri tiež 7.2 *Výrobca vyvíja typ produktu pred uplatnením CRA. Môže pokračovať vo výrobe produktov identických s týmto typom po uplatnení CRA?*

Odchýlka od tohto všeobecného pravidla sa však vzťahuje na oznamovacie povinnosti stanovené v článku 14. Výrobcovia sú povinní notifikovať aktívne zneužívané zraniteľnosti a závažné incidenty, ktoré majú vplyv na bezpečnosť produktu s digitálnymi prvkami, pre všetky produkty s digitálnymi prvkami, ktoré patria do pôsobnosti CRA, vrátane produktov, ktoré boli uvedené na trh pred 11. decembrom 2027 (článok 69 ods. 3). Ďalšie vysvetlenie

<sup>1</sup> Firmware uvedený v týchto príkladoch však môže spadať do pôsobnosti CRA, ak je uvádzaný na trh samostatne.

nájdete v bode 5.3. *Musí výrobca vykonávať hlásenie aktívne zneužívaných zraniteľností alebo závažných incidentov týkajúce sa produktov, ktoré boli uvedené na trh pred uplatnením CRA?*

## 1.5 Vzťahuje sa CRA na produkty, ktoré sú určené výlučne na vlastné použitie?

*„Uvedenie na trh sa nepovažuje za zrealizované vtedy, keď výrobok je vyrobený na vlastné použitie“ (Modrá príručka o vykonávaní pravidiel EÚ týkajúcich sa produktov 2022<sup>2</sup>, oddiel 2.3).*

CRA sa uplatňuje, keď sa produkt s digitálnymi prvkami uvádza na trh (a v následných prípadoch sprístupnenia tohto produktu). Modrá príručka o vykonávaní pravidiel EÚ týkajúcich sa výrobkov 2022 (ďalej len „modrá príručka“) objasňuje, že uvedenie na trh sa nepovažuje za uskutočnené, ak je produkt vyrobený pre vlastné použitie.<sup>3</sup>

Napríklad vývojové a konfiguračné nástroje vyvinuté výrobcom produktu s digitálnymi prvkami pre vlastné použitie nespádajú do pôsobnosti CRA, pokiaľ nie sú uvedené na trh ako samostatné produkty.

## 1.6 Môžu výrobcovia uvádzať na trh verzie softvéru, ktoré nie sú súladné, na testovanie?

*Členské štáty nesmú brániť sprístupňovaniu nedokončeného softvéru, ktorý nie je v súlade s týmto nariadením, na trhu za predpokladu, že softvér sa sprístupní len na obmedzený čas potrebný na účely testovania s viditeľným označením, ktoré jasne uvádza, že nie je v súlade s týmto nariadením a že nebude dostupný na trhu na iné účely, než je testovanie.*

Výrobcovia môžu uvádzať na trh nesúladný nedokončený softvér na účely skúšania, napríklad alfa verzie, beta verzie alebo kandidátske verzie, za predpokladu, že tento softvér je sprístupnený len na dobu potrebnú na jeho skúšanie a zhromažďovanie spätnej väzby a že je doplnený viditeľným označením, ktoré poukazuje na jeho nesúlad.

Odôvodnenie 37 ďalej objasňuje, že „výrobcovia by mali zabezpečiť, aby sa softvér sprístupnený podľa týchto podmienok uvoľnil iba po posúdení rizika a aby v najväčšej možnej miere spĺňal požiadavky bezpečnosti týkajúce sa vlastností produktov s digitálnymi prvkami, ktoré stanovuje toto nariadenie. Výrobcovia by takisto mali v najväčšej možnej miere spĺňať požiadavky na riešenia zraniteľností. Výrobcovia by nemali nútiť používateľov, aby prešli na vyššie verzie uvoľnené iba na účely testovania“.

<sup>2</sup> Oznámenie Komisie – „Modrá príručka“ o vykonávaní pravidiel EÚ týkajúcich sa produktov 2022 (2022/C 247/01), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2022:247:FULL>

<sup>3</sup> To neplatí v prípade, ak harmonizačné právne predpisy Únie zahŕňajú produkty vyrobené na vlastné použitie. CRA však nezahŕňa produkty vyrobené na vlastné použitie.

## 1.7 Môžu výrobcovia udržiavať verejne prístupné archívy softvéru?

*Výrobcovia môžu viesť verejné softvérové archívy na zlepšenie prístupu používateľov k historickým verziám. V týchto prípadoch musia byť používatelia jasne a jednoducho dostupným spôsobom informovaní o rizikách spojených s používaním softvéru, ktorý už nie je podporovaný.*

Výrobcovia môžu udržiavať verejné archívy softvéru pre historické verzie svojich produktov s digitálnymi prvkami, ktoré už nie sú dostupné na trhu. Používatelia by mali byť jasne informovaní o rizikách, ktoré môžu vyplývať z používania softvéru, ktorý už nie je podporovaný.

## 1.8 Sú produkty určené na použitie na účely národnej bezpečnosti alebo obrany vylúčené z CRA?

*CRA „neuplatňuje na produkty s digitálnymi prvkami vyvinuté alebo upravené výlučne na účely národnej bezpečnosti alebo na účely obrany alebo na produkty osobitne určené na spracúvanie utajovaných skutočností.“ (článok 2 ods. 7).*

Ak produkt s digitálnymi prvkami nie je špecificky a výlučne vyvinutý alebo upravený na účely národnej bezpečnosti alebo obrany, alebo nie je špecificky navrhnutý na proces utajovaných informácií, spadá do pôsobnosti CRA. Takzvané produkty „dvojitého použitia“, ktoré majú civilné aj obranné využitie, preto podliehajú CRA, ak sú uvedené na trh, pokiaľ nie sú upravené výlučne na účely národnej bezpečnosti alebo obrany.

Členské štáty môžu podriaďiť produkty s digitálnymi prvkami, ktoré spadajú do pôsobnosti CRA, dodatočným požiadavkám kybernetickej bezpečnosti pri ich obstarávaní alebo používaní na špecifické účely, ak sú takéto požiadavky v súlade s povinnosťami členských štátov stanovenými v práve Únie a ak sú nevyhnutné a primerané na dosiahnutie týchto účelov, ako sa stanovuje v článku 5 ods. 1.

## 1.9 Existujú produkty s digitálnymi prvkami, na ktoré sa vzťahujú iné právne predpisy Únie a ktoré sú vyňaté z CRA?

CRA sa neuplatňuje na produkty s digitálnymi prvkami:

- na ktoré sa vzťahuje nariadenie (EÚ) 2017/745 o zdravotníckych pomôckach a nariadenie (EÚ) 2017/746 o zdravotníckych pomôckach na in vitro diagnostiku;
- na ktoré sa vzťahuje nariadenie (EÚ) 2019/2144 o požiadavkách na typové schvaľovanie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá, pokiaľ ide o ich všeobecnú bezpečnosť a ochranu cestujúcich vo vozidle a zraniteľných účastníkov cestnej premávky;

- certifikované v súlade s nariadením (EÚ) 2018/1139 o spoločných pravidlách v oblasti civilného letectva, ktorým sa zriaďuje Agentúra Európskej únie pre bezpečnosť letectva; pozri tiež oddiel 2.1 *nariadenia (EÚ) 2018/1139 o spoločných pravidlách v oblasti civilného letectva*.

CRA sa neuplatňuje ani na zariadenia, ktoré patria do pôsobnosti smernice 2014/90/EÚ o námorných zariadeniach; pozri tiež oddiel 2.2 *smernice (EÚ) 2014/90 o námorných zariadeniach*.

Delegované nariadenie (EÚ) 2025/1535 vylučuje z pôsobnosti CRA aj produkty s digitálnymi prvkami, ktoré spadajú do pôsobnosti nariadenia (EÚ) č. 168/2013 o schvaľovaní a dohľade nad trhom dvoj- alebo trojkolesových vozidiel a štvorkoliek, s výnimkou vozidiel kategórie L1e určených na šliapanie.

## 2 Vzájomné pôsobenie s inými právnymi predpismi

### 2.1 Nariadenie (EÚ) 2018/1139 o spoločných pravidlách v oblasti civilného letectva

#### 2.1.1 Vzťahuje sa CRA aj na produkty, ktoré patria do pôsobnosti nariadenia (EÚ) 2018/1139?

CRA aj nariadenie (EÚ) 2018/1139 (známe aj ako „základné nariadenie EASA“) stanovujú pravidlá uvádzania produktov na trh. CRA sa vzťahuje na produkty s digitálnymi prvkami, zatiaľ čo základné nariadenie EASA sa vzťahuje na letecké produkty, časti a vybavenie (vrátane softvéru).

Základné nariadenie EASA stanovuje základné požiadavky, vrátane požiadaviek na ochranu pred hrozbami pre informačnú bezpečnosť, a ukladá povinnosť certifikácie civilných lietadiel a súvisiacich produktov EASA v súlade s vykonávacím nariadením (EÚ) č. 748/2012, časť 21.

Od roku 2020 Európska agentúra pre bezpečnosť letectva (EASA) výslovne začlenila aspekty informačnej bezpečnosti do svojich pravidiel certifikácie zmenou a doplnením viacerých certifikačných špecifikácií a vydaním nových usmernení.

Na tomto základe článok 2 ods. 3 CRA vyníma produkty certifikované podľa nariadenia (EÚ) 2018/1139 z jeho pôsobnosti.

Produkty, ktoré spadajú do pôsobnosti nariadenia (EÚ) 2018/1139, ale nie sú certifikované podľa tohto nariadenia, ako napríklad drony v otvorenej kategórii (väčšina rekreačných činností s dronmi a komerčných činností s nízkym rizikom), však môžu spadať pod CRA (ak sú to produkty s digitálnymi prvkami a sú dostupné na trhu).

Ak sú komponenty určené na integráciu do produktov certifikovaných podľa nariadenia (EÚ) 2018/1139, ale tieto komponenty nie sú certifikované podľa uvedeného nariadenia, môžu sa na ne vzťahovať CRA (ak sú to produkty s digitálnymi prvkami a sú dostupné na trhu).

### 2.2 Smernica (EÚ) 2014/90 o námornom zariadení

#### 2.2.1 Sú produkty, ktoré patria do pôsobnosti smernice (EÚ) 2014/90, tiež zahrnuté v CRA?

CRA a smernica (EÚ) 2014/90 stanovujú pravidlá pre uvádzanie určitých produktov na trh: pre produkty s digitálnymi prvkami, resp. pre námorné vybavenie.

Podľa článku 2 ods. 4 sa CRA nevzťahuje na zariadenia, ktoré spadajú do pôsobnosti smernice (EÚ) 2014/90.

Zariadenia, ktoré spadajú do pôsobnosti smernice (EÚ) 2014/90, sú uvedené v prílohe k vykonávaciemu nariadeniu Komisie (EÚ) 2025/1533, pokiaľ ide o požiadavky na konštrukčný

návrh, konštrukciu a výkonnosť vybavenia námorných lodí a skúšobné normy pre toto vybavenie.

Ak sú však komponenty určené na integráciu do zariadení, ktoré patria do pôsobnosti smernice (EÚ) 2014/90, ale tieto komponenty nespádajú do pôsobnosti tejto smernice, môžu sa na ne vzťahovať CRA (ak sú to produkty s digitálnymi prvkami a sú dostupné na trhu).

## 2.3 Smernica o zodpovednosti za produkty (EÚ) 2024/2853

### 2.3.1 Aký je vzájomný vzťah medzi CRA a smernicou o zodpovednosti za produkty?

CRA smernica o zodpovednosti za produkty (PLD) majú odlišnú povahu a hoci sa navzájom dopĺňajú, nedochádza k ich právnemu prekryvaniu.

PLD stanovuje pravidlá zodpovednosti za chybné produkty, aby poškodené osoby mohli podať výrok za škodu, ak bola škoda spôsobená chybnými produktmi. Stanovuje zásadu, že výrobca produktu zodpovedá za škody spôsobené chybou svojho produktu bez ohľadu na zavinenie alebo nedbanlivosť (objektívna zodpovednosť).

Posudzovanie chybnosti produktu sa vykonáva na základe toho, či produkt poskytoval bezpečnosť, ktorú možno očakávať, alebo ktorú sa vyžaduje podľa práva Únie alebo vnútroštátneho práva. Posudzovanie chybnosti produktu sa musí vykonávať s prihliadnutím na všetky okolnosti, vrátane požiadaviek v oblasti kybernetickej bezpečnosti.

CRA napríklad stanovuje výrobcom osobitné povinnosti týkajúce sa bezpečnostných aktualizácií produktov s digitálnymi prvkami (príloha I).

Hoci PLD neukladá výrobcom žiadnu podstatnú povinnosť aktualizovať alebo modernizovať produkt, podľa PLD výrobca naďalej zodpovedá za akékoľvek chyby, ktoré vznikli aktualizáciou alebo modernizáciou produktu po jeho uvedení na trh. Alebo za akékoľvek chyby, ktoré vznikli po uvedení produktu na trh v dôsledku chýbajúcej aktualizácie alebo modernizácie.

## 2.4 Nariadenie o strojových zariadeniach (nariadenie (EÚ) 2023/1230)

### 2.4.1 Aký je vzťah medzi CRA a nariadením o strojových zariadeniach?

*Výrobcovia produktov patriacich do rozsahu pôsobnosti nariadenia Európskeho parlamentu a Rady (EÚ) 2023/1230, ktoré sú zároveň produktmi s digitálnymi prvkami v zmysle vymedzenia v tomto nariadení, by mali spĺňať základné požiadavky kybernetickej bezpečnosti stanovené v tomto nariadení, ako aj základné požiadavky na bezpečnosť a ochranu zdravia stanovené v nariadení (EÚ) 2023/1230. Základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení a určitými základnými požiadavkami stanovenými v nariadení (EÚ) 2023/1230 sa môžu riešiť podobné kybernetickobezpečnostné riziká. Dodržiavanie základných požiadaviek kybernetickej bezpečnosti stanovených v tomto nariadení by preto mohlo uľahčiť dodržiavanie základných požiadaviek na určité kybernetickobezpečnostné riziká*

*stanovené v nariadení (EÚ) 2023/1230, a to najmä požiadaviek na ochranu pred zneužitím a bezpečnosť a spoľahlivosť ovládacích systémov stanovených v oddieloch 1.1.9 a 1.2.1 prílohy III k uvedenému nariadeniu. Takéto synergie musí výrobca preukázať, napríklad uplatnením harmonizovaných noriem alebo iných technických špecifikácií, ktoré sa vzťahujú na príslušné základné požiadavky kybernetickej bezpečnosti, ak sú k dispozícii, na základe posúdenia rizík, ktoré sa vzťahuje na uvedené kybernetickobezpečnostné riziká. Výrobca by sa mal riadiť aj uplatniteľnými postupmi posudzovania zhody stanovenými v tomto nariadení a v nariadení (EÚ) 2023/1230. Komisia a európske normalizačné organizácie by v rámci prípravných prác na podporu vykonávania tohto nariadenia a nariadenia (EÚ) 2023/1230 a súvisiacich normalizačných postupov mali podporovať konzistentnosť spôsobu posudzovania kybernetickobezpečnostných rizík a toho, ako majú byť tieto riziká pokryté harmonizovanými normami, pokiaľ ide o príslušné základné požiadavky. Komisia a európske normalizačné organizácie by mali toto nariadenie zohľadniť najmä pri príprave a vypracovaní harmonizovaných noriem s cieľom uľahčiť vykonávanie nariadenia (EÚ) 2023/1230, najmä pokiaľ ide o aspekty kybernetickej bezpečnosti súvisiace s ochranou pred zneužitím a bezpečnosťou a spoľahlivosťou ovládacích systémov stanovených v oddieloch 1.1.9 a 1.2.1 prílohy III k uvedenému nariadeniu. Komisia by mala poskytnúť usmernenia na podporu výrobcov, na ktorých sa vzťahuje toto nariadenie a tiež aj nariadenie (EÚ) 2023/1230, najmä s cieľom uľahčiť preukazovanie dodržiavania príslušných základných požiadaviek stanovených v tomto nariadení a v nariadení (EÚ) 2023/1230 (odôvodnenie 53 CRA).*

Nariadenie o strojových zariadeniach (MR) sa bude uplatňovať od 20. januára 2027. V prílohe III stanovuje základné požiadavky na zdravie a bezpečnosť, pričom sa zaoberá aj kybernetickobezpečnostnými rizikami, ktoré môžu mať vplyv na bezpečnosť.

Nariadenie CRA aj nariadenie MR stanovujú pravidlá pre uvádzanie určitých produktov na trh. Kým nariadenie CRA sa vzťahuje na produkty s digitálnymi prvkami, nariadenie MR sa vzťahuje na stroje a súvisiace výrobky, s výnimkou určitých prípadov.

CRA stanovuje v prílohe I základné požiadavky kybernetickej bezpečnosti produktov s digitálnymi prvkami. MR stanovuje v prílohe III základné požiadavky na zdravie a bezpečnosť strojov a súvisiacich produktov, pričom sa zaoberá aj kybernetickobezpečnostnými rizikami, ktoré môžu mať vplyv na bezpečnosť (t. j. príloha III, oddiely 1.1.9 a 1.2.1).

Produkt môže byť zároveň produktom s digitálnymi prvkami v zmysle CRA, ako aj strojovým zariadením alebo súvisiacim produktom v zmysle MR. V takýchto prípadoch môže dôjsť k vzájomnému ovplyvňovaniu, ako je opísané v odôvodnení 53 CRA, medzi CRA a MR, pokiaľ ide o požiadavky kybernetickej bezpečnosti, ako je uvedené vyššie, a postupy posudzovania zhody, ako sú stanovené individuálne v CRA aj v MR.

Napríklad: určitý typ strojov v zmysle MR, ktoré sa môžu používať napríklad na balenie zeleniny pre supermarkety, môže obsahovať hardvér a softvér na zabezpečenie ich fungovania. V tomto zmysle môžu byť stroje na balenie potravín aj produktom s digitálnymi prvkami v zmysle CRA.

### 2.4.2 Mal by produkt spĺňať požiadavky CRA aj MR v oblasti kybernetickej bezpečnosti?

Produkt s digitálnymi prvkami v zmysle CRA môže byť zároveň aj strojovým zariadením alebo súvisiacim produktom v zmysle MR. V takýchto prípadoch bude musieť takýto produkt spĺňať požiadavky kybernetickej bezpečnosti CRA, ako aj MR. Požiadavky kybernetickej bezpečnosti stanovené v CRA a MR sú takej povahy, že súlad s požiadavkami kybernetickej bezpečnosti iba jedného z nariadení nemožno automaticky považovať za úplné splnenie požiadaviek druhého nariadenia.

Keďže však požiadavky kybernetickej bezpečnosti stanovené v CRA a MR môžu v niektorých aspektoch riešiť podobné riziká, súlad s CRA by mohol uľahčiť súlad s požiadavkami stanovenými v MR. Výrobcovia produktov, ktoré spadajú do pôsobnosti CRA aj MR, by však museli preukázať takéto potenciálne synergie na základe posudzovania rizika a napríklad s odvolaním sa na harmonizované normy alebo iné relevantné technické špecifikácie, ak sú k dispozícii.

### 2.4.3 Mal by výrobca zabezpečiť posudzovanie zhody produktu prostredníctvom postupov stanovených v CRA aj MR?

CRA aj MR stanovujú postupy posudzovania zhody pre príslušné produkty s digitálnymi prvkami (v článku 32 CRA) a stroje a súvisiace výrobky (v článku 25 MR).

V prípade produktu s digitálnymi prvkami v zmysle CRA, ktorý je zároveň strojom alebo súvisiacim produktom v zmysle MR, budú výrobcovia musieť zabezpečiť posudzovanie zhody prostredníctvom postupov stanovených individuálne v CRA aj v MR. Postupy posudzovania zhody stanovené v CRA a MR sú také povahy, že posúdenie zhody na základe postupu v jednom nástroji nemožno automaticky považovať za dostatočné na splnenie postupu, ktorý sa vyžaduje podľa druhého nástroja (pozri aj odôvodnenie 53 CRA).

## 2.5 Nariadenie o všeobecnej bezpečnosti produktov (EÚ) 2023/988

### 2.5.1 Aká je vzájomná súvislosť medzi CRA a nariadením o všeobecnej bezpečnosti produktov

CRA a nariadenie o všeobecnej bezpečnosti produktov (GPSR) stanovujú pravidlá pre uvádzanie produktov na trh, ale majú odlišný rozsah pôsobnosti, pokiaľ ide o produkty a aspekty, na ktoré sa vzťahujú, a požiadavky, ktoré stanovujú. Pokiaľ ide o produkty, na ktoré sa vzťahujú nariadenia, CRA sa vzťahuje len na produkty s digitálnymi prvkami, zatiaľ čo GPSR sa vzťahuje na všetky spotrebné produkty, pokiaľ neexistujú osobitné ustanovenia s rovnakým cieľom v rámci práva Únie, ktoré upravujú bezpečnosť príslušných produktov. Pokiaľ ide o požiadavky stanovené nariadeniami, CRA stanovuje požiadavky kybernetickej bezpečnosti, zatiaľ čo GPSR stanovuje bezpečnostné požiadavky na produkty.

## 2.5.2 Musí produkt s digitálnymi prvkami spĺňať požiadavky CRA aj GPSR?

Produkt s digitálnymi prvkami môže musieť spĺňať požiadavky CRA aj GPSR. Ak produkt s digitálnymi prvkami predstavuje aj iné riziká ako kybernetickobezpečnostné riziká, na ktoré sa vzťahuje CRA, tieto iné riziká môžu byť upravené inými právnymi predpismi EÚ, napríklad GPSR. Pokiaľ neexistuje žiadny predpis špecifický pre daný produkt, ktorý by reguloval tieto ďalšie riziká produktu s digitálnymi prvkami, na bezpečnostné aspekty týchto rizík sa vzťahuje GPSR (článok 11 CRA).

## 2.6 Smernica o rádiových zariadeniach 2014/53/EÚ a delegované nariadenie Komisie (EÚ) 2022/30

### 2.6.1 Aký je vzťah medzi CRA a smernicou o rádiových zariadeniach?

CRA sa vzťahuje na kategórie rádiových zariadení, ktoré patria do pôsobnosti delegovaného nariadenia (EÚ) 2022/30 prijatého na základe smernice o rádiových zariadeniach 2014/53/EÚ („delegované nariadenie RED“). CRA zahŕňa základné požiadavky kybernetickej bezpečnosti RED, ktoré sa stali uplatniteľnými prostredníctvom delegovaného nariadenia RED od 1. augusta 2025 a vzťahujú sa na kategórie rádiových zariadení, na ktoré sa vzťahuje delegované nariadenie RED, ak sú uvedené na trh 1. augusta 2025 alebo neskôr.

Na účely delegovaného nariadenia RED boli vyžiadané technické normy, ktoré sú uvedené v Úradnom vestníku Európskej únie v podpore príslušných základných požiadaviek RED (séria EN 18031). S cieľom zabezpečiť právnu jasnosť sa Komisia zameriava na zrušenie delegovaného nariadenia RED s účinnosťou od 11. decembra 2027<sup>4</sup>.

V takom prípade budú kategórie rádiových zariadení uvedené v delegovanom nariadení RED, ak budú uvedené na trh v období od 1. augusta 2025 do 10. decembra 2027, podliehať základným požiadavkám kybernetickej bezpečnosti RED, ktoré sa stali uplatniteľnými prostredníctvom delegovaného nariadenia RED. Naopak, ak sa tieto produkty uvedú na trh 11. decembra 2027 alebo neskôr, keď CRA začne platiť, budú tieto produkty podliehať základným požiadavkám CRA.

Zrušenie delegovaného nariadenia RED s účinnosťou od 11. decembra 2027 nebude mať vplyv na dohľad nad trhom a riadenie trhu Únie podľa smernice 2014/53/EÚ o rádiových zariadeniach, pokiaľ ide o súlad rádiových zariadení so základnými požiadavkami kybernetickej bezpečnosti RED, ak boli alebo sú tieto rádiové zariadenia uvedené na trh EÚ v období od 1. augusta 2025 do 10. decembra 2027 a podliehajú niektorej z týchto základných požiadaviek.

---

<sup>4</sup> [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14766-Kybernetická-bezpečnosť-repealof-Delegated-Regulation-supplementing-the-Radio-Equipment-Directive\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14766-Kybernetická-bezpečnosť-repealof-Delegated-Regulation-supplementing-the-Radio-Equipment-Directive_en)

## 2.7 Nariadenie o európskom priestore pre zdravotné údaje (nariadenie (EÚ) 2025/327)

### 2.7.1 Aký je vzťah medzi CRA a nariadením o európskom priestore pre zdravotné údaje

CRA a nariadenie o európskom priestore pre zdravotné údaje (EHDS) stanovujú pravidlá pre uvádzanie produktov na trh: CRA stanovuje základné požiadavky kybernetickej bezpečnosti produktov s digitálnymi prvkami, zatiaľ čo nariadenie EHDS stanovuje okrem iného základné požiadavky, vrátane požiadaviek na interoperabilitu a logovanie, a ďalšie povinnosti, ktoré musia spĺňať systémy elektronických zdravotných záznamov (EHR).

Produkt môže byť zároveň produktom s digitálnymi prvkami v zmysle CRA a systémom EHR v zmysle nariadenia EHDS.

Príklad: Počítač alebo softvér, ktorý bol uvedený na trh a zakúpený nemocnicou a ktorý je určený na ukladanie a na náhľad súhrnov o pacientoch pri poskytovaní zdravotných služieb, by mohol byť produktom s digitálnymi prvkami v zmysle CRA, ktorý je zároveň systémom EHR v zmysle nariadenia EHDS.

### 2.7.2 Mal by produkt spĺňať požiadavky CRA aj nariadenia EHDS?

Produkt môže byť zároveň produktom s digitálnymi prvkami v zmysle CRA a systémom EHR v zmysle nariadenia EHDS. V takýchto prípadoch bude produkt musieť spĺňať požiadavky stanovené v CRA aj v nariadení EHDS (odôvodnenie 112 nariadenia EHDS). Požiadavky kybernetickej bezpečnosti stanovené v nariadení CRA a nariadení EHDS sú takej povahy, že súlad požiadaviek buď nariadenia CRA, alebo nariadenia EHDS samo o sebe nebude plne spĺňať požiadavky druhého nariadenia.

CRA (článok 13 ods. 4 CRA) však stanovuje, že v prípade produktov s digitálnymi prvkami, ktoré sú zároveň systémami EHR, môže byť posudzovanie kybernetickobezpečnostného rizika vyžadované CRA súčasťou posudzovania rizika vyžadovaného nariadením EHDS.

### 2.7.3 Mal by výrobca zabezpečiť posudzovanie zhody produktu prostredníctvom postupov stanovených v nariadení CRA aj v nariadení EHDS?

Nariadenie CRA aj nariadenie EHDS stanovujú postupy posudzovania zhody pre príslušné produkty. V prípade CRA sa to vzťahuje na produkty s digitálnymi prvkami, zatiaľ čo podľa nariadenia EHDS sa to vzťahuje na harmonizované softvérové komponenty systémov EHR (ako sú definované v článku 25 ods. 1 nariadenia EHDS).

To však neznamená, že výrobcovia musia zabezpečiť posudzovanie zhody kybernetickej bezpečnosti produktu prostredníctvom postupov stanovených v nariadení CRA aj v nariadení EHDS v prípadoch, keď je produkt produktom s digitálnymi prvkami v zmysle CRA a zároveň systémom EHR v zmysle nariadenia EHDS. CRA (článok 32 ods. 5a, ktorý bol zavedený

nariadením EHDS) určuje, že v takýchto prípadoch by sa mal namiesto postupu CRA uplatňovať postup posudzovania zhody podľa nariadenia EHDS.

#### 2.7.4 Mal by výrobca vypracovať samostatné EÚ vyhlásenia o zhode podľa jednotlivých právnych aktov Únie?

Pokiaľ ide o vypracovanie EÚ vyhlásenia o zhode výrobcom, článok 39 ods. 2 nariadenia EHDS stanovuje, že sa vypracuje jedno EÚ vyhlásenie o zhode pre všetky právne akty Únie, ktoré sa vzťahujú na systém EHR. Toto EÚ vyhlásenie o zhode obsahuje všetky informácie potrebné na identifikáciu právnych aktov Únie, na ktoré sa vzťahuje. CRA stanovuje to isté pre produkty s digitálnymi prvkami v článku 28 ods. 3.

## 2.8 Všeobecné nariadenie o ochrane údajov (nariadenie (EÚ) 2016/679)

### 2.8.1 Aký je vzťah medzi CRA a nariadením o všeobecnej ochrane údajov?

CRA a všeobecné nariadenie o ochrane údajov (GDPR) majú odlišnú povahu a nedochádza k ich právnemu prekryvaniu. CRA stanovuje povinnosti pre hospodárske subjekty, ktoré uvádzajú na trh produkty s digitálnymi prvkami, zatiaľ čo GDPR stanovuje pravidlá, vrátane povinností, pre fyzické a právnické osoby, ktoré konajú ako riadiaci alebo spracovatelia osobných údajov.

Hoci majú odlišnú povahu, tieto nariadenia sa môžu navzájom dopĺňať. CRA stanovuje požiadavky kybernetickej bezpečnosti pre produkty s digitálnymi prvkami, ktoré môžu prispieť k ochrane osobných údajov fyzických osôb. Patria sem okrem iného dôvernosť a integrita osobných a iných údajov, minimalizácia údajov, konfigurácia zabezpečenia ako predvolená bezpečnosť, ako aj požiadavky týkajúce sa riešenia zraniteľností a minimalizácie vplyvu závažných incidentov (príloha I). Podobne GDPR stanovuje požiadavky na činnosti spracúvania osobných údajov, ako sú minimalizácia údajov a zásady integrity a dôvernosti údajov (článok 5 GDPR), povinnosť ochrany údajov už pri návrhu (článok 25 GDPR), bezpečnosť údajov (článok 32 GDPR) a notifikácia porušení ochrany osobných údajov (článok 33 GDPR), ktoré môžu prispieť k kybernetickej bezpečnosti produktov s digitálnymi prvkami.

Súlady výrobcu s požiadavkami CRA v prípade produktu s digitálnymi prvkami však nemá žiadny formálny vplyv na nástroje, ktoré používajú prevádzkovatelia alebo spracovatelia podľa GDPR na preukázanie súladu spracúvania osobných údajov s GDPR (napríklad prostredníctvom kódexov správania (článok 40 GDPR) alebo certifikačnej schémy (článok 42 GDPR)).

## 2.9 Akt o údajoch (nariadenie (EÚ) 2023/2854)

### 2.9.1 Aká je vzájomná súvislosť medzi CRA a aktom o údajoch?

CRA a akt o údajoch (DA) majú v podstate odlišnú povahu, pričom CRA stanovuje pravidlá pre sprístupňovanie produktov s digitálnymi prvkami na trhu, zatiaľ čo DA stanovuje pravidlá (okrem iného) pre sprístupňovanie údajov o produktoch a súvisiacich službách iným subjektom.

V určitých prípadoch však môžu požiadavky CRA a DA platiť pre podobné produkty. V určitých prípadoch môže byť produkt s digitálnymi prvkami v zmysle CRA aj prepojeným produktom alebo súvisiacou službou v zmysle DA.

Napríklad domáce spotrebiče, ktoré obsahujú hardvér a softvér a môžu byť pripojené k internetu, aby mohli fungovať, ako napríklad „inteligentná“ chladnička, môžu tiež zbierať údaje o svojom používaní a môžu tieto údaje o produkte komunikovať prostredníctvom internetu. V tomto zmysle môže byť inteligentná chladnička zároveň produktom s digitálnymi prvkami v zmysle CRA a pripojeným produktom v zmysle DA.

### 2.9.2 Ako požiadavky na produkty s digitálnymi prvkami podľa CRA zohľadňujú povinnosti sprístupňovať údaje používateľom alebo tretím stranám podľa aktu o údajoch?

CRA okrem iného určuje, že produkty s digitálnymi prvkami sa môžu uvádzať na trh len vtedy, ak spĺňajú určité požiadavky kybernetickej bezpečnosti (článok 6). Výrobcovia musia zabezpečiť, aby produkty s digitálnymi prvkami, ktoré uvádzajú na trh, boli navrhnuté, vyvinuté a vyrobené v súlade s týmito požiadavkami (článok 13). Výrobcovia budú musieť vykonať posudzovanie rizika, ktoré bude zahŕňať analýzu kybernetickobezpečnostných rizík na základe zamýšľaného účelu a odôvodnene predvídateľného použitia produktu.

Ak sa na produkt s digitálnymi prvkami v zmysle CRA môžu vzťahovať aj požiadavky DA na sprístupňovanie údajov používateľom alebo tretím stranám (články 4 a 5 DA), výrobca bude musieť zabezpečiť, aby sa príslušné požiadavky podľa DA tiež zohľadnili v rámci posudzovania rizika. Výrobcovia by mali mať na pamäti, že hoci DA ukladá povinnosť sprístupniť údaje o produktoch a súvisiacich službách používateľom a tretím stranám, stanovuje tiež merania, ktoré držiteľia údajov môžu v určitých prípadoch využiť na obmedzenie alebo odmietnutie zdieľania údajov (napr. prostredníctvom tzv. „obchodného tajomstva“ a „bezpečnosti a ochrany“ (článok 4 ods. 8 a článok 5 ods. 11, resp. článok 4 ods. 2 DA).

### 2.9.3 Mal by výrobca prepracovať svoje produkty, aby vyhovovali požiadavkám DA a CRA?

Podľa DA neexistuje prísna povinnosť (pre)konštruovať produkty. Výrobcovia si skôr môžu voľne navrhovať produkty podľa vlastného uváženia, pokiaľ sú splnené povinnosti súvisiace so sprístupňovaním údajov.

Hoci sa CRA má v plnom rozsahu uplatňovať od 11. decembra 2027, produkty s digitálnymi prvkami, ktoré boli uvedené na trh pred týmto dátumom, podliehajú požiadavkám kybernetickej bezpečnosti CRA len v prípade, ak od tohto dátumu prejdú podstatnou úpravou (článok 69 ods. 2 CRA). Povinnosti podávať hlásenia, napr. o aktívne zneužívaných zraniteľnostiach, sa vzťahujú na všetky produkty s digitálnymi prvkami (článok 14). Pozri tiež *1.4. Vzťahuje sa CRA na produkty s digitálnymi prvkami, ktoré boli uvedené na trh pred 11. decembrom 2027?*

## 3 Dôležité a kritické produkty

### 3.1 Určenie, či je produkt s digitálnymi prvkami dôležitým alebo kritickým produktom?

V súlade s článkom 7 ods. 1 a článkom 8 ods. 1 by mal výrobca posúdiť základnú funkcionálnosť svojho produktu s digitálnymi prvkami, aby určil, či je tento produkt dôležitým alebo kritickým produktom s digitálnymi prvkami, a či sa naň preto vzťahujú príslušné postupy posudzovania zhody.

Technické opisy kategórií dôležitých a kritických produktov s digitálnymi prvkami sú stanovené vo vykonávacom nariadení Komisie (EÚ) 2025/2392 z 28. novembra 2025 o technickom opise kategórií dôležitých a kritických produktov s digitálnymi prvkami.

### 3.2 Stáva sa produkt dôležitým alebo kritickým, ak sa dôležitý alebo kritický produkt s digitálnymi prvkami integruje do iného produktu s digitálnymi prvkami?

Ako sa uvádza v článku 7 ods. 1, integrácia dôležitého alebo kritického produktu s digitálnymi prvkami do iného produktu s digitálnymi prvkami automaticky nespôsobuje, že tento produkt podlieha postupom posudzovania zhody platným pre dôležité a kritické produkty. Napríklad integrácia vstavaného prehliadača ako komponentu aplikácie na čítanie správ určenej na používanie v smartfónoch sama osebe nespôsobuje, že táto aplikácia podlieha postupu posudzovania zhody platnému pre produkty s digitálnymi prvkami, ktorých základnou funkcionálnosťou je „samostatné a vstavané prehliadače“. Podobne, integrácia bezpečnostného prvku do prenosného počítača sama o sebe nespôsobuje, že prenosný počítač podlieha postupu posudzovania zhody uplatniteľnému na produkty s digitálnymi prvkami, ktorých základnou funkcionálnosťou sú „smart karty a podobné zariadenia, vrátane bezpečnostných prvkov“.

Ako sa uvádza v *bode 3.1 Čo určuje, či je produkt s digitálnymi prvkami dôležitým alebo kritickým produktom?*, základná funkcionálnosť produktu s digitálnymi prvkami, do ktorého sú integrované iné komponenty, určuje, či je tento produkt dôležitým alebo kritickým produktom s digitálnymi prvkami.

### 3.3 Ovplyvňuje klasifikácia produktu ako dôležitého alebo s kritického posudzovanie rizika výrobcom?

V súlade s odsekmi 1 až 3 článku 13 CRA stanovuje, že výrobcovia produktov s digitálnymi prvkami musia implementovať základné požiadavky kybernetickej bezpečnosti spôsobom, ktorý je primeraný rizikám produktu s digitálnymi prvkami, na základe zamýšľaného účelu a odôvodnene predvídateľného použitia, ako aj podmienok používania produktu s digitálnymi

prvkami, s prihliadnutím na predpokladaný čas používania produktu. Bez ohľadu na to, či sa produkt s digitálnymi prvkami považuje za dôležitý alebo kritický produkt s digitálnymi prvkami, výrobcovia musia vykonať komplexné posudzovanie kybernetickobezpečnostného rizika a uviesť, ako sa implementujú základné požiadavky kybernetickej bezpečnosti na základe posudzovania rizika, vrátane ich skúšania a záruky.

Napríklad výrobca chce uviesť na trh dve rôzne verzie VPN. Na základe posudzovania rizika výrobca určí, že jedna z týchto dvoch VPN predstavuje významnejšie riziko, napríklad preto, že je určená na použitie v kritickej infraštruktúre, zatiaľ čo druhá VPN predstavuje menšie riziko, napríklad preto, že je určená iba na použitie v domácnostiach. V dôsledku toho sa od výrobcu očakáva, že implementuje základné požiadavky pre oba produkty tak, aby zabezpečil primerané zmiernenie príslušných rizík.

### 3.4 Znamená prítomnosť viacerých funkcií, že produkt nemá základnú funkcionality dôležitého alebo kritického produktu?

Ako sa vysvetľuje v odôvodnení 4 vykonávacieho nariadenia Komisie (EÚ) 2025/2392 z 28. novembra 2025 o technickom opise kategórií dôležitých a kritických produktov s digitálnymi prvkami, skutočnosť, že produkt s digitálnymi prvkami vykonáva aj iné alebo dodatočné funkcie, a nie len funkcie rozvedené v technickom opise stanovenom v tomto nariadení, ako taká neznamená, že produkt s digitálnymi prvkami nemá základnú funkcionality produktu kategórie stanovenej v prílohách III a IV k nariadeniu (EÚ) 2024/2847. Napríklad produkty s digitálnymi prvkami, ktoré majú základnú funkcionality „operačných systémov“, často zahŕňajú softvér, ktorý vykonáva doplnkové funkcie, ktoré nefigurujú v technickom opise danej kategórie produktov, ako napríklad funkcie kalkulačky alebo jednoduchých grafických editorov. Produkty s digitálnymi prvkami takisto často zahŕňajú komponenty s funkcionalitami iného dôležitého alebo kritického produktu s digitálnymi prvkami, ako sú operačné systémy s integrovanou funkciou prehliadača, alebo smerovače s integrovanou funkcionalitou firewallu. Táto skutočnosť ako taká však neznamená, že dané produkty s digitálnymi prvkami nemajú základnú funkcionality „operačných systémov“ alebo „smerovače, modemy určené na pripojenie k internetu a prepínače“ (tiež dôležité produkty s digitálnymi prvkami triedy I).

Na druhej strane sa pri produktoch s digitálnymi prvkami, ktoré dokážu vykonávať funkcie kategórie produktov stanovenej v prílohách III a IV k nariadeniu (EÚ) 2024/2847, ale ktorých samotná základná funkcionality je iná než základná funkcionality produktov danej kategórie, nevychádza z predpokladu, že spĺňajú technický opis predmetnej kategórie produktov. Napríklad softvér orchestrácie, automatizácie a odozvy zabezpečenia (SOAR) často dokáže vykonávať funkciu produktov s digitálnymi prvkami kategórie „systémy riadenia bezpečnostných informácií a udalostí (SIEM)“. Pretože však základnou funkcionalitou softvéru SOAR nie je funkcionality SIEM, nemá sa vo všeobecnosti vychádzať z predpokladu, že spĺňa technický opis „systémov riadenia bezpečnostných informácií a udalostí (SIEM)“. Podobne smartfóny spravidla zahŕňajú komponenty vykonávajúce funkcie viacerých kategórií produktov stanovených v prílohách III a IV k nariadeniu (EÚ) 2024/2847, napríklad funkcie ako operačný

system alebo integrovaný správca hesiel. Pretože však základnou funkcionalitou smartfónov nie je funkcionalita operačného systému ani správcu hesiel, vo všeobecnosti sa nemá vychádzať z predpokladu, že spĺňajú technický opis predmetných kategórií produktov.

## 4 Povinnosti výrobcu

### 4.1 Prístup založený na riziku a posudzovanie rizika

#### 4.1.1 Čo CRA vyžaduje od posúdenia kybernetickobezpečnostných rizík výrobcu?

Harmonizačné právne predpisy Únie týkajúce sa produktov dostupných na vnútornom trhu a založené na novom legislatívnom rámci (NLF)<sup>5</sup> zvyčajne vyžadujú, aby výrobcovia vykonali posúdenie rizika, na základe ktorého musia implementovať príslušné základné požiadavky definované v príslušných právnych predpisoch (pozri napríklad časť 4.1.1 Modrej príručky). Tieto posúdenia rizika sú dôležitou dokumentáciou, ktorou výrobcovia preukazujú (t. j. orgánom dohľadu nad trhom), že implementovali primerané požiadavky. Výrobcovia môžu vykonať jedno posúdenie rizika, ktoré pokryje požiadavky rôznych právnych predpisov, alebo môžu vykonať individuálne posúdenie rizika pre každý právny predpis samostatne. Hoci je na výrobcovi, aby si štruktúroval svoju činnosť v oblasti posúdenia rizika, musí byť schopný preukázať súlad s každým jednotlivým právnym predpisom. V súlade s definíciou produktu s digitálnymi prvkami (článok 3 ods. 1) musí posúdenie kybernetickobezpečnostného rizika výrobcu pokrývať celý produkt s digitálnymi prvkami, vrátane spracovania údajov na diaľku, ak patrí do rozsahu pôsobnosti, a akýchkoľvek podporných funkcií, ktoré môžu byť súčasťou produktu s digitálnymi prvkami, ktorý sa má uviesť na trh.

Článok 13 ods. 2 vyžaduje, aby výrobcovia vykonali posúdenie kybernetickobezpečnostných rizík spojených s produktom s digitálnymi prvkami a výsledok tohto posúdenia zohľadnili vo fáze plánovania, návrhu, vývoja, výroby, dodania a údržby produktu s digitálnymi prvkami s cieľom minimalizovať kybernetickobezpečnostné riziká, predchádzať incidentom a minimalizovať ich vplyv, a to aj v súvislosti so zdravím a bezpečnosťou používateľov. Je preto dôležité poznamenať, že posúdenie kybernetickobezpečnostného rizika sa netýka len počiatkových fáz identifikácie rizika, analýzy rizika a hodnotenia rizika počas fáz návrhu a vývoja, ale aj opatrení na zaobchádzanie s rizikom vykonávaných počas fáz výroby, dodávky a údržby. Táto povinnosť sa navyše vzťahuje na výrobcov všetkých produktov s digitálnymi prvkami v zmysle CRA, bez ohľadu na to, či produkt s digitálnymi prvkami patrí do „default kategórie“, je dôležitým alebo kritickým produktom.

V súlade s článkom 13 ods. 3 v posúdení kybernetickobezpečnostných rizík sa uvedie, či a ak áno, akým spôsobom sa bezpečnostné požiadavky stanovené v bode 2 časti I prílohy I vzťahujú na príslušný produkt s digitálnymi prvkami a ako sa tieto požiadavky vykonávajú na základe posúdenia kybernetickobezpečnostných rizík. Malo by tiež uvádzať, ako výrobca naplánoval, navrhol, vyvinul, vyrobil, dodal a udržiaval produkt s digitálnymi prvkami tak, aby zabezpečil jeho primeranú úroveň kybernetickej bezpečnosti voči rizikám (časť I bod 1 prílohy I) a požiadaviek na riešenie zraniteľnosti (stanovených v časti II prílohy I).

---

<sup>5</sup> Nový legislatívny rámec pozostáva z nariadenia (ES) č. 765/2008, ktorým sa stanovujú požiadavky na akreditáciu a dohľad nad trhom s výrobkami, rozhodnutia č. 768/2008 o spoločnom rámci pre uvádzanie výrobkov na trh a nariadenia (EÚ) č. 2019/1020 o trhovom dohľade a súlade výrobkov.

#### 4.1.2 Vyžaduje CRA konkrétnu metodiku posudzovania rizika?

CRA nepredpisuje konkrétnu metodiku posudzovania kybernetickobezpečnostného rizika. Výrobcovia môžu rozhodnúť o metodike, ktorú použijú na identifikáciu a riešenie príslušných rizík. Výrobcovia musia riešiť všetky príslušné riziká vyplývajúce z posudzovania kybernetickobezpečnostného rizika, a metodika posudzovania rizika by preto mala výrobcom poskytovať podporu pri dokumentovaní, že tak urobili (v súlade s článkom 13 ods. 3), čím orgánom dohľadu nad trhom umožnia overiť, ako boli riziká identifikované, hodnotené a zmiernené.

Pri modelovaní scenárov hrozieb by výrobcovia mali zabezpečiť použitie metodiky modelovania hrozieb, ktorá primerane odráža hrozby a vyplývajúce riziko spojené s určeným účelom produktu a jeho odôvodnene predvídateľným použitím. Napríklad, zatiaľ čo produkty určené na použitie v kritickej infraštruktúre môžu spĺňať požiadavku na riešenie rizík súvisiacich s aktérmi na národnej úrovni štátu a pokročilými trvalými hrozbami, produkty určené na súkromné použitie spotrebiteľmi majú zvyčajne nižšie riziko a môžu používať iný model hrozieb. Týmto spôsobom môžu výrobcovia vo svojom posudzovaní rizika pokryť všetky relevantné riziká pre produkt.

#### 4.1.3 Musí výrobca implementovať všetky základné požiadavky?

Výrobcovia musia počas celého obdobia podpory produktu spĺňať všetky základné požiadavky kybernetickej bezpečnosti súvisiace s riešením zraniteľnosti (uvedené v časti II prílohy I). Pokiaľ však ide o základné požiadavky kybernetickej bezpečnosti súvisiace s vlastnosťami produktu (uvedené v časti I prílohy I), výrobcovia musia na základe posúdenia kybernetickobezpečnostného rizika určiť, ktoré z týchto požiadaviek sú relevantné pre daný typ produktu s digitálnymi prvkami. V súlade s článkom 13 ods. 4, ak sa určité základné požiadavky kybernetickej bezpečnosti nevzťahujú na produkt s digitálnymi prvkami, výrobca by mal do posúdenia kybernetickobezpečnostného rizika zahrnutého v technickej dokumentácii zahrnúť jasné odôvodnenie. Takýto prípad by mohol nastať, ak je základná požiadavka kybernetickej bezpečnosti nezlučiteľná s povahou produktu s digitálnymi prvkami (pozri odôvodnenie 55) alebo ak neexistujú žiadne riziká, ktoré by si vyžadovali zmiernenie v súvislosti s touto základnou požiadavkou.

Napríklad produkt nemusí obsahovať žiadne osobitné zmierňujúce opatrenia týkajúce sa ochrany osobných údajov, ak zamýšľaný účel produktu a odôvodnene predvídateľné použitie nezahŕňajú spracúvanie akéhokoľvek druhu osobných údajov. V takýchto prípadoch môže produkt stále disponovať technickou schopnosťou spracúvať niektoré druhy osobných údajov, ale takéto použitie by nebolo zahrnuté v zamýšľanom účele a odôvodnene predvídateľnom použití deklarovanom výrobcom. Ak technická schopnosť produktu spracúvať osobné údaje môže viesť k významným kybernetickobezpečnostným rizikám v prípade odôvodnene predvídateľného zneužitia, informácie a pokyny pre používateľa môžu musieť obsahovať túto informáciu v súlade s bodom 5 prílohy II CRA.

Napríklad, ako sa uvádza v odôvodnení 55, zamýšľaný účel produktu s digitálnymi prvkami môže vyžadovať, aby výrobca dodržiaval všeobecne uznávané normy interoperability, aj keď sa jeho bezpečnostné prvky už nepovažujú za najmodernejšie. Podobne sa v iných právnych predpisoch Únie vyžaduje, aby výrobcovia uplatňovali osobitné požiadavky na interoperabilitu. Ak sa základná požiadavka kybernetickej bezpečnosti na produkt s digitálnymi prvkami nevzťahuje, ale výrobca v súvislosti s touto základnou požiadavkou kybernetickej bezpečnosti identifikoval kybernetickobezpečnostné riziká, mal by prijať opatrenia na riešenie týchto rizík inými prostriedkami, napríklad obmedzením zamýšľaného účelu produktu na dôveryhodné prostredia alebo informovaním používateľov o týchto rizikách.

#### 4.1.4 Čo je zamýšľaný účel a odôvodnene predvídateľné použitie a aký vplyv majú na posúdenie kybernetickobezpečnostného rizika?

V súlade s článkom 13 ods. 2 sa posúdenie kybernetickobezpečnostných rizík vykonáva s cieľom minimalizovať takéto riziká, predchádzať incidentom a minimalizovať ich vplyv, a to aj v súvislosti so zdravím a bezpečnosťou používateľov. Okrem toho sa v článku 13 ods. 3 objasňuje, že analýza kybernetickobezpečnostných rizík zohľadňuje aspoň zamýšľaný účel a odôvodnene predvídateľné použitie, ako aj podmienky používania produktu s digitálnymi prvkami, ako je prevádzkové prostredie alebo aktíva, ktoré sa majú chrániť, s ohľadom na dĺžku predpokladaného používania produktu. Napríklad výrobcovia hardvérových alebo softvérových komponentov, ktoré sa používajú v mnohých ďalších produktoch na nižších úrovniach dodávateľského reťazca, môžu zvážiť, či zamýšľaný účel a odôvodnene predvídateľné použitie zahŕňa integráciu týchto komponentov. V takýchto prípadoch musí výrobca zabezpečiť, aby sa príslušné riziká riadne riešili (článok 13 ods. 1 a 2), a poskytnúť používateľom jasné, zrozumiteľné, zrozumiteľné a čitateľné pokyny, ktoré umožňujú bezpečnú inštaláciu, prevádzku a používanie produktu s digitálnymi prvkami (podľa článku 13 ods. 8).

V článku 3 ods. 23 sa „zamýšľaný účel“ vymedzuje ako použitie produktu s digitálnymi prvkami, ktoré určil výrobca, vrátane osobitného kontextu a podmienok používania, ako sa uvádza v informáciách od výrobcu v návode na použitie, v propagačných alebo predajných materiáloch a vyhláseniach, ako aj v technickej dokumentácii. Okrem toho sa „odôvodnene predvídateľné použitie“ v článku 3 ods. 24 vymedzuje ako použitie, ktoré nemusí byť nevyhnutne zamýšľaným účelom, ktorý výrobca uvádza v návode na použitie, v propagačných alebo predajných materiáloch a vyhláseniach, ako aj v technickej dokumentácii, ale ktoré pravdepodobne vyplynie z odôvodnene predvídateľného ľudského správania alebo technických operácií či interakcií. Ak je to relevantné pre zamýšľaný účel a odôvodnene predvídateľné použitie, výrobca by mal zvážiť aj to, ako môže integrácia a konečné použitie ovplyvniť posúdenie kybernetickobezpečnostného rizika (t. j. konkrétny kontext a podmienky použitia). Okrem toho by výrobcovia mali prostredníctvom informácií a pokynov pre používateľov informovať svojich používateľov, či už sú to integrátori, profesionálni vlastníci alebo prevádzkovatelia, spotrebitelia alebo iné osoby, o všetkých predpokladoch alebo požiadavkách, ktoré sú potrebné na bezpečnú inštaláciu, prevádzku a používanie produktu s digitálnymi prvkami, v súlade s článkom 13 ods. 18.

Ako sa uvádza v oddiele 2.8 Modrej príručky, výrobcovia musia zabezpečiť úroveň ochrany zodpovedajúcu použitiu, ktoré predpisujú pre výrobok v rámci podmienok použitia, ktoré možno odôvodnene predpokladať pred uvedením produktu na trh, najmä ak takéto používanie môže vyplývať zo zákonného a ľahko predvídateľného ľudského správania. To znamená, že výrobcovia musia pozerieť ďalej ako na to, čo považujú za zamýšľané použitie produktu, a vžiť sa do pozície priemerného používateľa konkrétneho produktu a predstaviť si, akým spôsobom by rozumne zvažovali používanie produktu. Napríklad, ako sa uvádza v oddiele 3.1 Modrej príručky, nástroj navrhnutý a určený na používanie výlučne odborníkmi (napríklad priemyselný senzor IoT alebo virtuálna súkromná sieť) môže nakoniec používať aj neodborník; dôsledok je, že sa táto možnosť musí zohľadniť v konštrukcii a v priložených pokynoch. Podobne by informácie potrebné na bezpečnú inštaláciu mali byť naďalej poskytované spôsobom, ktorý je jasný, zrozumiteľný, zrozumiteľný a čitateľný, so zreteľom na zamýšľané publikum, od ktorého sa očakáva, že inštaláciu vykoná, v súlade s článkom 13 ods. 18. Ak je produkt ľahko dostupný a je pravdepodobné, že ho budú používať spotrebitelia, výrobca by mal zohľadniť potreby a riziko týchto spotrebiteľov, napríklad prostredníctvom vhodných informácií a pokynov pre používateľov, vrátane pokynov na bezpečnú inštaláciu, prevádzku a používanie produktu s digitálnymi prvkami.

Ako sa však uvádza v oddiele 2.8 Modrej príručky, pri navrhovaní výrobku nie je možné predísť všetkým rizikám, preto by sa mali zohľadniť aj zamýšľané alebo predvídateľné podmienky používania. V prípade potreby by sa pri posudzovaní kybernetickobezpečnostného rizika mali zohľadniť aj ďalšie merania, ktoré môže zaviesť zamýšľaná alebo predvídateľná kategória používateľov (napr. profesionáli). Napríklad dozor a pomoc zamýšľaných používateľov by sa mali považovať za súčasť podmienok, ktoré možno rozumne predpokladať v prípade produktov, ktoré sa majú inštalovať a používať v určitých profesionálnych prostrediach, napríklad v priemyselných závodoch. Ďalším príkladom sú niektoré profesionálne obrábacie stroje, ktoré sú určené na používanie priemerne kvalifikovanými vyškolenými pracovníkmi pod vedením ich zamestnávateľa; výrobca nemôže niesť zodpovednosť, ak takéto obrábacie stroje prenajímajú distribútorom alebo tretej strane poskytujúcej službu na používanie nekvalifikovanými a nevyškolenými spotrebiteľmi. Okrem toho môže byť v niektorých prípadoch rozumné, aby výrobca prostredníctvom návrhu produktu umožnil používateľovi zmeniť konfiguráciu produktu, odstrániť bezpečnostnú funkcionálnosť alebo znížiť úroveň bezpečnostných opatrení s cieľom zabezpečiť kompatibilitu so staršími verziami. V takýchto prípadoch by výrobca mal zahrnúť príslušné kybernetickobezpečnostné riziká do svojho posúdenia kybernetickobezpečnostného rizika, zaviesť osobitné opatrenia na riešenie týchto rizík a k týmto možnostiam použitia priložiť vhodné informácie a pokyny pre používateľa, aby sa zabezpečilo bezpečné nasadenie a dosiahnutie požadovaných výsledkov v oblasti bezpečnosti. Okrem toho, ak táto okolnosť môže viesť k významným kybernetickobezpečnostným rizikám, výrobca by mal tieto riziká výslovne uviesť v súlade s bodom 5 prílohy II CRA.

#### 4.1.5 Čo je odôvodnene predvídateľné nesprávne použitie a aký vplyv má na posúdenie kybernetickobezpečnostného rizika?

V súlade s článkom 13 ods. 18 by mal výrobca poskytnúť informáciu pre používateľa o očakávaných podmienkach bezpečného nasadenia a integrácie produktu. Používatelia by mali zohľadniť zákonné podmienky používania produktu stanovené výrobcom, ak sú primerané a vhodné na zamýšľaný účel a odôvodnene predvídateľné použitie, najmä pokiaľ ide o menej kvalifikovaných alebo zraniteľných používateľov. V článku 3 ods. 24 sa „odôvodnene predvídateľné nesprávne použitie“ vymedzuje ako použitie, ktoré nemusí byť nevyhnutne zamýšľaným účelom, ktorý výrobca uvádza v návode na použitie, v propagačných alebo predajných materiáloch a vyhláseniach, ako aj v technickej dokumentácii, ale ktoré pravdepodobne vyplynie z odôvodnene predvídateľného ľudského správania alebo technických operácií či interakcií. Napríklad ak informácia a pokyny pre používateľa uvádzajú, že produkt sa musí používať v zabezpečenej sieti, jeho používanie v nezabezpečenej sieti by mohlo predstavovať odôvodnene predvídateľné nesprávne použitie. Podobne, hoci niektorí používatelia môžu „hackovať“ svoje zariadenia pre zábavu (alebo pre výskum v oblasti bezpečnosti), takéto použitie nie je nevyhnutne v súlade s určeným účelom a odôvodnene predvídateľným použitím uvedeným výrobcom, a preto by predstavovalo formu nesprávneho použitia.<sup>6</sup>

Okrem toho výrobcovia zabezpečia, aby produkty s digitálnymi prvkami boli sprevádzané informáciami a pokynmi pre používateľa uvedenými v prílohe II, vrátane akýchkoľvek známych alebo predvídateľných okolností súvisiacich s používaním produktu s digitálnymi prvkami v súlade s jeho určeným účelom alebo za podmienok odôvodnene predvídateľného nesprávneho používania, ktoré môžu viesť k významným kybernetickobezpečnostným rizikám. Riziká týkajúce sa odôvodnene predvídateľného nesprávneho používania musia byť tiež uvedené v informáciách a pokynoch pre používateľa. Ak napríklad informácie a pokyny pre používateľa uvádzajú, že produkt sa musí používať v zabezpečenej sieti, znamená to, že výrobca nemusel zohľadniť určité riziká vyplývajúce z používania v nezabezpečených sieťach. Výrobca by preto mal informovať používateľa vždy, keď takéto odôvodnene predvídateľné nesprávne používanie môže stále viesť k významným kybernetickobezpečnostným rizikám v oblasti.

---

<sup>6</sup> Ako sa uvádza v odôvodnení 75, členské štáty by sa mali v súlade s vnútroštátnym právom snažiť v čo najväčšej miere riešiť výzvy, ktorým čelia výskumní pracovníci zaoberajúci sa zraniteľnosťami, vrátane ich možnej trestnej zodpovednosti. Keďže fyzické a právnické osoby, ktoré skúmajú zraniteľnosti, by v niektorých členských štátoch mohli byť vystavené trestnej a občianskoprávnej zodpovednosti, členským štátom sa odporúča prijať usmernenia, aby výskumní pracovníci v oblasti bezpečnosti informácií neboli za svoju činnosť stíhaní a dostali výnimku z občianskoprávnej zodpovednosti.

#### 4.1.6 Aký vplyv má predpokladaná dĺžka používania produktu na posúdenie kybernetickobezpečnostného rizika výrobcu?

Na účely zabezpečenia bezpečnosti produktov s digitálnymi prvkami po ich uvedení na trh by výrobcovia mali určiť obdobie podpory, ktoré by malo odzrkadľovať predpokladanú dĺžku používania produktu s digitálnymi prvkami. V súlade s článkom 13 ods. 3 by preto analýza kybernetickobezpečnostných rizík vykonaná výrobcom mala zohľadňovať predpokladanú dĺžku používania produktu (článok 13 ods. 8). Výrobca by mal zohľadniť životnosť produktu aj vo fáze návrhu a vývoja a mal by najmä pripraviť produkt tak, aby sa počas celého obdobia podpory efektívne a v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I riešili zraniteľnosti tohto produktu, vrátane jeho komponentov. Okrem toho sa podľa článku 13 ods. 7 posúdenie rizika dokumentuje a v prípade potreby aktualizuje počas obdobia podpory produktu. Ak sa posúdenie rizika opiera o informácie a pokyny pre používateľov na riešenie určitých rizík, tieto informácie a pokyny pre používateľov by sa mali primerane aktualizovať.

Výrobca môže napríklad zvážiť primerané prognózy týkajúce sa zmien v prostredí hrozby a toho, ako by tieto zmeny mohli mať vplyv na posúdenie rizika počas životnosti produktu.

#### 4.1.7 Aký je vzťah medzi harmonizovanými normami a posúdením kybernetickobezpečnostného rizika výrobcu?

Ako sa uvádza v Modrej príručke, harmonizované normy nenahrádzajú právne záväzné základné požiadavky. Technická špecifikácia uvedená v harmonizovanej norme nie je alternatívou k príslušnej základnej alebo inej zákonnej požiadavke, ale len možným technickým prostriedkom na jej splnenie. V právnych predpisoch týkajúcich sa harmonizácie v oblasti rizík to znamená najmä to, že výrobcovia vždy, aj keď používajú harmonizované normy, ktorých odkazy sú uverejnené v Úradnom vestníku Európskej únie („Ú. v. EÚ“), zostávajú plne zodpovední za posúdenie všetkých rizík svojho produktu s cieľom určiť, ktoré základné (alebo iné) požiadavky sú relevantné. Po tomto posudzovaní sa výrobca môže rozhodnúť uplatniť technické špecifikácie uvedené v harmonizovaných normách, ktorých odkazy sú uverejnené v Ú. v. EÚ, s cieľom implementovať „meranie rizika“, ktoré sú špecifikované v harmonizovaných normách. V harmonizačných právnych predpisoch týkajúcich sa rizík harmonizované normy, ktorých odkazy sú uverejnené v Ú. v. EÚ, najčastejšie poskytujú určité prostriedky na zníženie alebo odstránenie rizík, pričom výrobcovia naďalej nesú plnú zodpovednosť za posudzovanie rizika s cieľom identifikovať relevantné riziko a identifikovať relevantné základné požiadavky, aby mohli vybrať vhodné harmonizované normy, ktorých odkazy sú uverejnené v Ú. v. EÚ, alebo iné špecifikácie.

Preto aj v prípade, že výrobca používa harmonizovanú normu (ktorého odkaz je uverejnený v Úradnom vestníku a ktorej cieľom je pokryť určité riziko) na splnenie základných požiadaviek, musí sa vykonať posúdenie kybernetickobezpečnostného rizika a musí sa skontrolovať, či harmonizovaná norma pokrýva všetky riziká produktu. V súlade s článkom 27, ak výrobca správne uplatňuje harmonizovanú normu, ktorej odkaz je uverejnený v Úradnom vestníku EÚ

a ktorá pokrýva všetky riziká relevantné pre produkt s digitálnymi prvkami, produkt sa považuje za vyhovujúci.<sup>7</sup>

Ako sa uvádza v článku 27 ods. 1 CRA a v oddiele 4.1.2.2 Modrej príručky, ak harmonizovaná norma pokrýva len časť základných požiadaviek, ktoré výrobcovia považujú za relevantné, alebo len niektoré ich aspekty, musia výrobcovia dodatočne použiť iné relevantné technické špecifikácie alebo vyvinúť riešenia v súlade so všeobecnými technickými alebo vedeckými poznatkami stanovenými v technickej a vedeckej literatúre, aby splnili základné požiadavky CRA. Podobne, ak sa výrobcovia rozhodnú neuplatňovať všetky ustanovenia uvedené v harmonizovanej norme, ktoré by za normálnych okolností poskytovali domnienku zhody, musia na základe vlastného posúdenia kybernetickobezpečnostného rizika vo svojej technickej dokumentácii uviesť, ako sa dosahuje súlad, alebo že príslušné základné požiadavky nie sú pre produkt relevantné.

Žiadosť CRA o normalizáciu CRA požaduje vypracovanie súboru harmonizovaných noriem, ktorých cieľom je poskytnúť výrobcovi buď horizontálne, alebo produktovo špecifické informácie na podporu ich súladu s CRA. Pozri tiež *6.10 Kedy budú pripravené harmonizované normy na podporu súladu s CRA?*

#### 4.1.8 Čo musí výrobca zahrnúť do technickej dokumentácie, ktorá má byť k dispozícii orgánom dohľadu nad trhom, pokiaľ ide o posúdenie kybernetickobezpečnostného rizika?

Článok 13 ods. 12 a článok 31 vyžadujú, aby výrobca vypracoval technickú dokumentáciu obsahujúcu informácie preukazujúce zhodu produktu s príslušnými požiadavkami, bez ohľadu na postup posudzovania zhody. Táto dokumentácia môže byť súčasťou dokumentácie systému kvality, ak si výrobca zvolí postup posudzovania zhody založený na systéme kvality v súlade s článkom 32. To platí v prípade zhody založenej na úplnom zabezpečení kvality na základe modulu H (časť IV prílohy VIII CRA). Technická dokumentácia musí byť k dispozícii pri uvedení produktu na trh, bez ohľadu na jeho geografický pôvod alebo umiestnenie. V súlade s článkom 13 ods. 4 výrobca pri uvedení produktu s digitálnymi prvkami na trh zahŕňa posúdenie kybernetickobezpečnostného rizika do technickej dokumentácie požadovanej podľa článku 31 a prílohy VII. Po uvedení na trh výrobca systematicky dokumentuje spôsobom, ktorý je primeraný povahe a kybernetickobezpečnostným rizikám, relevantné aspekty kybernetickej bezpečnosti týkajúce sa produktov s digitálnymi prvkami, vrátane zraniteľností, o ktorých sa dozvedel, a akýchkoľvek relevantných informácií poskytnutých tretími stranami, a v prípade potreby aktualizuje posudzovanie kybernetickobezpečnostného rizika produktov. Najmä v rámci požiadavky na riešenie zraniteľností uvedenej v prílohe I časti 2 ods. 3 musí výrobca aktualizovať posúdenie rizika po vykonaní pravidelných skúšaniach a preskúmaní, ak z týchto skúšaniach a preskúmaní vyplynú relevantné informácie týkajúce sa kybernetickej bezpečnosti produktu.

---

<sup>7</sup> Ako sa uvádza v poznámke pod čiarou 179 Modrej príručky.

Podľa oddielu 4.3 Modrej príručky v prípade, že produkt bol predmetom prepracovania a opätovného posudzovania zhody, technická dokumentácia musí odrážať všetky verzie produktu; opisovať vykonané zmeny, spôsob identifikácie rôznych verzií produktu a informácie o rôznych posudzovaniach zhody.

V súlade s článkom 53, ak je potrebné posúdiť zhodu produktov s digitálnymi prvkami a postupov zavedených ich výrobcami so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, orgánom dohľadu nad trhom sa na základe odôvodnenej žiadosti poskytne prístup k údajom v jazyku pre ne ľahko zrozumiteľnom, požadovaným na posúdenie návrhu, vývoja, výroby a riešenia zraniteľností takýchto produktov vrátane súvisiacej internej dokumentácie príslušného hospodárskeho subjektu.

## 4.2 Základné požiadavky týkajúce sa produktov (príloha I, časť I)

### 4.2.1 Aké technické opatrenia musí výrobca zaviesť?

CRA stanovuje súbor základných požiadaviek kybernetickej bezpečnosti týkajúcich sa vlastností produktov s digitálnymi prvkami. Tieto požiadavky sú orientované na ciele a technologicky neutrálne a uplatňujú sa horizontálne na všetky produkty s digitálnymi prvkami.

Konkrétna technická implementácia základných požiadaviek závisí od posúdenia kybernetickobezpečnostného rizika, ktoré je každý výrobca povinný podniknúť a zohľadniť počas fáz plánovania, návrhu, vývoja, výroby, dodávky a údržby produktu s digitálnymi prvkami v súlade s článkom 13 ods. 12. Ďalšie informácie o posúdení rizika nájdete v oddiele 4.1 *Prístup založený na riziku a posudzovanie rizika*.

Výrobca je povinný vo svojej technickej dokumentácii podrobne opísať prostriedky použité na zabezpečenie súladu produktu so základnými požiadavkami kybernetickej bezpečnosti, vrátane prípadov, keď sa určité základné požiadavky kybernetickej bezpečnosti nevzťahujú na produkt s digitálnymi prvkami, v súlade s článkom 13 ods. 4.

S cieľom uľahčiť posudzovanie zhody so základnými požiadavkami Komisia prijala [žiadosť o normalizáciu](#) adresovanú CEN, CENELEC a ETSI (európskym normalizačným organizáciám), v ktorej žiada o vypracovanie harmonizovaných noriem v technických oblastiach, na ktoré sa vzťahuje CRA.

Žiadosť o normalizáciu pre CRA požaduje *okrem iného* vypracovanie horizontálnych harmonizovaných noriem, ktoré pokrývajú základné požiadavky týkajúce sa produktov stanovené v prílohe I časti I CRA, s náhľadom na podporu „i) vypracovania ďalších podrobných vertikálnych harmonizovaných noriem pre konkrétne produkty alebo typy produktov a (ii) [na] podporu výrobcov pri definovaní a implementácii bezpečnostných požiadaviek uplatniteľných na ich príslušné produkty, najmä na produkty, na ktoré sa nevzťahujú existujúce alebo plánované vertikálne normy“ (príloha II, oddiel 2.1 CRA SR). Ďalšie informácie nájdete v bode 6.10 *Kedy budú pripravené harmonizované normy na podporu súladu s CRA?*

Je potrebné poznamenať, že používanie harmonizovaných noriem je dobrovoľné. Výrobcovia môžu preukázať zhodu so základnými požiadavkami prostredníctvom iných technických prostriedkov a sú povinní ich zdokumentovať vo svojej technickej dokumentácii.

#### 4.2.2 Ako môže výrobca zabezpečiť, aby produkt neobsahoval žiadnu zraniteľnosť?

*Na základe posúdenia kybernetickobezpečnostných rizík uvedeného v článku 13 ods. 2 a podľa potreby sa produkty s digitálnymi prvkami [...] sprístupňujú na trhu bez známych zneužívateľných zraniteľností; (príloha I, základná požiadavka 2 písm. a))*

*„zraniteľnosť“ je slabá stránka, náchylnosť alebo chyba produktu s digitálnymi prvkami, ktorú môže zneužiť kybernetická hrozba (článok 3 ods. 40)*

*„zneužívateľná zraniteľnosť“ je zraniteľnosť, ktorú môže nepriateľský subjekt účinne využiť za reálnych prevádzkových podmienok (článok 3 ods. 41)*

CRA nevyžaduje od výrobcov, aby zabezpečili, že produkt neobsahuje žiadne zraniteľnosti.

CRA vyžaduje, aby výrobcovia v čase uvedenia na trh na základe svojho posúdenia kybernetickobezpečnostného rizika a v prípade potreby zabezpečili, že produkt neobsahuje známe zraniteľnosti, ktoré je možné zneužiť.

V skutočnosti nie všetky zraniteľnosti sú zneužívateľné za praktických prevádzkových podmienok. Niektoré zraniteľnosti možno zneužiť len za teoretických podmienok (napr. v laboratóriu alebo v simulácii) a/alebo nie za podmienok, ktoré by nastali v prevádzkovom prostredí daného produktu s digitálnymi prvkami. Otázka, či je zraniteľnosť zneužívateľná, sa musí riešiť individuálne v závislosti od konkrétnych prevádzkových a technických podmienok, vrátane napríklad rozsahu, v akom sa zraniteľný kód vyvoláva alebo načíta, keď je produkt v prevádzke; úrovne a typu prístupu potrebného na vykonanie zneužitia; či už existujú kompenzačné kontroly na zmiernenie zneužitia.

Napríklad smartfón môže mať zraniteľnosť, ktorá by útočníkovi umožnila obísť bezpečnostné opatrenia (napr. preskočiť kontrolu hesla), ale aby toho dosiahol, útočník potrebuje fyzický prístup k zariadeniu a invazívne fyzické zasahovanie (napr. použitie lasera na spôsobenie poruchy), aby mohol zneužitie využiť. Na základe posúdenia rizika môže výrobca dospieť k záveru, že táto zraniteľnosť sa nepovažuje za zneužívateľnú, pretože ju nie je možné rozumne zneužiť v praktických prevádzkových podmienkach.

#### 4.2.3 Ako by mali výrobcovia postupovať v prípade známych zneužívateľných zraniteľností, ktoré je možné zneužiť a ktoré boli zistené po uvedení produktu na trh, ale predtým, ako sa dostal k konečnému používateľovi?

Produkt s digitálnymi prvkami môže byť uvedený na trh a vstúpiť do distribučného reťazca určitý čas predtým, ako sa dostane k konečnému používateľovi. Tak je to často napríklad v prípade, keď je produkt zaslaný do distribučnej pobočky výrobcu, alebo je ponúkaný na predaj online alebo prostredníctvom iných prostriedkov predaja na diaľku a je odovzdaný poskytovateľom služieb na doručenie, pričom sa k konečnému používateľovi dostane niekoľko dní alebo mesiacov po uvedení na trh. Napríklad notebook môže zostať určitý čas na polici v obchode s elektronikou, než sa dostane k používateľovi.

V období medzi uvedením na trh a transakciou s konečným používateľom môžu byť objavené známe zneužívateľné zraniteľnosti, ktoré ovplyvňujú daný produkt. Povinnosť dodávať na základe posúdenia rizika produkty bez známych zneužívateľných zraniteľností sa však uplatňuje v okamihu uvedenia na trh (článok 13 ods. 1). Keďže produkt už bol uvedený na trh, od výrobcov sa preto neočakáva, že budú opravovať novo objavené zraniteľnosti, pokiaľ ich produkty ešte nedosiahli svojho používateľa.

Keďže CRA stanovuje aj požiadavky na riešenie zraniteľností, ktoré sa uplatňujú počas obdobia podpory produktu, výrobcovia musia v súvislosti s rizikami, ktoré predstavujú produkty s digitálnymi prvkami, bezodkladne riešiť a odstraňovať zraniteľnosti v súlade s prílohou I časť II bod 2. Napríklad vzhľadom na riziko, ktoré predstavujú novo objavené zraniteľnosti, ktoré možno zneužiť, výrobca notebookov stanoví, že na odstránenie týchto zraniteľností je potrebná bezpečnostná aktualizácia. Od výrobcu sa môže vyžadovať, aby poskytol bezpečnostnú aktualizáciu pre notebook hneď, ako ho používateľ uvedie do prevádzky.

#### 4.2.4 Ako funguje požiadavka zabezpečenia na úrovni štandardného nastavenia (secure by default)?

*Na základe posúdenia kybernetickobezpečnostných rizík uvedeného v článku 13 ods. 2 a podľa potreby sa produkty s digitálnymi prvkami: [...] sprístupňujú na trhu v konfigurácii zabezpečenej na úrovni štandardného nastavenia, pokiaľ sa výrobca a komerčný používateľ v súvislosti s individualizovaným produktom s digitálnymi prvkami nedohodnú inak, vrátane možnosti vrátiť nastavenie produktu na pôvodné (príloha I časť I bod 2 písm. b)).*

Výrobcovia sú povinní uvádzať produkty s digitálnymi prvkami na trh s konfiguráciou na úrovni štandardného nastavenia (secure by default), so zreteľom na zamýšľaný účel a odôvodnene predvídateľné použitie daného produktu a na základe posúdenia kybernetickobezpečnostného rizika výrobcu.

Ak výrobcovia uvádzajú na trh komponent určený na integráciu do iného produktu s digitálnymi prvkami, nemajú kontrolu nad tým, ako výrobca, ktorý komponent integruje, upraví jeho konfiguráciu. Povinnosť zabezpečiť konfiguráciu, ktorá je štandardne zabezpečená

(secure by default), sa preto vzťahuje len na komponent, ak je uvedený na trh samostatne, a nie na to, ako ho neskôr konfigurujú alebo nasadzujú výrobcovia, ktorí ho integrujú.

Napríklad výrobca kryptografickej knižnice môže byť na základe svojho posúdenia rizika povinný uvádzať túto knižnicu na trh s predvolene deaktivovanými nezabezpečenými alebo zastaranými algoritmami alebo s predvolene aktivovanou validáciou certifikátov. Integrátor môže pri vývoji svojho vlastného produktu s digitálnymi prvkami rozhodnúť o zmene niektorých z týchto nastavení. Výrobca kryptografickej knižnice je zodpovedný iba za konfiguráciu, s ktorou je knižnica dodávaná, a nie za následné úpravy, ktoré vykoná integrátor.

Podobne môže byť výrobca mikrokontroléra s integrovaným sieťovým zásobníkom na základe svojho posúdenia rizika povinný uvádzať mikrokontrolér na trh s predvolene deaktivovanými sieťovými rozhraniami. Integrátor môže potom rozhodnúť o ich aktivácii, aby splnil zamýšľaný účel svojho vlastného produktu. Výrobca mikrokontroléra je zodpovedný iba za konfiguráciu, s ktorou je mikrokontrolér dodávaný, a nie za následné úpravy, ktoré vykoná integrátor.

Ďalšie informácie o výnimkách z konfigurácie predvolenej bezpečnosti nájdete v položke 4.2.5 *Kedy je produkt „vyrobený na mieru“? Aká dokumentácia sa v týchto prípadoch vyžaduje?*

Nakoniec je možné, že táto základná požiadavka sa nevzťahuje na niektoré produkty s digitálnymi prvkami. Ďalšie usmernenia k tejto otázke nájdete v bode 4.1.3 *Musí výrobca implementovať všetky základné požiadavky?*

#### 4.2.5 Kedy je produkt „vyrobený na mieru“? Aká dokumentácia sa v týchto prípadoch vyžaduje?

*Výrobcovia by mali svoje produkty s digitálnymi prvkami sprístupniť na trhu so štandardne zabezpečenou konfiguráciou a používateľom bezplatne poskytovať bezpečnostné aktualizácie. Výrobcovia by mali mať možnosť odchyliť sa od základných požiadaviek kybernetickej bezpečnosti len v súvislosti s produktmi na mieru, ktoré sú namontované na konkrétny účel pre konkrétno komerčného používateľa, a ak výrobca aj používateľ výslovne súhlasili s iným súborom zmluvných podmienok (odôvodnenie 64).*

CRA stanovuje, že výrobcovia sa môžu odchyliť od dvoch základných požiadaviek (konkrétne od požiadavky na štandardne zabezpečenou konfiguráciu (secure by default) v bode 2 písm. b) prílohy I časť I a poskytovanie bezpečnostných aktualizácií používateľom bezplatne v bode 8 prílohy I, časť II) v súvislosti s produktmi vyrobenými na mieru, ktoré sú prispôsobené konkrétnemu účelu pre konkrétno podnikového používateľa a v prípade, že výrobca aj používateľ výslovne súhlasili s odlišnými zmluvnými podmienkami, ako je uvedené v uvedených bodoch prílohy I, časť I.

To by mohol byť napríklad prípad hardvéru alebo softvéru vyvinutého na mieru, ktorý je navrhnutý tak, aby spĺňal potreby konkrétno podnikového používateľa, alebo produktov, ktoré sú vyvinuté na integráciu do vysoko riadených prostredí konkrétno zákazníka (napr.

uzavreté siete alebo prostredia so vzduchovou medzerou) a podliehajú osobitným zmluvným podmienkam.

Na druhej strane, produkt nie je vyrobený na mieru, ak pred predajom zákazníkovi prechádza menej podstatnými úpravami bez osobitných zmluvných podmienok alebo dohôd. Tak je to napríklad v prípade platformy na manažment vzťahov so zákazníkmi (CRM), ktorá sa predáva viacerým podnikom, aj keď výrobca umožňuje niektoré menej významné úpravy, alebo v prípade platforiem, ktoré používajú na úpravy doplnky alebo rozhrania API, ale v podstate sú pre každého zákazníka rovnakým produktom.

V súlade s článkom 31 sa od výrobcu očakáva, že do svojej technickej dokumentácie zahrnie všetky relevantné údaje alebo podrobnosti, ktoré preukazujú, že jeho produkt spĺňa príslušné základné požiadavky kybernetickej bezpečnosti, vrátane primeraných dôkazov, ktoré preukazujú, že produkt je vyrobený na mieru.

## 4.3 Povinnosti v oblasti riešenia zraniteľností (príloha I, časť II)

### 4.3.1 Sú výrobcovia povinní aplikovať záplaty na všetky zraniteľnosti, ktoré boli zistené počas obdobia podpory?

*Výrobcovia produktov s digitálnymi prvkami musia [...] vo vzťahu k rizikám, ktorým sú vystavené produkty s digitálnymi prvkami, bezodkladne riešiť a napravujú zraniteľnosti, a to aj poskytovaním bezpečnostných aktualizácií; ak je to technicky možné, nové bezpečnostné aktualizácie sa poskytujú oddelene od aktualizácií funkcií (príloha I, časť II, bod 2).*

CRA nevyžaduje, aby výrobcovia poskytovali záplaty všetkých zraniteľností, ktoré sa zistia počas obdobia podpory produktu. Pri zistení zraniteľnosti sa od výrobcov očakáva, že v rámci posúdenia rizika výrobcami určia jej relevantnosť pre svoj produkt a posúdia výsledné riziko. Na základe rizika, ktoré zraniteľnosť predstavuje, musia výrobcovia zabezpečiť, aby boli bezodkladne prijaté nápravné opatrenia. CRA preto nepredpisuje, aby výrobcovia poskytovali záplaty pre všetky zraniteľnosti, ktoré sa zistia počas obdobia podpory produktu.

V závislosti od rizika môžu nápravné opatrenia nadobúdať rôzne formy, vrátane, ale nielen, okamžitých záplat, odporúčaní týkajúcich sa dočasných riešení, ktoré budú neskôr doplnené aktualizáciami softvéru, aktualizáciami používateľských príručiek, pokynmi na konfiguráciu s cieľom deaktivovať postihnuté vlastnosti.

Napríklad výrobca inteligentného domáceho rozbočovača zistí vo svojom produkte zraniteľnosť, ktorá umožňuje vzdialeným útočníkom vykonávať ľubovoľný kód na rozbočovači; posúdenie rizika výrobcu ukazuje, že existuje vysoké riziko kompromitácie, pretože útočník by mohol riadiť iné pripojené zariadenia. Od výrobcu sa môže očakávať, že napríklad poskytne okamžitú záplatu a vhodné pokyny svojim používateľom.

Na druhej strane, výrobca Wi-Fi routera zistí zraniteľnosť pretečenia vyrovnávacej pamäte v jednej zo softvérových knižníc obsiahnutých vo firmvéri routera; posúdenie rizika výrobcu však ukazuje, že zraniteľnosť nemožno zneužiť, pretože funkcie knižnice sa vo firmvéri nikdy nevyvolávajú. Od výrobcu sa môže očakávať, že napríklad zdokumentuje zraniteľnosť, ale môže sa rozhodnúť, že ju nebude opravovať špeciálnou aktualizáciou. Od výrobcu sa môže tiež očakávať, že napríklad odstráni nepoužívanú knižnicu v ďalšej pravidelnej verzii firmvéru.

Nakoniec výrobca kancelárskej laserovej tlačiarne zistí, že základná doska tlačiarne má rozhranie na ladenie, ktoré zostáva aktivované. Hoci by sa táto zraniteľnosť mohla teoreticky zneužiť na obídenie autentizácie a vloženie škodlivého kódu, jej zneužitie si vyžaduje fyzický prístup k tlačiarne, porušenie jej bezpečnostnej plomby, rozobratie vnútorných komponentov a spájkovanie na základnej doske. Posúdenie rizika výrobcu ukazuje, že táto zraniteľnosť predstavuje veľmi nízke riziko a v prevádzkovom prostredí sa nedá zneužiť. Od výrobcu sa môže očakávať, že napríklad zdokumentuje zraniteľnosť, aktualizuje svoju technickú dokumentáciu a poskytne svojim používateľom vhodné odporúčania.

#### 4.3.2 Musí výrobca riešiť a odstraňovať zraniteľnosti vo všetkých verziách softvérového produktu?

*Ak výrobca uviedol na trh následné podstatne upravené verzie softvérového produktov, môže zabezpečiť súlad so základnou požiadavkou kybernetickej bezpečnosti stanovenou v bode 2 časti II prílohy I len v prípade verzie, ktorú naposledy uviedol na trh, za predpokladu, že používatelia verzií, ktoré boli uvedené na trh predtým, majú bezplatný prístup k verzii naposledy uvedenej na trh a nevznikajú im dodatočné náklady na úpravu hardvérového a softvérového prostredia, v ktorom používajú pôvodnú verziu tohto produktu. (článok 13.10).*

Odôvodnenie 40 podrobne vysvetľuje ustanovenie článku 13.10 a objasňuje, že výrobcovia nie sú povinní riešiť a odstraňovať zraniteľnosti všetkých verzií softvérového produktu, ak sú splnené určité kritéria.

Konkrétne, „Vzhľadom na cyklický charakter vývoja softvéru by výrobcovia, ktorí uviedli na trh nové verzie softvérového produktu v dôsledku následnej podstatnej úpravy tohto produktu, mali mať možnosť poskytovať bezpečnostné aktualizácie počas obdobia podpory len pre verziu softvérového produktu, ktorú uviedli na trh naposledy. Mali by mať možnosť tak urobiť, len ak používatelia príslušných predchádzajúcich verzií produktu majú bezplatný prístup k verzii produktu, ktorá bola naposledy uvedená na trh, a nevznikajú im dodatočné náklady na prispôbienie hardvérového alebo softvérového prostredia, v ktorom produkt prevádzkujú. Mohlo by ísť napríklad o prípad, keď si modernizácia operačného systému pre stolové počítače nevyžaduje nový hardvér, napríklad rýchlejší centrálny procesor alebo väčšiu pamäť. Výrobca by však mal počas obdobia podpory naďalej spĺňať ďalšie požiadavky na riešenie zraniteľností, ako je politika koordinovaného zverejňovania zraniteľností alebo opatrenia na uľahčenie

výmeny informácií o potenciálnych zraniteľnostiach pre všetky následné podstatne upravené verzie softvérového produktu uvedeného na trh. Výrobcovia by mali mať možnosť poskytovať menšie bezpečnostné alebo funkčné aktualizácie, ktoré nepredstavujú podstatnú úpravu, len pre poslednú verziu alebo čiastkovú verziu softvérového produktu, ktorý nebol podstatne upravený. Ak zároveň hardvérový produkt, napríklad smartfón, nie je kompatibilný s najnovšou verziou operačného systému, s ktorým bol pôvodne dodaný, výrobca by mal naďalej poskytovať bezpečnostné aktualizácie aspoň pre poslednú kompatibilnú verziu operačného systému počas obdobia podpory.“ (odôvodnenie 40).

#### 4.3.3 Je výrobca zodpovedný za inštaláciu bezpečnostných aktualizácií používateľmi produktu?

Jedným z najdôležitejších opatrení, ktoré majú používatelia prijať na ochranu svojich produktov s digitálnymi prvkami pred kybernetickými útokmi, je čo najskôr nainštalovať najnovšie dostupné bezpečnostné aktualizácie. Výrobcovia by preto mali navrhovať svoje produkty a zavádzať postupy tak, aby zabezpečili, že produkty s digitálnymi prvkami zahŕňajú funkcie, ktoré umožňujú automatické oznamovanie, distribúciu, sťahovanie a inštaláciu bezpečnostných aktualizácií, najmä v prípade spotrebných produktov. Mali by tiež umožniť v poslednom kroku súhlas so stiahnutím a inštaláciou bezpečnostných aktualizácií. Používatelia by mali mať ponechanú možnosť deaktivovať automatické aktualizácie jasným a ľahko použiteľným mechanizmom a so zrozumiteľným návodom na vypnutie aktualizácie. Požiadavky týkajúce sa automatických aktualizácií stanovené v prílohe k tomuto nariadeniu sa neuplatňujú na produkty s digitálnymi prvkami, ktoré sú primárne určené na integráciu ako komponenty do iných produktov. Nevzťahujú sa ani na produkty s digitálnymi prvkami, v prípade ktorých používatelia dôvodne neočakávajú automatické aktualizácie vrátane produktov s digitálnymi prvkami, ktoré sa majú používať v profesionálnych sieťach informačných a komunikačných technológií, a najmä v kritickom a priemyselnom prostredí, v ktorom by automatická aktualizácia mohla spôsobiť zasahovanie do prevádzky. Bez ohľadu na to, či je produkt s digitálnymi prvkami navrhnutý tak, aby prijímal automatické aktualizácie alebo nie, jeho výrobca by mal používateľov informovať o zraniteľnostiach a bezodkladne poskytnúť bezpečnostné aktualizácie. Ak má produkt s digitálnymi prvkami používateľské rozhranie alebo podobné technické prostriedky umožňujúce priamu interakciu s používateľmi, výrobca by mal takéto funkcie využiť na informovanie používateľov o tom, že ich produkt s digitálnymi prvkami dosiahol koniec obdobia podpory. Oznámenia by sa mali obmedziť na to, čo je potrebné na zabezpečenie účinného prijímania týchto informácií, a nemali by mať negatívny vplyv na skúsenosti používateľov s produktom s digitálnymi prvkami (odôvodnenie 56).

Produkty s digitálnymi prvkami sa na trhu sprístupnia, len ak: a) spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I za predpokladu, že sú riadne nainštalované, udržiavané, používané na ich zamýšľaný účel alebo za podmienok, ktoré možno

*odôvodnene predvídať, a prípadne s nainštalovanými potrebnými aktualizáciami; a b) postupy zavedené výrobcom sú v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I (článok 6).*

*Na základe posúdenia kybernetickobezpečnostného rizika uvedeného v článku 13 ods. 2 a v prípade potreby produkty s digitálnymi prvkami: c)zaisťujú, aby zraniteľnosti bolo možné riešiť bezpečnostnými aktualizáciami, prípadne aj automatickými bezpečnostnými aktualizáciami, ktoré sa inštalujú v primeranom čase aktiváciou podľa predvoleného nastavenia, s jasnou a ľahko použiteľnou možnosťou pre používateľa odmietnuť ich po oznámení o dostupných aktualizáciách a možnosti ich dočasného odkladu (príloha I, časť I, bod 2 písm. c)).*

*Výrobcovia produktov s digitálnymi prvkami: (7)zaisťujú mechanizmy bezpečnej distribúcie aktualizácií pre produkty s digitálnymi prvkami s cieľom zabezpečiť včasnú opravu zraniteľností alebo ich zmiernenie a aby sa v relevantnom prípade bezpečnostné aktualizácie uskutočňovali automaticky (príloha I, časť II, bod 7).*

*Výrobcovia produktov s digitálnymi prvkami: (8) ak sú k dispozícii bezpečnostné aktualizácie na riešenie zistených bezpečnostných problémov, zabezpečujú ich bezodkladné šírenie a ak sa výrobca a komerčný používateľ nedohodli v súvislosti s individualizovaným produktom s digitálnymi prvkami inak, bezplatné šírenie sprievodných informačných správ s relevantnými informáciami pre používateľov, aj o možných potrebných krokoch (Príloha I, časť II, bod 8).*

CRA zavádza rad mechanizmov, ktoré vyžadujú, aby výrobcovia zabezpečili, že bezpečnostné aktualizácie sa bezodkladne šíria, že sa tieto aktualizácie inštalujú automaticky, ak je to možné, a že používatelia produktov s digitálnymi prvkami sú riadne informovaní. CRA tiež uznáva, že automatické aktualizácie nie sú vždy použiteľné a používatelia by mali mať možnosť odložiť inštaláciu týchto aktualizácií.

Výrobca nie je podľa CRA zodpovedný, ak používateľ neinštaluje bezpečnostné aktualizácie, napr. ak aktualizácie nie sú inštalované buď preto, že automatické aktualizácie nie sú použiteľné, alebo preto, že používateľ sa rozhodol pre odhlásenie.

#### 4.3.4 Musí výrobca stiahnuť produkt z trhu, ak nedokáže odstrániť zraniteľnosť?

*Od uvedenia na trh a počas obdobia podpory výrobcovia, ktorí majú vedomosť alebo dôvod domnievať sa, že produkt s digitálnymi prvkami alebo nimi zavedené postupy nie sú v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, bezodkladne prijímú podľa vhodnosti nápravné opatrenia potrebné na uvedenie tohto produktu s digitálnymi prvkami alebo postupov výrobcu do súladu s príslušnými požiadavkami alebo na stiahnutie produktu z trhu alebo od používateľa (článok 13 ods. 21).*

Ako sa vysvetľuje v bode 4.3.1 Sú výrobcovia povinní urobiť záplatu všetkých zraniteľností, ktoré sa zistia počas obdobia podpory?, výrobca je povinný v súvislosti s rizikami, ktoré

predstavujú, riešiť a odstraňovať zraniteľnosti počas obdobia podpory. Vhodné nápravné opatrenia môžu mať rôzne formy, vrátane zmierňujúcich opatrení.

Za určitých okolností je však možné, že zraniteľnosť, ktorá predstavuje veľmi významné riziko kompromitácie, najmä v prípade hardvérového produktu s digitálnymi prvkami, nemožno primerane riešiť a odstrániť a produkt nemožno uviesť do zhoda. V takýchto prípadoch, ktoré budú pravdepodobne výnimočné, môže byť výrobca povinný podľa potreby stiahnuť alebo spätne prevziať produkt.

Je pravdepodobné, že za takýchto okolností budú zapojené príslušné orgány dohľadu nad trhom a že sa aktivujú príslušné postupy stanovené v článkoch 54 až 58 CRA.

#### 4.3.5 Ako by mali výrobcovia zabezpečiť oddelenie aktualizácií bezpečnosti a funkcionality, najmä ak aktualizácie slúžia obom účelom?

*Výrobcovia produktov s digitálnymi prvkami: (2)vo vzťahu k rizikám, ktorým sú vystavené produkty s digitálnymi prvkami, bezodkladne riešia a naprávajú zraniteľnosti, a to aj poskytovaním bezpečnostných aktualizácií; ak je to technicky možné, nové bezpečnostné aktualizácie sa poskytujú oddelene od aktualizácií funkcií (príloha I, časť II, bod 2).*

*S cieľom zlepšiť transparentnosť procesov riešenia zraniteľností a zabezpečiť, aby používatelia neboli povinní inštalovať nové aktualizácie funkcií výlučne na účely prijímania najnovších bezpečnostných aktualizácií, by výrobcovia mali zabezpečiť, ak je to technicky možné, aby sa nové bezpečnostné aktualizácie poskytovali oddelene od aktualizácií funkcií (odôvodnenie 57).*

CRA stanovuje, že výrobcovia by mali, ak je to technicky možné, poskytovať nové bezpečnostné aktualizácie oddelene od aktualizácií funkcionality, aby sa zabezpečilo, že aktualizácie môžu byť dodávané bezodkladne a že používatelia nie sú povinní inštalovať aktualizácie funkcionality, aby mohli získať najnovšie bezpečnostné aktualizácie.

Výrobcovia, ktorí vydávajú bezpečnostnú aktualizáciu na odstránenie zraniteľnosti, nesmú túto aktualizáciu spájať s inými aktualizáciami funkcionality. Napríklad inteligentné domáce zariadenie má zraniteľnosť v procese overovania certifikátov SSL, ktorá útočníkovi umožňuje vykonať útok typu „man-in-the-middle“. Na odstránenie tejto zraniteľnosti stačí, aby výrobca aktualizoval rutinu overovania certifikátov SSL. Výrobca by mal túto aktualizáciu poskytovať samostatne, bez spájania bezpečnostnej opravy s inými aktualizáciami súvisiacimi s funkcionalitou.

Ak je však na dodanie bezpečnostnej aktualizácie potrebná aktualizácia funkcionality, základné požiadavky nebránia výrobcovi dodať aktualizáciu, ktorá kombinuje bezpečnostné a funkčné úpravy. Napríklad čítačka PDF má zraniteľnosť, ktorá je obsiahnutá v zastaranom parserovi formátu súborov a ktorá spúšťa pretečenie vyrovnávacej pamäte. Oprava má požiadavku na nahradenie parseru formátu súborov novým, bezpečnejším parserom s podporou mierne

odlišného správania (napr. prísnejšiu kontrolu formátu) a ktorý môže viesť k určitým zmenám funkcionality, pretože niektoré súbory, ktoré predtým fungovali, môžu byť teraz odmietnuté. Keďže by to nebolo technicky realizovateľné, výrobca nie je povinný zabezpečiť oddelenie týchto typov softvérových úprav.

Podobne, v určitých situáciách môže aktualizácia funkcionality sama osebe zodpovedať bezpečnostnej aktualizácii. Napríklad produkt s digitálnymi prvkami pristupuje k tej istej vlastnosti prostredníctvom rôznych rozhraní (napr. webové rozhranie, rozhranie mobilnej aplikácie, rozhranie príkazového riadku, koncový bod API). Ak jedno z týchto rozhraní obsahuje zraniteľnosť, výrobca môže určiť, že je potrebné toto zraniteľné rozhranie deaktivovať, čím poskytne aktualizáciu funkcionality, ktorá je zároveň bezpečnostnou aktualizáciou.

#### 4.3.6 Ako by sa mali riešiť a odstraňovať zraniteľnosti v integrovaných komponentoch?

*Povinnosti riešiť zraniteľnosti stanovené v tomto nariadení, ktoré sú výrobcovia povinní dodržiavať pri uvádzaní produktu s digitálnymi prvkami na trh a počas obdobia podpory, sa vzťahujú na produkty s digitálnymi prvkami v ich celistvosti, ako aj na všetky integrované komponenty. Ak pri vykonávaní náležitej starostlivosti výrobca produktu s digitálnymi prvkami zistí zraniteľnosť komponentu, a to aj komponentu, ktorý obsahuje slobodný softvér a softvér s otvoreným zdrojovým kódom, mal by informovať osobu alebo subjekt, ktorý komponent vyrába alebo poskytuje jeho údržbu, riešiť a napraviť zraniteľnosť a prípadne poskytnúť tejto osobe alebo subjektu používanú bezpečnostnú nápravu (odôvodnenie 34).*

Výrobcovia musia počas obdobia podpory plniť požiadavky týkajúce sa riešenia zraniteľností v súvislosti so svojimi produktmi v celom rozsahu, a to aj riešením zraniteľností, ktoré ovplyvňujú ich produkty a sú obsiahnuté v integrovaných komponentoch. Pozri tiež 4.3.1. Sú výrobcovia povinní aplikovať záplaty na všetky zraniteľnosti, ktoré sa zistia počas obdobia podpory?

Ak výrobca produktu integroval komponent, ktorý bol uvedený na trh po nadobudnutí účinnosti CRA (t. j. komponent je sám osebe produktom podľa CRA), tento výrobca sa môže spoľahnúť na opatrenia, ktoré je výrobca komponentu povinný podniknúť, aby splnil svoje vlastné povinnosti v oblasti riešenia zraniteľností. Napríklad výrobca komponentu môže byť povinný vyvinúť bezpečnostnú aktualizáciu na opravu zraniteľnosti v komponente. Výrobca, ktorý integruje komponenty, je naďalej povinný plniť svoje povinnosti týkajúce sa riešenia zraniteľnosti svojho produktu, napríklad informovaním používateľov, poskytovaním opatrení na zmiernenie rizika, aktualizáciou dokumentácie, ale jeho povinnosti týkajúce sa riešenia zraniteľnosti sú zmiernené príslušnými povinnosťami výrobcu komponentov.

Ak výrobca integroval komponent, ktorý nebol uvedený na trh (alebo ktorý bol uvedený na trh pred uplatnením CRA), osoba alebo subjekt, ktorý komponent vyvinul, nepodlieha povinnostiam CRA v oblasti riešenia zraniteľností. Integrátor je však povinný zabezpečiť, aby jeho produkt v celom rozsahu spĺňal požiadavky na riešenie zraniteľnosti. Ak osoba alebo

subjekt, ktorý komponent vyvinul, neposkytuje podporu výrobcovi pri riešení a odstraňovaní zraniteľností, integrujúci výrobca by mal riešiť zraniteľnosť inými prostriedkami, napríklad deaktivovaním kompromitovaných funkcií, výmenou postihnutého komponentu alebo vyvinutím vlastnej záplaty (napríklad v prípade, že komponent je komponentom s otvoreným zdrojovým kódom).

V súlade s článkom 13 ods. 6, ak integrujúci výrobca vyvinie záplatu pre komponent, je vyžadované, aby ju zdieľal s osobou alebo subjektom, ktorý komponent udržiava.

#### 4.3.7 Aký vplyv má koniec obdobia podpory integrovanej súčasti na súlad produktu s CRA?

*Pri určovaní obdobia podpory môžu výrobcovia zohľadniť aj obdobia podpory produktov s digitálnymi prvkami s podobnou funkciou, ktoré na trh uvádzajú iní výrobcovia, dostupnosť prevádzkového prostredia, obdobia podpory integrovaných komponentov so základnými funkciami, ktoré pochádzajú od tretích strán[...] (článok 13 ods. 8).*

Výrobcovia musia počas trvania obdobia podpory dodržiavať povinnosti týkajúce sa riešenia zraniteľností pre svoje produkty ako celok, vrátane všetkých integrovaných komponentov, ale môžu sa spoliehať na povinnosti týkajúce sa riešenia zraniteľností, ktorým podliehajú aj výrobcovia komponentov, ako sa uvádza v bode 4.3.6. *Ako by sa mali riešiť a odstraňovať zraniteľnosti v integrovaných komponentoch?*

Obdobie podpory integrovaných komponentov je faktor, ktorý môžu výrobcovia zohľadniť pri určení obdobia podpory svojich produktov, aby sa uistili, že sú schopní využiť obdobie podpory kľúčových komponentov na riešenie a odstránenie zraniteľností produktu. Pozri tiež časť 4.5 *Obdobie podpory*.

Môže sa však stať, že produkt s aktívnym obdobím podpory obsahuje zraniteľnosť v integrovanom komponente, na ktorý sa už nevzťahuje obdobie podpory tohto komponentu, a túto zraniteľnosť nie je možné primerane riešiť a odstrániť prostredníctvom rôznych foriem zmierňujúcich opatrení (pozri tiež bod 4.3.1 *Sú výrobcovia povinní aplikovať záplaty na všetky zraniteľnosti, ktoré sa zistia počas obdobia podpory?* V takom prípade je výrobca produktu povinný odstrániť zraniteľnosť inými prostriedkami, napríklad výmenou integrovaného komponentu alebo autonómnymi opravami.

## 4.4 Požiadavky na náležitú starostlivosť pri integrácii komponentov

### 4.4.1 Čo CRA predpisuje pri integrácii komponentov?

*Výrobcovia pri uvádzaní produktu s digitálnymi prvkami na trh zaistia, aby bol navrhnutý, vyvinutý a vyrobený v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti I prílohy I.I (článok 13 ods. 1).*

*Na účely dosiahnutia súladu s odsekom 1 výrobcovia uplatňujú náležitú starostlivosť pri integrácii komponentov získaných od tretích strán tak, aby tieto komponenty neohrozovali kybernetickú bezpečnosť produktu s digitálnymi prvkami, a to aj pri integrácii komponentov slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktoré neboli sprístupnené na trhu v priebehu obchodnej činnosti. (článok 13 ods. 5).*

*Pri integrácii komponentov získaných od tretích strán do produktov s digitálnymi prvkami vo fáze návrhu a vývoja by výrobcovia s cieľom zabezpečiť, aby sa produkty navrhovali, vyvíjali a vyrábali v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v tomto nariadení, mali uplatňovať náležitú starostlivosť, pokiaľ ide o tieto komponenty vrátane komponentov so slobodným softvérom a softvérom s otvoreným zdrojovým kódom, ktoré neboli sprístupnené na trhu. Primeraná úroveň náležitej starostlivosti závisí od povahy a úrovne kybernetickobezpečnostného rizika spojeného s daným komponentom a na tento účel by mala zahŕňať jedno alebo viaceré z týchto opatrení: podľa potreby overenie, či výrobca komponentu preukázal zhodu s týmto nariadením, a to aj kontrolou toho, či komponent už má označenie CE; overenie, či je komponent pravidelne aktualizovaný na účely bezpečnosti, napríklad kontrolou histórie jeho bezpečnostných aktualizácií; overenie, či komponent neobsahuje zraniteľnosti zaznamenané v európskej databáze zraniteľností zriadenej podľa článku 12 ods. 2 smernice (EÚ) 2022/2555 alebo v iných verejne prístupných databázach zraniteľností; alebo vykonanie dodatočných bezpečnostných testov[...] (Odôvodnenie 34).*

*Ihneď po prechodnom období na uplatňovanie tohto nariadenia výrobca produktu s digitálnymi prvkami, ktorý integruje jeden alebo viacero komponentov od tretích strán, na ktoré sa takisto vzťahuje toto nariadenie, nemusí byť schopný v rámci svojej povinnosti náležitej starostlivosti overiť, či výrobcovia týchto komponentov preukázali zhodu s týmto nariadením, napríklad overením toho, či tieto komponenty už majú označenie CE. Môže ísť o prípad, keď komponenty boli integrované skôr, ako sa toto nariadenie začne uplatňovať na výrobcov týchto komponentov. V tom prípade by mal výrobca, ktorý takéto komponenty integruje, uplatňovať náležitú starostlivosť inými prostriedkami (odôvodnenie 35).*

Aby sa zabezpečilo, že ich produkt s digitálnymi prvkami spĺňa základné požiadavky CRA, výrobcovia musia pri integrácii komponentov tretích strán do svojich produktov postupovať s náležitou starostlivosťou.

Výrobcovia môžu integrovať rôzne typy komponentov, vrátane tých, ktoré nemajú označenie CE (napr. voľné a otvorené komponenty, ktoré nespádajú do pôsobnosti CRA, komponenty

uvedené na trh pred uplatňovaním CRA alebo komponenty, ktoré neboli uvedené na trh), ale musia však zabezpečiť, aby takéto komponenty neohrozovali kybernetickú bezpečnosť ich produktov s digitálnymi prvkami.

Pri integrácii komponentov, ktoré majú označenie CE, sa výrobcovia môžu spoľahnúť na EÚ vyhlásenie o zhode pre daný komponent a sprievodnú dokumentáciu, ktoré poskytujú podporu preukázaniu vlastného súladu s CRA.

Vhodná úroveň náležitej starostlivosti závisí od povahy a úrovne kybernetickobezpečnostného rizika daného komponentu – pozri tiež položku 4.4.2 *Aká je vhodná úroveň náležitej starostlivosti?*

#### 4.4.2 Aká je primeraná úroveň náležitej starostlivosti?

Vhodná úroveň náležitej starostlivosti závisí od povahy a úrovne kybernetickobezpečnostného rizika daného komponentu a jej cieľom je zabezpečiť, aby integrované komponenty neohrozovali kybernetickú bezpečnosť výrobcu produktu s digitálnymi prvkami. Posudzovanie rizika produktu s digitálnymi prvkami tiež poskytuje informáciu o primeranej úrovni náležitej starostlivosti. Ak je komponent alebo produkt spojený s väčším rizikom, opatrenia, ktoré by mal výrobca podniknúť pri vykonávaní náležitej starostlivosti, by mali byť rozsiahlejšie ako v prípade komponentu alebo produktu spojeného s menším rizikom. V súlade s odôvodnením 34 príklady jedného alebo viacerých opatrení, ktoré môžu výrobcovia podniknúť, zahŕňajú:

- kontrola, či komponent už nesie označenie CE;
- overenie, či komponent dostáva pravidelné bezpečnostné aktualizácie, napríklad kontrolou histórie jeho bezpečnostných aktualizácií;
- overenie v európskej databáze zraniteľností zriadenej podľa článku 12 ods. 2 smernice (EÚ) 2022/2555 alebo iných verejne prístupných databázach zraniteľností alebo iných verejne prístupných databázach zraniteľností tých zraniteľností, ktoré sa vzťahujú na komponent, a navrhovanie, vývoj a výroba produktu s digitálnymi prvkami, ktoré integrujú komponent takým spôsobom, aby tieto zraniteľnosti neohrozovali kybernetickú bezpečnosť produktu s digitálnymi prvkami;
- vykonávanie dodatočných bezpečnostných skúšok, ako sú fuzz testovanie, penetračné testovanie, analýza firmvéru, analýza bočných kanálov, red teaming, analýza sieťovej prevádzky, spoofing senzorov.

Ďalšie príklady opatrení, ktoré môžu výrobcovia podniknúť, zahŕňajú:

- výkonnosť analýzy zloženia softvéru komponentov;
- sandboxovanie alebo izolovanie vysoko kritických komponentov;
- ak je k dispozícii, preskúmavanie SBOM danej komponenty;
- kontrola doby podpory komponentu;
- overenie, či zamýšľaný účel komponentu zodpovedá použitiu integrátorom;
- posudzovanie bezpečnostnej situácie výrobcu komponentu.

#### 4.4.3 Aby výrobca konal s náležitou starostlivosťou, mal by integrovať iba komponenty, ktoré nesú označenie CE?

V súlade s článkom 13 ods. 5 môžu výrobcovia integrovať rôzne typy komponentov, vrátane komponentov, ktoré neboli uvedené na trh alebo ktoré boli uvedené na trh pred uplatnením CRA, za predpokladu, že vykonajú náležitú starostlivosť, aby sa uistili, že komponent nevedie k ohrozeniu kybernetickej bezpečnosti ich vlastného produktu s digitálnymi prvkami.

Výrobca nemusí pred integráciou takýchto komponentov zabezpečiť ich súlad so základnými požiadavkami stanovenými v prílohe I časti I.<sup>8</sup>

Výrobca však musí zabezpečiť, aby jeho vlastné produkty s digitálnymi prvkami boli bezpečné a spĺňali základné požiadavky CRA, pričom náležitá starostlivosť je kľúčovou povinnosťou na splnenie týchto požiadaviek. Výrobca je tiež povinný počas celého obdobia podpory dodržiavať povinnosti týkajúce sa riešenia zraniteľností uvedené v časti II prílohy I, a to v plnom rozsahu pre svoje produkty.

Integrácia komponentov, ktoré nesú označenie CE, môže zjednodušiť určité požiadavky (napr. pozri bod 4.3.6 *Ako by sa mali riešiť a odstraňovať zraniteľnosti v integrovaných komponentoch?*)

#### 4.4.4 Ako by mali výrobcovia vykonávať náležitú starostlivosť v súvislosti s komponentmi s otvoreným zdrojovým kódom, na ktoré sa CRA nevzťahuje?

Výrobcovia môžu integrovať komponenty s otvoreným zdrojovým kódom, ktoré nespádajú do pôsobnosti CRA (t. j. pretože nie sú sprístupnené na trhu v rámci obchodnej činnosti), ako aj komponenty s otvoreným zdrojovým kódom, ktoré zverejňuje správca softvéru s otvoreným zdrojovým kódom.

Ako sa vysvetľuje v bode 4.4.2 *Aká je primeraná úroveň náležitej starostlivosti?*, primeraná úroveň náležitej starostlivosti závisí od povahy a úrovne kybernetickobezpečnostného rizika daného komponentu s otvoreným zdrojovým kódom.

Komisia je oprávnená zaviesť dobrovoľné programy osvedčovania bezpečnosti, ktoré možno použiť na posudzovanie zhody komponentov s voľným a otvoreným zdrojovým kódom s CRA. Ak sú k dispozícii, takéto programy osvedčovania by uľahčili výrobcovi povinnosť náležitej starostlivosti.

---

<sup>8</sup> Výrobcovia takýchto komponentov sú povinní zabezpečiť, aby boli súladní s CRA, ak ich uvádzajú na trh.

## 4.5 Obdobie podpory

### 4.5.1 Aké kritéria by mal výrobca zohľadniť pri určení obdobia podpory

*Výrobcovia určia obdobie podpory s ohľadom na dĺžku predpokladaného používania produktu, pričom zohľadnia najmä primerané očakávania používateľov, povahu produktu vrátane jeho zamýšľaného účelu, ako aj príslušné právo Únie, ktorým sa určuje životnosť produktov s digitálnymi prvkami. Pri určovaní obdobia podpory môžu výrobcovia zohľadniť aj obdobia podpory produktov s digitálnymi prvkami s podobnou funkciou, ktoré na trh uvádzajú iní výrobcovia, dostupnosť prevádzkového prostredia, obdobia podpory integrovaných komponentov so základnými funkciami, ktoré pochádzajú od tretích strán, ako aj príslušné usmernenia od špecializovanej skupiny pre administratívnu spoluprácu (ďalej len „ADCO“) zriadenej podľa článku 52 ods. 15 a Komisiou. Záležitosti, ktoré sa majú zohľadniť pri určovaní obdobia podpory, sa posudzujú spôsobom, ktorým sa zabezpečí proporcionalita (článok 13 ods. 8 druhý pododsek).*

#### produktu?

Výrobcovia sú podliehajúci požiadavke určiť obdobie podpory tak, aby odzrkadľovalo dĺžku času, počas ktorého sa očakáva, že bude produkt používaný, pričom sa zohľadnia najmä:

- primerané očakávania používateľov;
- povahu produktu, vrátane jeho zamýšľaného účelu;
- iné právne predpisy Únie, ktoré určujú životnosť produktov s digitálnymi prvkami.

Medzi ďalšie relevantné faktory, ktoré môžu výrobcovia zohľadniť, patria:

- obdobie podpory podobných produktov, ktoré uviedli na trh iní výrobcovia;
- dostupnosť prevádzkového prostredia;
- obdobie podpory integrovaných komponentov tretích strán, ktoré zabezpečujú základné funkcie;
- relevantné usmernenia poskytnuté CRA ADCO.

Všetky tieto faktory by sa mali zohľadniť spôsobom, ktorý zabezpečí proporcionalitu pri určení doby podpory.

Preto sa od výrobcov neočakáva, že jednoducho stanovia obdobia podpory, ktoré zodpovedajú predpokladanej dĺžke používania (pokiaľ predpokladaná dĺžka používania nie je kratšia ako päť rokov, ako sa uvádza v *bode 4.5.2 Existuje minimálne obdobie podpory?*

V súlade s článkom 13 ods. 8 by výrobca mal do svojej technickej dokumentácie zahrnúť informácie, ktoré boli zohľadnené pri určení obdobia podpory produktu s digitálnymi prvkami.

#### 4.5.2 Existuje minimálne obdobie podpory?

*Bez toho, aby bol dotknutý druhý pod odsek, trvá obdobie podpory najmenej päť rokov. Ak sa predpokladá, že produkt s digitálnymi prvkami sa bude používať menej ako päť rokov, obdobie podpory musí zodpovedať očakávanému obdobiu používania (článok 13 ods. 8 tretí pod odsek).*

*Obdobie podpory, počas ktorého výrobca zabezpečuje účinné riešenie zraniteľností, by nemalo byť kratšie ako päť rokov, pokiaľ životnosť produktu s digitálnymi prvkami nie je kratšia ako päť rokov, pričom v takom prípade by mal výrobca zabezpečiť riešenie zraniteľností počas tejto životnosti. Ak sa dôvodne očakáva, že produkt s digitálnymi prvkami sa bude používať dlhšie ako päť rokov, ako je to často v prípade hardvérových komponentov, ako sú základné dosky alebo mikroprocesory, sieťových zariadení, ako sú smerovače, modemy alebo prepínače, ako aj softvéru, ako sú operačné systémy alebo nástroje na editovanie videí, výrobcovia by mali zabezpečiť dlhšie obdobia podpory. Najmä produkty s digitálnymi prvkami určené na použitie v priemyselnom prostredí, ako sú priemyselné riadiace systémy, sa často používajú počas výrazne dlhšieho obdobia. Výrobca by mal mať možnosť vymedziť obdobie podpory kratšie ako päť rokov, len ak je to odôvodnené povahou dotknutého produktu s digitálnymi prvkami a ak sa očakáva, že tento produkt sa bude používať menej ako päť rokov, pričom v takom prípade by obdobie podpory malo zodpovedať očakávanému času používania. Napríklad životnosť aplikácie na sledovanie kontaktov určenej na použitie počas pandémie by mohla byť obmedzená na trvanie pandémie. Okrem toho niektoré softvérové aplikácie môžu byť pre svoju povahu prístupné len s predplatným, najmä ak sa aplikácia stane pre používateľa nedostupnou, a teda po skončení predplatného sa už nepoužíva (odôvodnenie 60).*

Obdobie podpory musí byť stanovené na najmenej päť rokov, ale to nie je dostatočné, ak sa dá rozumne očakávať, že produkty s digitálnymi prvkami budú používané dlhšie ako päť rokov. Za takýchto okolností by výrobcovia mali zvážiť všetky relevantné faktory (pozri bod 4.5.1 Aké kritéria by mal výrobca zohľadniť pri určovaní obdobia podpory produktu?), ktoré môžu viesť k potrebe poskytovať podporu dlhšiu ako päť rokov.

Obdobie podpory kratšie ako päť rokov je odôvodnené len v situáciách, keď je životnosť produktu s digitálnymi prvkami kratšia ako päť rokov. V týchto prípadoch sa obdobie podpory zhoduje s predpokladanou dĺžkou používania bez ďalšieho zohľadnenia ostatných kritérií uvedených v článku 13 ods. 8. To platí pre produkty, ktoré slúžia na veľmi špecifický účel (napr. aplikácia na sledovanie kontaktov, ktorá sa používa počas pandémie), ale aj pre niektoré softvérové aplikácie, ktoré zo svojej povahy môžu byť prístupné len na základe predplatného modelu, najmä ak sa aplikácia stane pre používateľa nedostupnou po uplynutí predplatného. Napríklad niektoré antivírusové programy pre podniky fungujú len pre používateľov s aktívnym predplatným, pretože používatelia sa spoliehajú na dostupnosť aktualizovaných antivírusových definícií, a po uplynutí platnosti predplatného už nie sú dostupné. Podobne niektoré slobodné (bezplatné) a otvorené softvéry, ktoré sú uvedené na trh, môže ich výrobca speňažiť len prostredníctvom predaja platených podporných služieb

ponúkaných na základe predplatného. Vzhľadom na svoju povahu slobodného (bezplatného) a otvoreného softvéru môže tento softvér zostať v používaní aj po tom, ako jeho používateľ prestane platiť za podporné služby; v takom prípade je výrobca povinný zabezpečiť obdobie podpory, ktoré je rovnaké ako trvanie aktívneho predplatného.

#### 4.5.3 Môže výrobca pokračovať v predaji produktov bez obdobia podpory?

Výrobcovia musia stanoviť obdobie podpory pre všetky produkty s digitálnymi prvkami, ktoré boli uvedené na trh po 11. decembri 2027. Tieto produkty môžu byť naďalej dostupné na trhu aj po uplynutí obdobia podpory. V prípade jednotiek tohto produktu, ktoré sú novo uvedené na trh, sú však výrobcovia povinní stanoviť obdobie podpory.

Napríklad výrobca vyrobí 10 000 identických jednotiek rovnakého modelu alebo série hardvérového produktu a uvedie ich na trh v januári 2028 s obdobím podpory päť rokov (t. j. do januára 2033). Distribútor dokáže pred koncom obdobia podpory predať len časť týchto jednotiek. Distribútor môže tieto jednotky naďalej poskytovať aj po januári 2033.

Dňa 1. januára 2030 ten istý výrobca vyrobí ďalších 5 000 identických jednotiek toho istého modelu alebo série produktu a uvedie ich na trh. Výrobca je povinný stanoviť obdobie podpory pre tieto jednotky v súlade s článkom 13 ods. 8 CRA.

## 5 Povinnosti hlásenia výrobcov

### 5.1 Ako sa môže výrobca dozvedieť o aktívne zneužívanej zraniteľnosti alebo závažnom incidente?

CRA nešpecifikuje, ako sa má výrobca dozvedieť o aktívne zneužívanom zraniteľnosti alebo závažnom incidentu, ale ukladá mu povinnosť nahlásiť to v súlade s článkom 14, akonáhle sa o tom dozvie.

V nasledujúcich odsekoch sa uvádzajú niektoré príklady toho, ako sa výrobca môže dozvedieť o takýchto zraniteľnostiach alebo incidentoch prostredníctvom rôznych činností a kanálov. Treba poznamenať, že to neznamena, že výrobca je povinný vykonávať takéto činnosti alebo monitorovať takéto kanály, aby splnil požiadavky na hlásenie.<sup>9</sup>

Výrobca sa o nich môže dozvedieť napríklad vtedy, keď ho zákazník alebo partnerská organizácia informuje o nezvyčajnej činnosti alebo ohrození a poskytne mu spoľahlivé dôkazy o tom, že jeho produkt obsahuje aktívne zneužívanú zraniteľnosť (alebo výrobca získa spoľahlivé dôkazy potvrdzujúce jej existenciu).

Výrobca sa môže dozvedieť o probléme aj prostredníctvom správ o hrozbách, napr. bezpečnostní výskumníci alebo spoločnosti zaoberajúce sa kybernetickou bezpečnosťou zverejňujú správy, v ktorých podrobne opisujú zraniteľnosť typu zero-day (t. j. zraniteľnosť, pre ktorú ešte nie je k dispozícii záplata alebo bezpečnostná aktualizácia) v produkte výrobcu, ktorý sa používa v cielených útokoch. Vládne agentúry zaoberajúce sa kybernetickou bezpečnosťou môžu výrobcu tiež oznámiť, ak prostredníctvom svojich systémov monitorovania zistia zneužitie zraniteľnosti. Etickí hackeri môžu tiež nahlásiť zraniteľnosť, ktorá sa už vo veľkom rozsahu zneužíva.

Okrem toho sa výrobca môže dozvedieť o zraniteľnosti aj prostredníctvom vnútorného monitorovania, skenovania alebo telemetrie. Napríklad telemetrický systém výrobcu alebo návada (t. j. bezpečnostný mechanizmus používaný na odlákavie kyber zločincov od legitímnych cieľov) indikuje zneužitie doteraz neznámej zraniteľnosti v produkte výrobcu, alebo bezpečnostný tím výrobcu monitoruje fóra na dark webe a nájde dôkazy, že hackeri úspešne zneužili zraniteľnosť v produkte výrobcu.

---

<sup>9</sup> Príloha I časť II však má požiadavku, aby výrobca mal okrem iného jedno kontaktné miesto, bod, kde je možné hlásiť zraniteľnosti, zaviedol a presadzoval koordinovanú politiku zverejňovania zraniteľností a prijal opatrenia na uľahčenie zdieľania informácie o potenciálnych zraniteľnostiach.

## 5.2 Musí výrobca urobiť hlásenie o zraniteľnostiach typu zero-day?

*„aktívne zneužitá zraniteľnosť“ je zraniteľnosť, v prípade ktorej existuje spoľahlivý dôkaz, že škodlivý subjekt ju zneužil v systéme bez povolenia vlastníka systému; (článok 3 ods. 42)*

*Aktívne zneužívané zraniteľnosti sa týkajú prípadov, keď výrobca zistí, že narušenie bezpečnosti ovplyvňujúce jeho používateľov alebo akékoľvek iné fyzické alebo právnické osoby bolo spôsobené tým, že škodlivý subjekt využil chybu v jednom z produktov s digitálnymi prvkami, ktoré výrobca sprístupnil na trhu. Príkladmi takýchto zraniteľností by mohli byť nedostatky v identifikačných a autentifikačných funkciách produktu. Zraniteľnosti, ktoré sa zistia bez zlého úmyslu na účely testovania, skúmania, opravy alebo zverejnenia v dobrej viere s cieľom podporiť bezpečnosť alebo ochranu vlastníka systému a jeho používateľov, by nemali podliehať povinnému oznamovaniu (odôvodnenie 68).*

Zraniteľnosti, pre ktoré ešte nie je k dispozícii záplata alebo bezpečnostná aktualizácia (tzv. „zraniteľnosti typu zero-day“), podliehajú oznamovaniu v súlade s článkom 14, ak má výrobca spoľahlivé dôkazy o tom, že škodlivý subjekt túto zraniteľnosť zneužil.

Napríklad zraniteľnosť typu zero-day, ktorú objavili etickí hackeri, pre ktorú neexistujú dôkazy o predchádzajúcom zlom úmysle a ktorá je oznámená výrobcovi produktu v rámci programu odmeňovania za nájdenie chýb (pozri odôvodnenie 76), nie je aktívne zneužívanou zraniteľnosťou, ktorá podlieha povinnému hláseniu. Podobne ani zraniteľnosť typu zero-day, ktorú objavilo laboratórium hodnotiace kybernetickú bezpečnosť vykonávajúce skúšanie v mene výrobcu a pre ktorú neexistujú dôkazy o predchádzajúcom zneužití zo strany zločincov, nie je aktívne zneužívanou zraniteľnosťou, ktorá podlieha povinnému hláseniu. Výrobcovia môžu tieto zraniteľnosti aj naďalej oznamovať dobrovoľne v súlade s článkom 15.

## 5.3 Musí výrobca vykonávať hlásenie aktívne zneužívaných zraniteľností alebo závažných incidentov týkajúcich sa produktov, ktoré boli uvedené na trh pred začatím uplatňovania CRA?

*Odchyľne od odseku 2 tohto článku sa povinnosti stanovené v článku 14 uplatňujú na všetky produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti tohto nariadenia a boli uvedené na trh pred 11. decembrom 2027 (článok 69 ods. 3).*

Povinnosti podávať hlásenia sa začínajú uplatňovať od 11. septembra 2026. Výrobcovia sú povinní dodržiavať článok 14, a to najmä povinnosť oznamovať aktívne zneužívané zraniteľnosti a závažné incidenty, ktoré majú vplyv na bezpečnosť produktu, pre všetky produkty s digitálnymi prvkami, ktoré patria do pôsobnosti CRA, vrátane produktov, ktoré boli uvedené na trh pred 11. decembrom 2027.

Ak bol produkt uvedený na trh pred 11. decembrom 2027, výrobcovia nemusia byť schopní takéto zraniteľnosti vyšetriť, napríklad preto, že nástroje na skenovanie alebo spúšťanie

starých verzí softvéru už nemusí existovať, prostredia pre starý kód nemusí byť možné znovu vytvoriť, závislosti môžu byť nedostupné alebo nekompatibilné s modernými systémami, zamestnanci so znalosťami starých kódových základní môžu odísť. V prípade takýchto produktov sú výrobcovia povinní hlásiť zraniteľnosť alebo incident, ale CRA od nich nevyžaduje splnenie ďalších požiadaviek, napríklad v súvislosti s riešením zraniteľností.

Okrem toho povinnosť oznamovať sa uplatňuje po zistení po nadobudnutí účinnosti požiadaviek na oznamovanie (pozri tiež bod 5.1 *Ako sa môže výrobca dozvedieť o aktívne zneužívanom zraniteľnom mieste alebo závažnom incidente?*)

Článok 14 ods. 8 však vyžaduje, aby výrobca informoval o týchto zraniteľnostiach alebo incidentoch používateľov produktu s digitálnymi prvkami, ktorých sa to týka, a v prípade potreby všetkých používateľov. Ak sa výrobca rozhodne neinformovať používateľov produktu s digitálnymi prvkami včas, CSIRT, ktoré dostanú hlásenie, môžu poskytnúť takéto informácie používateľom, ak to považujú za primerané a potrebné na prevenciu alebo zmiernenie vplyvu tejto zraniteľnosti alebo incidentu.

## 5.4 Ak je aktívne zneužívaná zraniteľnosť obsiahnutá v komponente tretej strany, sú všetci výrobcovia, ktorí túto komponentu integrujú, povinní hlásiť to?

*„Produkt s digitálnymi prvkami“ je softvérový alebo hardvérový produkt a jeho riešenia spracovania údajov na diaľku vrátane softvérových alebo hardvérových komponentov, ktoré sa uvádzajú na trh samostatne (článok 3 ods. 1).*

*Výrobca oznámi každú aktívne zneužitú zraniteľnosť produktu s digitálnymi prvkami, o ktorej sa dozvie (článok 14 ods. 1).*

*Výrobcovia by mali oznamovať aktívne zneužívané zraniteľnosti s cieľom zabezpečiť, aby jednotky CSIRT určené za koordinátorov a agentúra ENISA mali primeraný prehľad o takýchto zraniteľnostiach a aby im boli poskytnuté informácie potrebné na plnenie ich úloh stanovených v smernici (EÚ) 2022/2555 a zvýšenie celkovej úrovne kybernetickej bezpečnosti kľúčových a dôležitých subjektov uvedených v článku 3 uvedenej smernice, ako aj zabezpečenie účinného fungovania orgánov dohľadu nad trhom. Keďže väčšina produktov s digitálnymi prvkami sa predáva na celom vnútornom trhu, akákoľvek zneužitá zraniteľnosť produktu s digitálnymi prvkami by sa mala považovať za ohrozenie fungovania vnútorného trhu (odôvodnenie 66).*

Výrobcovia sú povinní nahlásiť akúkoľvek aktívne zneužívanú zraniteľnosť obsiahnutú v ich produkte s digitálnymi prvkami. Ak produkt s digitálnymi prvkami obsahuje aktívne zneužívanú zraniteľnosť pochádzajúcu z integrovanej súčasti, výrobca produktu s digitálnymi prvkami je povinný hlásiť túto zraniteľnosť. Výrobca integrovanej súčasti je tiež povinný nahlásiť túto zraniteľnosť, ak bola táto súčasť uvedená na trh.

Ak si výrobca produktu s digitálnymi prvkami uvedomuje, že integrovaný komponent obsahuje zraniteľnosť, ale táto zraniteľnosť nemôže byť zneužitá v jeho produkte s digitálnymi prvkami, táto zraniteľnosť nie je aktívne zneužívaná, a preto nepodlieha povinnému hláseniu. Výrobcovia môžu túto zraniteľnosť hlásiť na dobrovoľnej báze v súlade s článkom 15 a sú povinní hlásiť zraniteľnosť osobe alebo subjektu, ktorý komponent vyrába alebo udržiava, v súlade s článkom 13 ods. 6.

To umožňuje CSIRT, ktoré prijímajú hlásenia, a agentúra ENISA získať prehľad o bezpečnostnej situácii na vnútornom trhu a vykonávať posudzovanie úrovne kritickosti a penetrácie trhu aktívne zneužívaných zraniteľností.

## 5.5 Podliehajú správcovia softvéru s otvoreným zdrojovým kódom nahlasovacím povinnostiam podľa CRA?

Článok 24 ods. 3 CRA stanovuje, že nahlasovacie povinnosti uvedené v článku 14 ods. 1, 3 a 8 sa za určitých okolností vzťahujú aj na správcov softvéru s otvoreným zdrojovým kódom.

V súlade s článkom 71 ods. 2 CRA sa článok 24 ods. 3 uplatňuje od 11. decembra 2027.

## 6 Posudzovanie zhody

Posudzovanie zhody je právny postup, ktorý má výrobca vykonávať s cieľom preukázať, že produkt s digitálnymi prvkami je súladný so základnými požiadavkami CRA.

CRA poskytuje nasledujúce možnosti:

- Modul A alebo zhoda na základe vnútornej kontroly, stanovená v časti I prílohy VIII.
- Modul B+C, alebo EÚ skúška typu, uvedené v častiach II a III prílohy VIII.
- Modul H, alebo zhoda založená na úplnom zabezpečení kvality, stanovený v časti IV prílohy VIII.

Tieto tri moduly sú uvedené v poradí podľa zvyšujúcej sa zložitosti, nákladov, ale aj externej podpory pre výrobcov.

### 6.1 Čo je modul A? Ako funguje? Aké činnosti posudzovania zhody sa očakávajú pri samohodnotení?

Modul A, stanovený v časti I prílohy VIII, je postup posudzovania zhody, pri ktorom výrobca overuje, či produkt s digitálnymi prvkami spĺňa základné požiadavky CRA, a na vlastnú zodpovednosť vyhlási súlad.

Na tomto postupe sa nezúčastňujú žiadne notifikované osoby.

Modul A môžu používať tieto kategórie produktov:

- Všetky produkty s digitálnymi prvkami, ktoré nemajú základnú funkcionálnu kategóriu dôležitých alebo kritických produktov („default kategória“).
- Dôležité produkty s digitálnymi prvkami triedy I, ak sa uplatnila harmonizovaná norma v súlade s článkom 32 ods. 2;
- dôležité produkty s digitálnymi prvkami triedy I alebo II, ak ide o slobodný (bezplatný) softvér s otvoreným zdrojovým kódom, za predpokladu, že technická dokumentácia je sprístupnená verejnosti v súlade s článkom 32 ods. 5.

Výrobca musí vykonať tieto činnosti:

- Implementovať potrebné opatrenia na mitigáciu kybernetickej bezpečnosti v produkte na základe posúdenia rizika opísaného v oddiele 4.1 *Prístup založený na riziku a posúdenie rizika*.
- Overiť (prostredníctvom skúšania alebo iného mechanizmu), či produkt spĺňa príslušné základné požiadavky CRA. Ak je to vhodné, pozri aj časť 6.5 *Akú metodiku hodnotenia by mal výrobca použiť?*
- Vypracovať technickú dokumentáciu. Pozri tiež časť 6.6 *Čo je technická dokumentácia?*
- Akonáhle je výrobca schopný preukázať, že produkt s digitálnymi prvkami je súladný so základnými požiadavkami CRA, umiestniť označenie CE (pozri časť 6.7 *Čo je označenie*

CE?), vypracovať a podpísať vyhlásenie o zhode (pozri časť 6.8 Čo je vyhlásenie o zhode?).

- Zabezpečiť, aby výroba rôznych jednotiek produktu s digitálnymi prvkami nemala vplyv na súlad so základnými požiadavkami CRA.

## 6.2 Čo je modul B+C? Ako funguje?

Modul B+C, stanovený v častiach II a III prílohy VIII, je postup posudzovania zhody, pri ktorom výrobca overuje, či produkt s digitálnymi prvkami spĺňa základné požiadavky CRA, notifikovaná osoba skúma návrh a vývoj produktu a výrobca vyhlási súlad.

Výrobca môže podniknúť postup posudzovania zhody na základe modulu B+C pre všetky kategórie produktov, na ktoré sa vzťahuje CRA. Modul B+C alebo H je povinný v nasledujúcich prípadoch<sup>10</sup> :

- Dôležité produkty s digitálnymi prvkami triedy I, ak nebola uplatnená harmonizovaná norma v súlade s článkom 32 ods. 2.
- Dôležité produkty triedy II.
- Kritické produkty (pokiaľ sa v budúcnosti nestane povinným používanie Európskej schémy certifikácie kybernetickej bezpečnosti v súlade s článkom 8 ods. 1).

Na tomto postupe sa podieľa len jedna notifikovaná osoba, ktorá preskúma celý produkt a všetky príslušné základné požiadavky za podmienok opísaných nižšie.

Výrobca a notifikovaná osoba musia vykonávať tieto činnosti:

- Výrobca implementuje do produktu potrebné opatrenia na mitigáciu kybernetickej bezpečnosti v súlade s posudzovaním rizika opísaným v oddiele 4.1 *Prístup založený na riziku a posúdenie rizika*.
- Výrobca skúša produkt s cieľom overiť, či spĺňa príslušné základné požiadavky CRA. Ďalšie informácie nájdete v oddiele 6.5. *Akú metodiku hodnotenia by mal výrobca použiť?*
- Výrobca vypracuje technickú dokumentáciu. Ďalšie informácie nájdete v časti 6.6 *Čo je technická dokumentácia?*
- Notifikovaná osoba vykonáva posudzovanie návrhu produktu na základe jeho technickej dokumentácie a jedného exempláru alebo vzorky. Notifikovaná osoba nielenže vykonáva posudzovanie na základe dokumentácie, ale navyše vykonáva potrebné skúšky buď sama, alebo prostredníctvom externého laboratória. Výrobca sa môže musieť podieľať na týchto skúškach. Akonáhle dospeje k záveru, že produkt je súladný s CRA, vydá Certifikát EÚ skúšky typu, ktoré je platné po určitú dobu stanovenú notifikovanou osobou.

---

<sup>10</sup> V súlade s článkom 32 ods. 5 výrobcovia si zachovávajú možnosť používať modul A aj v prípade dôležitého produktu s digitálnymi prvkami triedy I alebo II, ak ich produkt spĺňa podmienky slobodného a otvoreného softvéru a technická dokumentácia je sprístupnená verejnosti.

- Po získaní certifikátu EÚ skúšky typu výrobca umiestni označenie CE (pozri časť 6.7 Čo je označenie CE?), vypracuje a podpíše vyhlásenie o zhode (pozri časť 6.8 Čo je vyhlásenie o zhode?).
- Výrobca zabezpečí, aby výroba jednotlivých produktov nemala vplyv na súlad so základnými požiadavkami CRA, ako je stanovené v bode 2 modulu C. Fáza výroby nie je predmetom posudzovania notifikovanou osobou. Inými slovami, výrobca nemôže odôvodniť, že produkt, ktorého návrh je súladná s CRA, nie je v praxi súladný z dôvodu chyby vo výrobnom procese.

Podstatné úpravy produktu si vyžadujú nové posudzovanie tým istým alebo iným notifikovanými osobami, čo môže viesť k potenciálnej revízii vydaného certifikátu EÚ. Ostatné úpravy, ktoré nemajú vplyv na súlad s požiadavkami CRA, nepodliehajú opätovnému posudzovaniu notifikovanými osobami. Okrem toho v súlade s bodom 8 modulu B musí notifikovaná osoba vykonávať pravidelný audit, aby sa zabezpečilo riadne vykonávanie procesov zaobchádzania so zraniteľnosťou.

Informácie o certifikátoch EÚ skúšky typu a ich revíziách sa musia zdieľať s ostatnými notifikovanými osobami a notifikačnými orgánmi v súlade s bodom 9 modulu B.

### 6.3 Čo je modul H? Ako funguje?

Modul H, uvedený v časti IV prílohy VIII, je postup posudzovania zhody, pri ktorom výrobca zavádza systém úplnej kontroly kvality, ktorý zabezpečuje, že produkty podliehajúce tomuto systému spĺňajú základné požiadavky CRA ako vo fáze návrhu, tak aj vo fáze výroby. Notifikovaná osoba posudzuje celkovú výkonnosť systému kontroly kvality, vrátane pravidelných skúšok a kontrol. Výrobca vyhlási súlad s požiadavkami CRA pred uvedením produktov na trh.

Na tomto postupe sa podieľa len jeden notifikovaná osoba, ktorý preskúma celý systém kontroly kvality podľa nižšie uvedených podmienok.

Tento modul môžu zväziť najmä výrobcovia, ktorí uvádzajú na trh viacero typov produktov alebo produkty, ktoré podliehajú častým aktualizáciám, pretože zjednodušuje príslušné postupy posudzovania zhody pre každý nový alebo podstatne upravený produkt.

Výrobca a notifikovaná osoba musia vykonávať tieto činnosti:

- Výrobca zavádza systém úplnej kontroly kvality, ktorý pokrýva určitý katalóg produktov a všetky relevantné fázy výroby, od návrhu až po výrobu. Systém môže byť založený na medzinárodných normách (napríklad séria noriem ISO 9000, ktorá pokrýva špecifiká CRA). Skutočnosť, že výrobca je akreditovaný podľa normy ISO 9000, ho automaticky neoprávňuje vykonávať činnosť posudzovania zhody podľa modulu H, pretože je potrebná účasť notifikovanej osoby CRA.
- Notifikovaná osoba posudzuje systém kontroly kvality ako celok, vrátane, okrem iného, technického návrhu produktov, ktoré sú predmetom posudzovania, noriem alebo špecifikácií, ktoré sa majú uplatňovať (najmä spôsob, akým sa zabezpečuje súlad so

základnými požiadavkami CRA), skúšok, ktoré sa majú vykonávať, a monitorovania celkového systému. Notifikovaná osoba posudzuje celý výrobný proces.

- Výrobca na základe systému kontroly kvality implementuje do produktu potrebné opatrenia na zmiernenie kybernetickej bezpečnosti v súlade s posudzovaním rizika opísaným v *oddiele 4.1 Čo CRA vyžaduje od výrobcu v súvislosti s posudzovaním kybernetickobezpečnostného rizika?*
- Výrobca na základe systému kontroly kvality skúša produkt s cieľom overiť, či spĺňa príslušné základné požiadavky CRA. Ďalšie informácie *nájdete v časti 6.5. Akú metodiku hodnotenia by mal výrobca použiť?*
- Výrobca na základe systému riadenia kvality vypracuje technickú dokumentáciu. Ďalšie informácie *nájdete v časti 6.6 Čo je technická dokumentácia?*
- Výrobca umiestni označenie CE (pozri časť 6.7 *Čo je označenie CE?*) spolu s číslom NANDO notifikovanej osoby, vypracuje a podpíše vyhlásenie o zhode (pozri časť 6.8 *Čo je vyhlásenie o zhode?*).
- Výrobca na základe systému riadenia kvality zabezpečuje, aby výroba rôznych jednotiek produktu nemala vplyv na súlad so základnými požiadavkami CRA.

Výrobca môže rozšíriť rozsah opísaného systému kvality na nové alebo podstatne upravené produkty. Systém kvality sa musí aktualizovať, aby sa riadne zdokumentoval nový rozsah, a môže byť potrebné uplatniť nové normy alebo vykonať nové skúšky. Toto rozšírenie však podlieha novému posudzovaniu tou istým notifikovanou osobou, ktorá vykonala pôvodné posudzovanie. V každom prípade, ako je uvedené vyššie, modul H poskytuje univerzálnejší a flexibilnejší rámec v porovnaní s modulom B+C. Zaradenie nových produktov je preto zjednodušeným procesom, keďže notifikovaná osoba bude musieť vykonať len posudzovanie potenciálnych nových noriem alebo skúšok uplatniteľných na nové produkty.

## 6.4 Sú výrobcovia povinní zabezpečiť zhodu „existujúcich“ typov produktov?

CRA sa vzťahuje na produkty uvádzané na trh ako jednotlivé jednotky odo dňa jej uplatniteľnosti. Inými slovami, staršie typy alebo modely nie sú vyňaté z uplatňovania CRA, ak sa po uvedenom dátume uvedú na trh ich nové jednotky. CRA stanovuje prechodné obdobie medzi nadobudnutím účinnosti (10. december 2024) a dátumom uplatňovania (11. december 2027 pre väčšinu povinností), aby sa zabezpečilo hladké zavedenie. Počas tohto obdobia musí výrobca v prípade potreby prispôbiť produkt požiadavkám CRA a vykonať posudzovanie zhody opísané v tejto kapitole.

Modul H môže byť užitočný pre výrobcov dôležitých a kritických produktov, ktorí uvádzajú na trh viacero typov alebo modelov, pretože poskytuje komplexný systém, ktorý zefektívňuje posudzovanie zhody.

## 6.5 Akú metodiku hodnotenia by mal výrobca použiť?

CRA nepredpisuje použitie žiadnej konkrétnej metodiky hodnotenia, vrátane skúšania. Výrobci však zvyčajne používajú vhodnú harmonizovanú normu alebo technickú špecifikáciu.

Výrobca môže vykonávať príslušné skúšky alebo skúšobné postupy vo svojich vlastných laboratóriách, ak sú k dispozícii, alebo v externých laboratóriách. CRA nestanovuje žiadne konkrétne požiadavky na laboratóriá, ktoré vykonávajú skúšky súvisiace s postupmi posudzovania zhody. Výrobca nesie výhradnú zodpovednosť za posudzovanie zhody.

Orgány dohľadu nad trhom môžu počas príslušných inšpekcií vykonávať skúšky alebo hodnotiace postupy. V tejto súvislosti môžu zvážiť použitie rovnakej metodiky, akú používa výrobca, najmä ak je táto metodika súčasťou harmonizovanej normy na podporu CRA. Orgán dohľadu nad trhom však môže na odôvodnenom základe použiť inú metodiku. Je potrebné zdôrazniť, že skúšanie kybernetickej bezpečnosti nie je deterministické ako v iných oblastiach regulovaných NLF a výsledky nemusia byť jednoznačné.

## 6.6 Čo je technická dokumentácia?

Technická dokumentácia musí obsahovať prvky uvedené v prílohe VII CRA.

Výrobca musí zohľadniť, že technická dokumentácia nie je len interným výstupom, ale môže ju požadovať orgán dohľadu nad trhom. Preto musí byť komplexná a jasná. Výrobca musí byť schopný preukázať, že produkt bol navrhnutý, vyvinutý a vyrobený tak, aby spĺňal základné požiadavky CRA. Táto požiadavka zahŕňa špecifikácie procesov riešenia zraniteľnosti.

Technická dokumentácia môže byť vyhotovená v akomkoľvek jazyku. Ak to však vyžaduje orgán dohľadu nad trhom, musí byť poskytnutá v jazyku, ktorému tento orgán ľahko rozumie.

Neexistuje povinnosť sprístupniť technickú dokumentáciu zákazníkom výrobcu alebo verejnosti, s výnimkou výrobcov slobodného a otvoreného softvéru, ktorí patria do kategórií uvedených v prílohe III (dôležité produkty triedy I alebo II) a ktorí si želajú sami osvedčiť ich zhodu v súlade s článkom 32 ods. 5.

## 6.7 Čo je označenie CE?

Označenie CE je jednoduché vizuálne vyhlásenie výrobcu, že produkt je súladný so všetkými platnými právnymi predpismi NLF, a najmä s CRA. Je určené spotrebiteľom a orgánom dohľadu na trhom. Je upravené v článkoch 29 a 30. Ďalšie informácie možno nájsť aj v oddiele 4.5.1. Modrej príručky.

Produkty musia byť označené označením CE viditeľným, čitateľným a nezmazateľným spôsobom. Spravidla musí byť väčšie ako 5 mm. Výnimky sa môžu akceptovať, ak to veľkosť produktu neumožňuje, za predpokladu, že zostane viditeľné. Označenie CE nemôže mať z estetických dôvodov veľkosť menšiu ako 5 mm.

Označenie CE nemožno umiestniť na časť produktu, ktorá nie je podľa jeho zamýšľaného použitia ľahko viditeľná.

Softvérové produkty musia tiež niesť označenie CE. V súlade s článkom 30 ods. 1 sa v prípade softvérových produktov označenie CE umiestňuje buď na EÚ vyhlásenie o zhode, alebo na webovú stránku, ktorá sprevádza softvérový produkt. V druhom prípade musí byť príslušná časť webovej stránky ľahko a priamo prístupná spotrebiteľom.

Označenie CE nemožno umiestniť, ak výrobca nevykonal postup posudzovania zhody s kladným výsledkom.

## 6.8 Čo je vyhlásenie o zhode?

Vyhlásenie o zhode je dokument, v ktorom výrobca vyhlasuje, že produkt je súladný s CRA, a preberá za to zodpovednosť.

Vyhlásenie o zhode musí sprevádzať produkt uvádzaný na trh. Sú povolené dva formáty:

- Úplné vyhlásenie o zhode podľa vzoru uvedeného v prílohe V.
- Zjednodušené vyhlásenie o zhode, ktoré je vetou podľa vzoru uvedeného v prílohe VI a obsahuje internetovú adresu, na ktorej je k dispozícii úplné vyhlásenie o zhode.

Vyhlásenie o zhode je dokument, ktorý sa vzťahuje na konkrétny produkt, a nie len na typ alebo model. V tomto ohľade nie je potrebné, aby obsahovalo jedinečný identifikátor produktu. Nová verzia produktu však môže vyžadovať nové vyhlásenie o zhode, najmä ak sa týka podstatnej úpravy.

Vyhlásenie o zhode nemožno podpísať, ak výrobca nevykonal jeden z príslušných postupov posudzovania zhody s kladným výsledkom.

V súlade s článkom 28 ods. 3 a ako sa uvádza v oddiele 4.4 Modrej príručky, ak sa na produkt vzťahuje viacero harmonizačných právnych predpisov Únie, výrobca alebo splnomocnený zástupca musí predložiť jedno vyhlásenie o zhode vo vzťahu ku všetkým týmto aktom Únie. S cieľom znížiť administratívnu záťaž pre hospodárske subjekty a uľahčiť jeho prispôsobenie sa zmene jedného z uplatniteľných aktov Únie môže byť jednotné vyhlásenie dokumentáciou pozostávajúcou z príslušných jednotlivých vyhlásení o zhode.

## 6.9 Čo sú notifikované osoby?

Notifikované osoby sú súkromné alebo verejné subjekty, ktoré skúmajú produkty s cieľom zabezpečiť ich súlad s CRA. Ich kompetentnosť je predmetom posudzovania notifikačnými orgánmi členských štátov a zoznam je k dispozícii v systéme [NANDO](#).

Notifikované osoby musia byť nezávislé vo vzťahu k výrobcovi a orgánom dohľadu nad trhom, aby sa predišlo akémukoľvek konfliktu záujmov.

## 6.10 Kedy budú pripravené harmonizované normy na podporu súladu s CRA?

Žiadosť Komisie o normalizáciu (M/606) adresovaná CEN, CENELC a ETSI predpokladá vypracovanie súboru harmonizovaných noriem na podporu súladu s CRA, pričom sa rozlišuje medzi horizontálnymi (nezávislými od produktov) normami a vertikálnymi (špecifickými pre produkt) normami.

Horizontálne normy majú poskytnúť koherentný všeobecný rámec, metodiku a taxonómiu na podporu vývoja ďalších podrobných vertikálnych harmonizovaných noriem pre konkrétne produkty alebo typy produktov, ako aj na podporu výrobcov pri definovaní a implementácii bezpečnostných požiadaviek platných pre ich príslušné produkty. Komisia požiadala o vypracovanie 15 horizontálnych noriem, ktoré európske normalizačné organizácie (ESO) zoskupili do 3 výstupov:

- harmonizovaná európska norma o navrhovaní, vývoji a výrobe produktov s digitálnymi prvkami tak, aby zabezpečovali primeranú úroveň kybernetickej bezpečnosti na základe rizík, ktorú majú ESO prijať do 30. augusta 2026;
- harmonizovaná európska norma, ktorá sa týka základných požiadaviek kybernetickej bezpečnosti súvisiacich s vlastnosťami produktov s digitálnymi prvkami, ako sa stanovuje v časti I prílohy I, ktorú majú ESO prijať do 30. októbra 2027;
- Harmonizovaná európska norma o riešení zraniteľnosti produktov s digitálnymi prvkami, ktorú majú európske normalizačné organizácie prijať do 30. augusta 2026.

Vertikálne normy majú byť špecifické pre jednotlivé produkty a majú pokrývať konkrétny súbor rizík, ktoré sú primerané konkrétnemu zamýšľanému účelu a odôvodnene predvídateľnému použitiu. Komisia požiadala o vypracovanie 26 vertikálnych noriem (ktorými sa európske normalizačné organizácie zaoberajú prostredníctvom 31 samostatných výstupov), ktoré majú európske normalizačné organizácie prijať do 30. októbra 2026. Vertikálne normy, ktoré sa vypracúvajú, sa vzťahujú na kategórie dôležitých a kritických produktov s digitálnymi prvkami stanovené v prílohách III a IV CRA.

V súlade s článkom 27 ods. 6, ak európske normotvorné orgány prijímajú harmonizovanú európsku normu, Komisia ju vykoná proces posudzovania v súlade s nariadením (EÚ) č. 1025/2012 na účely uverejnenia jej odkazu v Úradnom vestníku Európskej únie.

## 7 Prechodné obdobie

### 7.1 Kedy sa začne CRA uplatňovať?

Podľa článku 71 ods. 2 sa články 35 až 51 uplatňujú od 11. júna 2026. Členské štáty majú požiadavku do tohto dátumu určiť notifikačné orgány, ktoré sú zodpovedné za zavedenie a vykonávanie potrebných postupov na posudzovanie, určovanie a notifikáciu orgánov posudzovania zhody.

Oznamovacie povinnosti stanovené v článku 14 sa uplatňujú od 11. septembra 2026. Od tohto dátumu sú výrobcovia povinní prostredníctvom jednotnej oznamovacej platformy oznamovať aktívne zneužívané zraniteľnosti a závažné incidenty, ktoré majú vplyv na bezpečnosť ich produktov s digitálnymi prvkami.

Povinnosti výrobcov zabezpečiť, aby produkty s digitálnymi prvkami boli v zhode so základnými požiadavkami kybernetickej bezpečnosti stanovenými v prílohe I, ustanovenia o dohľade nad trhom a presadzovaní práva, ako aj všetky ostatné ustanovenia stanovené v CRA, sa uplatňujú od 11. decembra 2027.

Podľa článku 69 ods. 1 zostávajú certifikáty EÚ skúšky typu a rozhodnutia o schválení vydané v súvislosti s požiadavkami kybernetickej bezpečnosti produktov s digitálnymi prvkami, na ktoré sa vzťahujú iné harmonizačné právne predpisy Únie, ako je napríklad delegované nariadenie Komisie (EÚ) 2022/30, platné do 11. júna 2028 (ak sa v týchto právnych predpisoch nestanovuje inak alebo ak certifikát neplatí pred týmto dátumom).

### 7.2 Výrobca vyvinie produkt predtým, ako sa začne uplatňovať CRA.

#### Môže pokračovať vo výrobe produktov identických s týmto produktom aj po začatí uplatňovania CRA?

Ako sa uvádza v oddiele 2.2 Modrej príručky, harmonizačné právne predpisy Únie vrátane CRA sa vzťahujú na jednotlivé produkty, a nie na typy produktov. Preto len jednotlivé produkty, ktoré boli uvedené na trh pred 11. decembrom 2027, nemusia spĺňať CRA.

Produkty, ktoré sú vyrábané podľa typu, ktorý nie je súladný s CRA, nemôžu byť uvedené na trh 11. decembra 2027 alebo po tomto dátume, aj keď prvý exemplár tohto „typu“ produktu bol uvedený na trh pred 11. decembrom 2027.

Napríklad výrobca vyrobil 10 000 kusov smerovača typu, ktorý nie je súladný s CRA. Týchto 10 000 kusov uvedie na trh pred 11. decembrom 2027. Aj keď sa tieto jednotky nedostali k konečnému používateľovi (ale boli uvedené na trh), výrobca ich nemusí uviesť do súladu s CRA (pozri aj *bod 1.4. Uplatňuje sa CRA na produkty s digitálnymi prvkami, ktoré boli uvedené na trh pred 11. decembrom 2027?*) Tento výrobca však nesmie vyrobiť ďalších 5 000 kusov tohto smerovača a uviesť ich na trh po 11. decembri 2027, pretože týchto 5 000 kusov by neboli súladné s CRA.

### 7.3 Môže výrobca uvádzať na trh produkty s digitálnymi prvkami vyvinutými počas prechodného obdobia, ktoré obsahujú komponenty, ktoré nemajú označenie CE?

*Na účely dosiahnutia súladu s odsekom 1 výrobcovia uplatňujú náležitú starostlivosť pri integrácii komponentov získaných od tretích strán tak, aby tieto komponenty neohrozovali kybernetickú bezpečnosť produktu s digitálnymi prvkami, a to aj pri integrácii komponentov slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktoré neboli sprístupnené na trhu v priebehu obchodnej činnosti (článok 13 ods. 5).*

*Ihneď po prechodnom období na uplatňovanie tohto nariadenia výrobca produktu s digitálnymi prvkami, ktorý integruje jeden alebo viacero komponentov od tretích strán, na ktoré sa takisto vzťahuje toto nariadenie, nemusí byť schopný v rámci svojej povinnosti náležitej starostlivosti overiť, či výrobcovia týchto komponentov preukázali zhodu s týmto nariadením, napríklad overením toho, či tieto komponenty už majú označenie CE. Môže ísť o prípad, keď komponenty boli integrované skôr, ako sa toto nariadenie začne uplatňovať na výrobcov týchto komponentov. V tom prípade by mal výrobca, ktorý takéto komponenty integruje, uplatňovať náležitú starostlivosť inými prostriedkami (odôvodnenie 35).*

Ako sa vysvetľuje v bodoch 4.4.1 Čo CRA predpisuje pri integrácii komponentov? a 4.4.3 Aby výrobca vykonal náležitú starostlivosť, mal by integrovať len komponenty, ktoré sú označené označením CE?, výrobca môže integrovať komponenty, ktoré nie sú označené označením CE, ale je požiadavka vykonávať náležitú starostlivosť, aby sa uistil, že tieto komponenty nevedú k ohrozeniu kybernetickej bezpečnosti jeho produktu s digitálnymi prvkami.

Počas prechodného obdobia pred uplatňovaním CRA nebudú výrobcovia môcť skontrolovať, či sú komponenty tretích strán súladné s CRA. To však výrobcom nebráni v integrácii takýchto komponentov a mali by postupovať s náležitou starostlivosťou prostredníctvom iných prostriedkov (pozri aj bod 4.4.2 Aká je primeraná úroveň náležitej starostlivosti?).

### 7.4 Môže výrobca integrovať komponenty, ktoré sú dôležitými alebo kritickými produktmi s digitálnymi prvkami, ktoré nespĺňajú harmonizované normy?

Áno, výrobcovia môžu integrovať komponenty, ktoré sú dôležitými alebo kritickými produktmi, ktoré neboli navrhnuté v súlade s harmonizovanými normami – bez ohľadu na to, či sú takéto harmonizované normy k dispozícii alebo nie.

Uplatňovanie harmonizovaných noriem je prostriedkom na preukázanie súladu, ale nie je jediným prostriedkom na dosiahnutie tohto cieľa.

Okrem toho, ako sa uvádza v bodoch 4.4.1 Čo CRA predpisuje pri integrácii komponentov? a 4.4.3 Mal by výrobca v záujme vykonania náležitej starostlivosti integrovať iba komponenty,

*ktoré nesú označenie CE?*, výrobca nie je povinný integrovať iba komponenty, ktoré nesú označenie CE.

## 7.5 Sú distribútori povinní zabezpečiť súlad produktov s digitálnymi prvkami, ktoré boli uvedené na trh pred 11. decembrom 2027?

Nie, produkty s digitálnymi prvkami uvedené na trh pred 11. decembrom 2027 nepodliehajú požiadavkám CRA (s výnimkou oznamovacích povinností), pokiaľ nie sú podstatne upravené. Distribútori preto nie sú povinní uvádzať takéto produkty do súladu s CRA 11. decembrom 2027 alebo po tomto dátume, pokiaľ nevykonajú podstatnú úpravu.