



EURÓPSKA  
KOMISIA

Brusel, 27.7.2026

C(2026) 5252 v konečnom znení

PRÍLOHA

## **PRÍLOHA**

### **Oznámenie Komisie**

**Schválenie obsahu návrhu oznámenia Komisie – Usmernenia  
Komisie k uplatňovaniu nariadenia (EÚ) 2024/2847 (akt o  
kybernetickej odolnosti)**

## Obsah

|        |                                                                                                             |    |
|--------|-------------------------------------------------------------------------------------------------------------|----|
| 1.     | Úvod.....                                                                                                   | 4  |
| 1.1.   | Akt o kybernetickej odolnosti .....                                                                         | 4  |
| 1.2.   | Účel usmernení .....                                                                                        | 4  |
| 2.     | Rozsah pôsobnosti .....                                                                                     | 6  |
| 2.1.   | Uvedenie na trh.....                                                                                        | 6  |
| 2.2.   | Softvér ako produkt s digitálnymi prvkami .....                                                             | 7  |
| 2.3.   | Počítačový kód .....                                                                                        | 9  |
| 2.4.   | Kombinácia hardvéru a softvéru tvoriaca produkt s digitálnymi prvkami.....                                  | 10 |
| 2.5.   | Dátové pripojenie.....                                                                                      | 11 |
| 2.6.   | Zložité systémy .....                                                                                       | 11 |
| 2.7.   | Produkty s digitálnymi prvkami navrhnuté pred začatím uplatňovania CRA .....                                | 13 |
| 3.     | Slobodný softvér a softvér s otvoreným zdrojovým kódom .....                                                | 16 |
| 3.1.   | Určenie, či je slobodný softvér a softvér s otvoreným zdrojovým kódom v zodpovednosti daného subjektu ..... | 17 |
| 3.2.   | Určenie, či je slobodný softvér a softvér s otvoreným zdrojovým kódom uvádzaný na trh EÚ.....               | 18 |
| 3.2.1. | Účtovanie ceny .....                                                                                        | 18 |
| 3.2.2. | Speňažovanie iných služieb alebo vyžadovanie spracúvania osobných údajov .....                              | 19 |
| 3.2.3. | Podporné služby .....                                                                                       | 19 |
| 3.2.4. | Dary .....                                                                                                  | 21 |
| 3.2.5. | Financovanie slobodného softvéru a softvéru s otvoreným zdrojovým kódom .....                               | 22 |
| 3.2.6. | Neziskové subjekty zriadené na dosiahnutie neziskových cieľov .....                                         | 22 |
| 3.2.7. | Integrácia inými výrobcami .....                                                                            | 23 |
| 3.3.   | Správcovia softvéru s otvoreným zdrojovým kódom .....                                                       | 23 |
| 3.3.1. | Trvalá podpora a zabezpečenie životaschopnosti FOSS.....                                                    | 24 |
| 3.4.   | Prispievatelia a následné využitie .....                                                                    | 26 |
| 3.5.   | Ilustratívne scenáre.....                                                                                   | 27 |
| 4.     | Podstatné úpravy a náhradné diely .....                                                                     | 30 |
| 4.1.   | Fyzické opravy .....                                                                                        | 30 |
| 4.2.   | Náhradné diely .....                                                                                        | 31 |
| 4.3.   | Aktualizácie softvéru ako podstatné úpravy.....                                                             | 33 |
| 4.4.   | Dôsledky podstatnej úpravy.....                                                                             | 38 |
| 4.4.1. | Podstatné úpravy vykonané inou osobou ako pôvodným výrobcom.....                                            | 38 |
| 4.4.2. | Podstatné úpravy vykonané pôvodným výrobcom.....                                                            | 40 |

|        |                                                                                                                                                                   |    |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 5.     | Obdobie podpory .....                                                                                                                                             | 41 |
| 5.1.   | Podstatné úpravy a obdobie podpory .....                                                                                                                          | 43 |
| 6.     | Dôležité a kritické produkty s digitálnymi prvkami .....                                                                                                          | 46 |
| 6.1.   | Základná funkcionálnosť .....                                                                                                                                     | 46 |
| 6.2.   | Posudzovanie zhody dôležitých a kritických produktov s digitálnymi prvkami .....                                                                                  | 50 |
| 6.3.   | Dôsledky pre predpoklad zhody.....                                                                                                                                | 52 |
| 7.     | Posúdenie kybernetickobezpečnostného rizika a integrácia produktov s digitálnymi prvkami a komponentov.....                                                       | 55 |
| 7.1.   | O hodnotení a riešení kybernetickobezpečnostných rizík .....                                                                                                      | 55 |
| 7.2.   | O navrhovaní, vývoji a výrobe produktov s digitálnymi prvkami takým spôsobom, aby zabezpečovali primeranú úroveň kybernetickej bezpečnosti na základe rizík ..... | 56 |
| 7.3.   | Posúdenie kybernetickobezpečnostného rizika a náležitá starostlivosť vo vzťahu k externým závislostiam a integrovaným komponentom.....                            | 57 |
| 7.4.   | Opätovné použitie posúdenia rizík a dokumentácie o zhode pre skupiny produktov s digitálnymi prvkami.....                                                         | 59 |
| 8.     | Spracovanie údajov na diaľku .....                                                                                                                                | 61 |
| 8.1.   | Čo sa považuje za riešenie spracovania údajov na diaľku v prípade produktu s digitálnymi prvkami? .....                                                           | 62 |
| 8.1.1. | Pojem „na diaľku“ .....                                                                                                                                           | 62 |
| 8.1.2. | Zabránila by absencia takéhoto spracovania údajov tomu, aby produkt s digitálnymi prvkami plnil jednu zo svojich funkcií? .....                                   | 63 |
| 8.1.3. | Bol softvér navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť?.....                                                                                        | 64 |
| 8.2.   | Praktické a technické dôsledky riešenia spracovania údajov na diaľku a spoliehania sa na riešenia tretích strán .....                                             | 66 |
| 8.3.   | Príklady použitia riešenia spracovania údajov na diaľku .....                                                                                                     | 68 |
| 8.3.1. | Aplikácia pre mobilné bankovníctvo .....                                                                                                                          | 68 |
| 8.3.2. | Inteligentný termostát .....                                                                                                                                      | 70 |
| 8.3.3. | Čítačka e-knží .....                                                                                                                                              | 70 |
| 8.3.4. | Priemyselný robot .....                                                                                                                                           | 71 |
| 8.3.5. | Mobilná sieť.....                                                                                                                                                 | 71 |
| 9.     | Ďalšie prvky .....                                                                                                                                                | 72 |
| 9.1.   | Oznamovacie povinnosti .....                                                                                                                                      | 72 |
| 9.2.   | Riešenie zraniteľností .....                                                                                                                                      | 75 |
| 9.2.1. | Oznamovanie smerom nahor v dodávateľskom reťazci a zdieľanie bezpečnostných opráv .                                                                               | 75 |
| 9.2.2. | Známe zneužívané zraniteľnosti .....                                                                                                                              | 76 |
| 9.2.3. | Účinné a pravidelné testovanie a preskúmanie .....                                                                                                                | 77 |
| 9.3.   | Vzájomné pôsobenie s inými právnymi predpismi.....                                                                                                                | 78 |
| 9.3.1. | Nariadenie (EÚ) 2019/2144 a nariadenie (EÚ) č. 168/2013.....                                                                                                      | 78 |

|                                                                      |    |
|----------------------------------------------------------------------|----|
| 9.3.2. Platnosť certifikátov EÚ skúšky typu (článok 69 ods. 1) ..... | 79 |
|----------------------------------------------------------------------|----|

# 1. Úvod

## 1.1. Akt o kybernetickej odolnosti

1. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)<sup>1</sup> nadobudlo účinnosť 10. decembra 2024. Cieľom nariadenia je posilniť prístup EÚ ku kybernetickej bezpečnosti, riešiť kybernetickú odolnosť na úrovni EÚ a zlepšiť fungovanie vnútorného trhu stanovením jednotného právneho rámca pre základné požiadavky kybernetickej bezpečnosti pri uvádzaní produktov s digitálnymi prvkami na trh EÚ, ako aj počas životného cyklu produktu s digitálnymi prvkami.
2. Akt o kybernetickej odolnosti (CRA) vychádza z nového legislatívneho rámca EÚ (NLF) stanoveného v nariadení (ES) č. 765/2008 Európskeho parlamentu a Rady z 9. júla 2008, ktorým sa stanovujú požiadavky na akreditáciu a dohľad nad trhom v súvislosti s uvádzaním produktov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 a rozhodnutí č. 768/2008/ES Európskeho parlamentu a Rady z 9. júla 2008 o spoločnom rámci pre uvádzanie produktov na trh a ktorým sa zrušuje rozhodnutie Rady 93/465/EHS<sup>2</sup>.
3. Dohľad nad trhom a presadzovanie právnych predpisov vykonávajú vnútroštátne orgány dohľadu nad trhom. Na produkty s digitálnymi prvkami, ktoré spadajú do pôsobnosti CRA, sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1020 z 20. júna 2019 o dohľade nad trhom a súlade výrobkov, ktorým sa mení a dopĺňa smernica 2004/42/ES a nariadenia (ES) č. 765/2008 a (EÚ) č. 305/2011. Komisia a Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) podporujú hospodárske subjekty a členské štáty pri uplatňovaní CRA.

## 1.2. Účel usmernení

4. Článok 26 ods. 1 CRA ukladá Komisii povinnosť zverejniť usmernenia s cieľom pomôcť hospodárskym subjektom pri uplatňovaní nariadenia, so zvláštnym dôrazom na uľahčenie dosiahnutia súladu zo strany mikropodnikov, malých a stredných podnikov (MSP). V článku 26 ods. 2 sú stanovené minimálne aspekty, ktoré by mali byť v usmerneniach zahrnuté. Patria medzi ne:
  - i) rozsah pôsobnosti CRA (najmä riešenia spracovania údajov na diaľku, slobodný softvér a softvér s otvoreným zdrojovým kódom);
  - ii) pojem „obdobie podpory“;
  - iii) vzájomné pôsobenie medzi CRA a inými právnymi predpismi EÚ;
  - iv) pojem „podstatná úprava“.

<sup>1</sup> Ú. v. EÚ L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>

<sup>2</sup> Pracovný program Komisie na rok 2026 počíta s predložením „európskeho aktu o výrobkoch“, ktorým sa aktualizuje NLF a pravidlá týkajúce sa dohľadu nad trhom a normalizácie: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0870>

5. Dňa 3. decembra 2025 Komisia uverejnila súbor často kladených otázok (FAQ), ktorých cieľom je pomôcť hospodárskym subjektom pripraviť sa na vykonávanie CRA3.
6. Tieto usmernenia majú pomôcť hospodárskym subjektom dodržiavať CRA a podporiť činnosť orgánov dohľadu nad trhom, notifikujúcich orgánov a notifikovaných osôb s cieľom zabezpečiť harmonizované presadzovanie CRA v celej Únii. Tieto usmernenia nemajú za cieľ pokryť CRA v celom jej rozsahu, ale skôr poskytnúť vysvetlenia k odôvodneniu niektorých kľúčových ustanovení a k tomu, ako by sa mohli uplatňovať v praxi. Tieto usmernenia sa týkajú CRA a nevzťahujú sa na iné právne predpisy EÚ.
7. Pri príprave týchto usmernení prebehli rozsiahle konzultácie so zainteresovanými stranami, vrátane expertnej skupiny pre kybernetickú bezpečnosť produktov s digitálnymi prvkami<sup>4</sup> a prostredníctvom verejnej konzultácie, ktorá sa konala v období od 3. marca do 13. apríla 2026<sup>5</sup>.
8. Tieto usmernenia nie sú záväzné pre hospodárske subjekty ani iné subjekty, na ktoré sa vzťahuje CRA. Autoritatívny výklad CRA môže poskytnúť iba Súdny dvor Európskej únie. Tieto usmernenia však stanovujú výklad CRA zo strany Komisie s cieľom podporiť dodržiavanie predpisov a prispieť k účinnému vykonávaniu nariadenia. Okrem toho usmernenia obsahujú viacero príkladov, ktoré ilustrujú uplatňovanie konkrétnych ustanovení. Tieto príklady však nemajú nahradiť posúdenie každého prípadu osobitne, ktoré bude vždy potrebné s ohľadom na špecifiká každého jednotlivého prípadu.
9. V súlade s článkom 26 CRA môže Komisia zvážiť vydanie ďalších usmernení, vrátane usmernení zameraných na výrobcov, na ktorých sa vzťahuje CRA a ďalšie harmonizačné právne predpisy Únie alebo iné súvisiace právne akty Únie. Tieto usmernenia sa môžu napríklad zaoberať otázkami týkajúcimi sa vzájomného pôsobenia medzi CRA a nariadením (EÚ) 2024/1689, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii), a nariadením (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (DORA).

---

<sup>3</sup> Často kladené otázky si možno stiahnuť z [webovej stránky Komisie venovanej vykonávaniu CRA](#), a to na špeciálnej [webovej stránke s často kladenými otázkami](#).

<sup>4</sup> Skupina odborníkov pre kybernetickú bezpečnosť produktov s digitálnymi prvkami v registri expertných skupín Komisie a iných podobných subjektov.

<sup>5</sup> Verejná konzultácia k návrhu usmernení Komisie k aktu o kybernetickej odolnosti.

## 2. Rozsah pôsobnosti

### 2.1. Uvedenie na trh

10. CRA sa vzťahuje na produkty s digitálnymi prvkami, ktoré sú sprístupnené na trhu EÚ. Pojem „sprístupnenie na trhu“ je v článku 3 ods. 22 aktu o kybernetickej odolnosti definovaný ako „dodávka produktu s digitálnymi prvkami na distribúciu alebo použitie na trhu Únie v rámci obchodnej činnosti, či už za odplatu alebo bezodplatne“. V súlade s článkom 3 ods. 21 sa produkt s digitálnymi prvkami uvádza na trh EÚ v okamihu, keď je po prvýkrát sprístupnený.
11. Najnovšie vydanie „Modrej príručky o vykonávaní pravidiel EÚ týkajúcich sa produktov“, uverejnené v roku 2022 (ďalej len „Modrá príručka“)<sup>6</sup>, poskytuje usmernenia uľahčujúce pochopenie pravidiel EÚ týkajúcich sa produktov a ich jednotné uplatňovanie v rôznych sektorových právnych rámcoch zosúladených s novým legislatívnym rámcom (NLF), ako je napríklad CRA. Modrá príručka uvádza, že pojmy „uvádzanie na trh“ a „sprístupňovanie“ sa majú chápať tak, že sa vzťahujú „na každý jednotlivý produkt, nie na typ produktu, a to bez ohľadu na to, či bol vyrobený ako samostatná jednotka alebo sériovo“ (časť 2.3).
12. V prípade „tradičnejších“ produktov s digitálnymi prvkami, na ktoré sa vzťahuje NLF, ako je hardvér vo forme strojov alebo rádiových zariadení s digitálnymi prvkami, je pojem „uviedenie na trh“ dobre ustanovený a Modrá príručka poskytuje ďalšie usmernenia na objasnenie toho, kedy sa takéto produkty považujú za uvedené na trh. „Súhrnné príklady“ uvedené v oddiele 2.12 Modrej príručky poskytujú ďalšie príklady pojmu „uviedenie na trh“.
13. Vzhľadom na povahu nehmotných produktov s digitálnymi prvkami, ako je samostatný softvér, sú však potrebné ďalšie usmernenia o tom, kedy sa takéto produkty s digitálnymi prvkami považujú za uvedené na trh. Akonáhle je fáza výroby softvéru dokončená a produkt s digitálnymi prvkami je ponúknutý potenciálnym používateľom na trhu EÚ, možno považovať jeho výrobcu za subjekt, ktorý vyrobil viacero kópií toho istého softvérového produktu s digitálnymi prvkami a dodal ich na distribúciu alebo používanie. Na rozdiel od hmotných produktov s digitálnymi prvkami totiž samostatný softvér nepodlieha obmedzeniam fyzickej výroby ani zásob: každý akt sprístupnenia softvéru na stiahnutie alebo distribúciu vedie k vytvoreniu novej identickej kópie pre používateľa. Pokiaľ táto verzia softvéru nie je upravená spôsobom, ktorý ovplyvňuje súlad s CRA, uvedenie na trh EÚ sa považuje za uskutočnené v okamihu prvého ponúknutia na distribúciu alebo používanie. Možnosť následného stiahnutia alebo distribúcie tejto verzie softvérového produktu s digitálnymi prvkami sa preto považuje za prípad, keď je tento softvérový produkt s digitálnymi prvkami sprístupnený<sup>7</sup>.
14. Samostatný softvérový produkt s digitálnymi prvkami by sa preto mal považovať za

<sup>6</sup> Oznámenie Komisie – „Modrá príručka“ o vykonávaní pravidiel EÚ týkajúcich sa produktov z roku 2022 (text s významom pre EHP) 2022/C 247/01, Ú. v. EÚ C 247, 29.6.2022, s. 1–152.

<sup>7</sup> V súlade s článkom 13 ods. 11 môžu výrobcovia udržiavať verejné archívy softvéru, ktoré zlepšujú prístup používateľov k historickým verziám. V takýchto prípadoch musia byť používatelia jasne a ľahko zrozumiteľným spôsobom informovaní o rizikách spojených s používaním nepodporovaného softvéru.

uvedený na trh v okamihu, keď je dokončená jeho výrobná fáza a tento softvér je po prvýkrát dodaný na distribúciu alebo používanie na trhu EÚ v rámci obchodnej činnosti. Malo by sa považovať, že výrobca uviedol na trh viacero kópií toho istého softvérového produktu s digitálnymi prvkami súčasne. Preto hoci viaceré kópie toho istého softvéru zostávajú samostatnými produktmi s digitálnymi prvkami, považujú sa za uvedené na trh súčasne, bez ohľadu na to, kedy sa vlastníctvo alebo používanie každej jednotlivéj kópie prevedie na inú fyzickú alebo právnickú osobu. Zároveň, ak výrobca sprístupňuje softvér v rôznych variantoch, ktoré sa líšia svojimi zahrnutými komponentmi, konfiguráciami alebo povolenými funkcionalitami (napríklad verzie pre rôzne operačné systémy alebo balíky s odlišnými súbormi prvkov), tieto varianty nemožno považovať za viacero kópií toho istého softvérového produktu s digitálnymi prvkami. Na účely uvedenia na trh by sa preto mali považovať za odlišné produkty s digitálnymi prvkami.

*Príklad 1: 1. januára 2028 spoločnosť A po prvýkrát dodá na distribúciu prostredníctvom svojej webovej stránky verziu 1.0.0 svojho softvéru X. V ten istý deň si zákazník 1 zakúpi kópiu verzie 1.0.0 softvéru X. 15. januára 2028 si zákazník 2 zakúpi kópiu verzie 1.0.0 softvéru X. Obidve kópie verzie 1.0.0 softvéru X sú uvedené na trh 1. januára 2028.*

15. Vzhľadom na iteratívny charakter vývoja softvéru by sa malo ďalej objasniť, že následné iterácie softvérového produktu s digitálnymi prvkami sa považujú za novo uvedené na trh, ak tieto iterácie spĺňajú kritériá „podstatnej úpravy“ softvérového produktu s digitálnymi prvkami, ktorý je už uvedený na trhu, ako sa uvádza v odôvodnení 41 CRA. Iterácie, ktoré nespĺňajú kritériá podstatných úprav, nevyžadujú, aby výrobca vykonal nový postup posudzovania zhody, a preto nemenia dátum uvedenia daného softvéru na trh. Ďalšie usmernenia k pojmu podstatných úprav nájdete v časti 4. *Podstatné úpravy.*

*Príklad 2: Dňa 1. januára 2028 spoločnosť A po prvýkrát dodá na distribúciu prostredníctvom svojej webovej stránky verziu 1.0.0 softvéru X. V ten istý deň si zákazník 1 zakúpi kópiu verzie 1.0.0 softvéru X. Dňa 15. januára 2028 spoločnosť A vydá aktualizovanú verziu 1.0.1 softvéru X, ktorá nepredstavuje podstatnú úpravu. Dňa 30. januára 2028 si zákazník 2 zakúpi kópiu verzie 1.0.1 softvéru X. Obidve kópie verzií 1.0.0 aj 1.0.1 softvéru X sa považujú za uvedené na trh 1. januára 2028.*

16. Usmernenia uvedené v bodoch 13, 14 a 15 sa uplatňujú výlučne v prípade, ak ide o samostatný softvér obsahujúci digitálne prvky. V prípade kombinácie hardvéru a softvéru to však neplatí, ako sa uvádza v oddiele 2.4 *Kombinácia hardvéru a softvéru tvoriaca produkt.*

## 2.2. Softvér ako produkt s digitálnymi prvkami

17. Článok 3 ods. 1 CRA definuje produkt s digitálnymi prvkami ako „softvérový alebo hardvérový produkt a jeho riešenia spracovania údajov na diaľku vrátane softvérových alebo hardvérových komponentov, ktoré sa uvádzajú na trh samostatne“. Takéto produkty s digitálnymi prvkami spadajú do pôsobnosti CRA, ak ich zamýšľaný účel alebo

odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti.

18. CRA sa preto môže vzťahovať na širokú škálu produktov s digitálnymi prvkami, vrátane:
  - i) samostatného softvéru, ako sú aplikácie a počítačové programy, bez ohľadu na to, či sú distribuované digitálne alebo fyzicky;
  - ii) hardvéru so zabudovaným softvérom (napr. zariadenia internetu vecí, notebooky, tablety);
  - iii) samostatného hardvéru (napr. integrované obvody, základné dosky);
  - iv) akejkolvek kombinácie hardvéru a softvéru dodávaných samostatne, ale určených na spoločnú prevádzku.
19. Samostatný softvér preto spadá do pôsobnosti CRA, ak je uvádzaný na trh ako produkt s digitálnymi prvkami. Je užitočné rozlišovať medzi softvérovými produktmi s digitálnymi prvkami, na ktoré sa vzťahuje CRA, a poskytovaním služieb na diaľku, ktoré do pôsobnosti CRA nespádajú.
20. Aby softvér spadol do pôsobnosti CRA, softvérový produkt s digitálnymi prvkami musí byť poskytnutý používateľovi, získaný týmto používateľom a prevádzkovaný na elektronickom informačnom systéme na strane používateľa alebo ako jeho súčasť. Softvér, ktorý je stiahnutý, nainštalovaný alebo inak dodaný používateľovi a ktorý sa spúšťa v elektronickom informačnom systéme používateľa, spĺňa tieto kritériá, a to aj v prípade, ak má napríklad formu rozšírenia prehliadača alebo aplikácie vyvinutej s využitím webových technológií, ktorá je však dodávaná na lokálne spustenie.
21. Naopak, softvér, ktorý sa spúšťa na diaľku a ku ktorému má používateľ iba prístup, nie je na základe tohto kritéria sám osebe produktom s digitálnymi prvkami. Odôvodnenia 11 a 12 CRA v skutočnosti tento rozdiel zdôrazňujú, že vysvetľujú, že spracovanie alebo ukladanie na diaľku podlieha CRA len v rozsahu, v akom je to nevyhnutné na to, aby produkt s digitálnymi prvkami plnil svoju funkciu (t. j. prostredníctvom pojmu „spracovanie údajov na diaľku“ v zmysle článku 3 ods. 2), a nie samotné spracovanie alebo ukladanie ako produkty s digitálnymi prvkami. To platí typicky pre webové aplikácie, vrátane progresívnych webových aplikácií, ku ktorým sa pristupuje výlučne prostredníctvom webového prehliadača. To isté platí pre webové stránky: hoci sa webové stránky môžu v obmedzenom rozsahu technicky spúšťať a vykonávať na zariadení používateľa, z odôvodnenia č. 12 CRA vyplýva, že samotné webové stránky sa nemajú považovať za produkty s digitálnymi prvkami a spadajú do pôsobnosti CRA len vtedy, ak podporujú funkcionality produktu s digitálnymi prvkami, t. j. v rozsahu, v akom spĺňajú podmienky spracovania údajov na diaľku (ako je podrobnejšie vysvetlené v oddiele 8, a najmä v bode 8.1.2 „Zabránila by absencia takéhoto spracovania údajov tomu, aby produkt s digitálnymi prvkami plnil jednu zo svojich funkcií?“).

*Príklad 3: Mobilná aplikácia, ktorú si používateľ stiahne z obchodu s aplikáciami a nainštaluje na svoj smartfón, sa používateľovi dodáva a spúšťa sa na zariadení používateľa, a preto je produktom s digitálnymi prvkami. Ak sa uvádza na trh v rámci obchodnej činnosti, môže spadať do pôsobnosti CRA.*

*Príklad 4: Desktopová aplikácia vytvorená s využitím webových technológií, ale cielená*

na účely lokálnej inštalácie, je dodaná používateľovi a spúšťa sa na zariadení používateľa, a preto je produktom s digitálnymi prvkami. Ak je uvedená na trh v rámci obchodnej činnosti, môže spadať do pôsobnosti CRA.

*Príklad 5: Webová aplikácia, ku ktorej má používateľ prístup výlučne prostredníctvom webového prehliadača, nie je produktom s digitálnymi prvkami. Pokiaľ nepodporuje funkcionality produktu s digitálnymi prvkami, nespadá do pôsobnosti CRA. Naopak, aplikácia dodaná používateľovi ako lokálne nainštalovaný klient, ktorá sa spúšťa na zariadení používateľa, je produktom s digitálnymi prvkami. Ak je uvedená na trh v rámci obchodnej činnosti, môže spadať do pôsobnosti CRA. Ak sa tento klient na vykonávanie jednej alebo viacerých svojich funkcií spolieha na spracovanie údajov na diaľku, ktoré spĺňa definíciu spracovania údajov na diaľku, toto spracovanie údajov na diaľku je tiež súčasťou produktu s digitálnymi prvkami.*

*Príklad 6: webová stránka, ktorá svojim návštevníkom iba poskytuje informácie a nepodporuje funkcionality produktu s digitálnymi prvkami, sama o sebe nie je produktom s digitálnymi prvkami. Nepatrí preto do pôsobnosti CRA.*

## 2.3. Počítačový kód

22. Je tiež užitočné objasniť, či zdrojový kód môže predstavovať softvérový produkt s digitálnymi prvkami. CRA definuje softvér ako „časť elektronického informačného systému, ktorý pozostáva z počítačového kódu“ (článok 3 ods. 4). Počítačový kód môže mať formu:

- i) strojového kódu, čo je súbor inštrukcií priamo vykonávaných procesorom počítača, napísaných v binárnom formáte;
- ii) zdrojového kódu, t. j. súboru inštrukcií a príkazov napísaných v programovacom jazyku, ktoré musia byť skompilované alebo interpretované, aby ich mohol počítač vykonať.

Definícia softvéru stanovená v CRA zahŕňa obidve formy.

23. Samostatnou otázkou je, či dané dodanie počítačového kódu predstavuje uvedenie produktu s digitálnymi prvkami na trh EÚ, čo si vyžaduje dodanie v rámci obchodnej činnosti. V prípade zdrojového kódu to často nemusí platiť. Napríklad fyzická alebo právnická osoba, ktorá zdieľa slobodne šíriteľný počítačový kód s otvoreným zdrojovým kódom vo verejne prístupných repozitároch (úložiskách), sa na účely CRA vo všeobecnosti nepovažuje za subjekt uvádzajúci tento kód na trh EÚ (ako sa podrobnejšie rozoberá v časti 3 *Slobodný softvér a softvér s otvoreným zdrojovým kódom*). Nedokončený kód zdieľaný počas fázy návrhu a vývoja produktu s digitálnymi prvkami (napr. na účely testovania alebo preskúmania) sa na účely CRA tiež nepovažuje za uvedený na trh, keďže jeho výrobná fáza nie je dokončená. Podobne vzorový alebo demonštračný kód poskytovaný ako súčasť návodov alebo školiacich materiálov, sa na účely CRA<sup>8</sup> takisto nepovažuje za uvedený na trh.
24. Na druhej strane, ak výrobca poskytuje svojim zákazníkom počítačový kód ako produkt

---

<sup>8</sup> Treba tiež pripomenúť, že článok 4 ods. 3 umožňuje výrobcovi uvádzať na trh nedokončený softvér, ktorý nespĺňa požiadavky nariadenia, ako sú alfa verzie, beta verzie alebo kandidátske verzie, za predpokladu, že tento nedokončený softvér je sprístupnený len na dobu potrebnú na jeho testovanie a zber spätnej väzby.

s digitálnymi prvkami, tento kód sa považuje za uvedený na trh, bez ohľadu na to, či ide o strojový kód alebo zdrojový kód<sup>9</sup>.

*Príklad 7: Spoločnosť A poskytuje spoločnosti B licenciu na zdrojový kód pre prispôsobiteľnú internú platformu a tento zdrojový kód poskytuje v textovom súbore. Aj keby tento zdrojový kód vyžadoval ďalšie prispôbenie a kompiláciu zo strany spoločnosti B pred jeho použitím, spoločnosť A tento zdrojový kód uvádza na trh, a preto podlieha CRA. Spoločnosť A nie je zodpovedná za súlad následných úprav a kompilácie tohto kódu zo strany spoločnosti B s CRA.*

## 2.4. Kombinácia hardvéru a softvéru tvoriaca produkt s digitálnymi prvkami

25. To, či je softvér súčasťou produktu s digitálnymi prvkami, by sa nemalo posudzovať podľa toho, ako alebo kedy je tento softvér dodaný používateľovi, ale podľa toho, či je softvér vzhľadom na zamýšľaný účel produktu a odôvodnene predvídateľné použitie nevyhnutný na to, aby produkt s digitálnymi prvkami plnil svoje zamýšľané funkcie. Ak je hardvérový produkt s digitálnymi prvkami navrhnutý tak, aby na plnenie svojich funkcií spolupracoval s konkrétnym softvérom poskytnutým tým istým výrobcom, hardvér a tento softvér spolu tvoria produkt s digitálnymi prvkami. Softvér, ktorý je nevyhnutný na prevádzku, konfiguráciu, ovládanie alebo používanie produktu s digitálnymi prvkami v súlade s jeho zamýšľaným účelom, je preto súčasťou produktu s digitálnymi prvkami, aj keď sa získava prostredníctvom samostatného kanála (napr. obchodu s aplikáciami, odkazu na stiahnutie alebo iného digitálneho kanála po tom, čo bol hardvérový produkt s digitálnymi prvkami uvedený na trh). K jeho uvedeniu na trh teda dochádza v rovnakom čase, ako sa na trh uvádzajú jednotky hardvérových produktov s digitálnymi prvkami.

*Príklad 8: Sieťová tlačiareň sa uvádza na trh ako hardvérový produkt s digitálnymi prvkami, zatiaľ čo softvérové ovládače potrebné na odosielanie tlačových úloh, konfiguráciu zariadenia a riadenie jeho prevádzky sú k dispozícii na stiahnutie z webovej stránky výrobcu. Hoci sa tlačiareň a ovládače dodávajú prostredníctvom rôznych kanálov, spolu tvoria jeden produkt s digitálnymi prvkami, pretože tlačiareň nemôže plniť svoj zamýšľaný účel bez ovládačov.*

*Príklad 9: Na trh sa uvádza nositeľné fitness zariadenie na meranie srdcovej frekvencie a aktivity používateľa, pričom na zobrazenie nameraných hodnôt, históriu a konfiguráciu zariadenia je potrebná aplikácia pre smartfóny poskytovaná výrobcom. Hoci sa aplikácia sťahuje samostatne prostredníctvom obchodu s aplikáciami, nositeľné zariadenie a aplikácia spolu tvoria jeden produkt s digitálnymi prvkami, pretože sú navrhnuté a určené na spoločnú prevádzku s cieľom zabezpečiť funkcionálnosť produktu*

---

<sup>9</sup> Na druhej strane je potrebné poznamenať, že na účely práva týkajúceho sa zodpovednosti za produkt samotný počítačový kód nepredstavuje produkt, a preto výrobcovia, ktorí takýto kód uvádzajú na trh, nemôžu byť zodpovední podľa smernice (EÚ) 2024/2853 (smernica o zodpovednosti za produkt). V odôvodnení č. 13 uvedenej smernice sa uvádza, že „informácie sa však nemajú považovať za produkt, a preto by sa pravidlá o zodpovednosti za produkt nemali vzťahovať na obsah digitálnych súborov, ako sú mediálne súbory alebo elektronické knihy, ani na samotný zdrojový kód softvéru“. To nevylučuje, že výrobcovia môžu niesť zodpovednosť podľa vnútroštátneho práva týkajúceho sa deliktov.

s digitálnymi prvkami.

## 2.5. Dátové pripojenie

26. V článku 2 ods. 1 sa uvádza, že CRA „uplatňuje na produkty s digitálnymi prvkami sprístupnenými na trhu, ktorých zamýšľaný účel alebo odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k zariadeniu alebo sieti“. Rozsah pôsobnosti CRA teda nespočíva v samotnej prítomnosti elektroniky, ale v schopnosti produktu s digitálnymi prvkami vymieňať si digitálne informácie.
27. Hoci pojmy „logické pripojenie“ a „fyzické pripojenie“ sú definované v článku 3, CRA nedefinuje pojmy „dátové pripojenie“ ani „digitálne údaje“. Je preto užitočné uviesť výklad toho, čo je dátové pripojenie, s cieľom objasniť hranice rozsahu pôsobnosti CRA. Táto hranica je obzvlášť dôležitá na rozlíšenie produktov s digitálnymi prvkami, ktoré iba využívajú elektrické signály, od tých, ktoré sa podieľajú na digitálnej komunikácii a sú preto vystavené kybernetickobezpečnostným rizikám.
28. V najzákladnejšej podobe dátové pripojenie zahŕňa prenos informácií v binárnej forme, t. j. ako postupnosť núl a jednotiek. Samotné zapínanie a vypínanie výstupu (t. j. 0/1) ešte samo osebe nepredstavuje dátové pripojenie, ak tieto stavy nemajú reprezentovať údaje alebo nie sú čítané digitálnym vstupom. Aby dátové spojenie existovalo, binárne stavy musia byť zdrojom zámerne zakódované ako informácie a musia byť dekodované na mieste určenia ako informácie. Inými slovami, musí existovať odosielateľ, ktorý zámerne generuje digitálne symboly podľa definovanej schémy, a prijímateľ schopný interpretovať tieto symboly ako údaje. Ak sa elektrické alebo elektronické signály používajú výlučne na spustenie alebo napájanie funkcie bez prenosu digitálne zakódovaných informácií, na účely CRA neexistuje dátové pripojenie, a preto produkt s digitálnymi prvkami nespadá do rozsahu pôsobnosti článku 2 ods. 1.

## 2.6. Zložité systémy

29. Produkty s digitálnymi prvkami, ktoré spadajú do pôsobnosti CRA, môžu pozostávať nielen z samostatných zariadení alebo softvérových komponentov, ale aj zo zložitých systémov, vrátane systémov zložených z viacerých hardvérových a softvérových prvkov, ktoré spolupracujú na vykonávaní určitej funkcie. Ak sa takýto systém uvádza na trh ako jeden produkt s digitálnymi prvkami, predstavuje produkt s digitálnymi prvkami v zmysle CRA.
30. Takéto komplexné systémy sa často vyznačujú dlhými cyklami návrhu a vývoja, pričom zmluvy mohli byť podpísané ešte pred začatím uplatňovania CRA, majú predĺženú prevádzkovú životnosť a vysoký stupeň technickej a organizačnej zložitosti. Takéto systémy, ktoré majú byť uvedené na trh po začatí uplatňovania CRA, sa môžu opierať o komponenty uvedené na trh pred začatím uplatňovania CRA, o zavedené architektúry alebo o široko používané normy interoperability, vrátane noriem uvedených v iných právnych predpisoch EÚ alebo v odvetvových rámcoch. V dôsledku toho môže byť úprava určitých technických charakteristík týchto systémov náročná alebo neprimeraná bez toho, aby to ovplyvnilo ich zamýšľaný účel, bezpečnosť, spoľahlivosť alebo interoperabilitu s existujúcou infraštruktúrou.

31. Tieto charakteristiky samy osebe nevylučujú komplexné systémy z pôsobnosti CRA. Skôr ilustrujú uplatňovanie prístupu CRA založeného na riziku, ktorý umožňuje preukázať súlad rôznymi spôsobmi v závislosti od charakteristík a obmedzení produktu s digitálnymi prvkami v súlade s článkom 13 ods. 3 CRA. Tieto charakteristiky tvoria súčasť zamýšľaného účelu a prevádzkového kontextu a sú preto relevantné pri posudzovaní súladu so základnými požiadavkami kybernetickej bezpečnosti (ďalej len „základné požiadavky“). Najmä v odôvodnení č. 55 sa výslovne uznáva, že niektoré základné požiadavky nemusia byť plne zlučiteľné s povahou produktu s digitálnymi prvkami. Môže to byť napríklad v prípade, ak by súlad narušil povinné požiadavky na interoperabilitu alebo riadne fungovanie systému.
32. Výrobcovia sú preto povinní riešiť kybernetickobezpečnostné riziká na základe posúdenia kybernetickobezpečnostného rizika uvedeného v článku 13 ods. 2. Ako sa vysvetľuje aj v odôvodnení 55, v niektorých prípadoch sa konkrétne základné požiadavky neuplatňujú alebo ich nie je možné splniť zavedením najmodernejších bezpečnostných opatrení, a to napríklad z dôvodu zamýšľaného účelu systému, ktorý vyžaduje, aby produkt s digitálnymi prvkami interagoval s existujúcimi závislosťami alebo spĺňal určité požiadavky na interoperabilitu. V takýchto prípadoch by výrobcovia mali identifikovať a zdokumentovať tieto špecifické obmedzenia, posúdiť súvisiace riziká a zaviesť primerané alternatívne alebo kompenzačné opatrenia na zmiernenie rizík, aby nedošlo k ohrozeniu bezpečnosti produktu s digitálnymi prvkami. Na tieto účely zohrávajú kľúčovú úlohu pri transparentnom opise identifikovaných obmedzení, súvisiacich kybernetickobezpečnostných rizík a zavedených opatrení na zmiernenie rizík tak technická dokumentácia uvedená v článku 31, ako aj informácie a pokyny pre používateľa uvedené v prílohe II. V súlade s povinnosťou aktualizovať posúdenie rizika počas obdobia podpory by výrobcovia mali tiež pravidelne opätovne posudzovať, či takéto obmedzenia naďalej existujú. Ak je možné takéto obmedzenia v priebehu času odstrániť alebo znížiť, výrobcovia by mali produkt s digitálnymi prvkami zodpovedajúcim spôsobom aktualizovať, aby sa mohol priblížiť k primeranej úrovni kybernetickej bezpečnosti<sup>10</sup>.

*Príklad 10: Výrobca uvádza na trh produkt s digitálnymi prvkami, ktorý komunikuje s externými systémami prostredníctvom sieťového protokolu. V rámci uplatňovania základných požiadaviek výrobca na základe posúdenia kybernetickobezpečnostného rizika zistí, že na zabezpečenie dôvernosti a integrity údajov, ktoré si produkt s digitálnymi prvkami vymieňa, je potrebné použiť bezpečný komunikačný protokol. Jeho zamýšľaný účel však zahŕňa interoperabilitu s existujúcimi systémami, ktoré podporujú iba starší alebo menej bezpečný protokol. V takýchto prípadoch môže výrobca implementovať tento protokol, ak je to potrebné na dosiahnutie interoperability, za predpokladu, že súvisiace kybernetickobezpečnostné riziká sú identifikované a zmiernené inými prostriedkami. Ak je technicky možné, aby produkt s digitálnymi prvkami podporoval aj bezpečný protokol, aj menej bezpečný protokol, od výrobcu sa očakáva, že implementuje bezpečný protokol a povolí jeho používanie ako*

---

<sup>10</sup> Je potrebné poznamenať, že úvahy uvedené v tomto odseku sa môžu podľa potreby vzťahovať na všetky produkty s digitálnymi prvkami, ktoré spadajú do rozsahu pôsobnosti CRA, a nielen na „zložité systémy“.

*predvolené nastavenie. Menej bezpečný protokol by bol povolený len v prípade, ak je to nevyhnutné na zabezpečenie interoperability.*

*Príklad 11: Výrobca systému priemyselnej automatizácie zakúpi niektoré mikrokontroléry pred začatím uplatňovania CRA. Výrobca vykoná posúdenie kybernetickobezpečnostných rizík pre svoj systém priemyselnej automatizácie, ktorý má byť uvedený na trh po začatí uplatňovania CRA. Na základe tohto posúdenia kybernetickobezpečnostného rizika výrobca nezistil žiadne konkrétne kybernetickobezpečnostné riziká spojené s používaním jedného z týchto mikrokontrolérov. Výrobca ho integruje do svojho systému priemyselnej automatizácie a zabezpečí, aby produkt s digitálnymi prvkami ako celok (systém priemyselnej automatizácie) spĺňal základné požiadavky.*

## 2.7. Produkty s digitálnymi prvkami navrhnuté pred začatím uplatňovania CRA

33. V niektorých prípadoch výrobca uvedie na trh po začatí uplatňovania CRA dňa 11. decembra 2027 kusy produktu s digitálnymi prvkami, ktoré boli vyrobené v súlade s typom alebo modelom navrhnutým a vyvinutým pred dátumom začatia uplatňovania CRA. V takýchto prípadoch súlad s týmto nariadením nevyžaduje nevyhnutne, aby boli tieto kusy produktu s digitálnymi prvkami prepracované. Výrobca je povinný vykonať posúdenie kybernetickobezpečnostného rizika v súlade s článkom 13 ods. 2 CRA s cieľom určiť na základe zamýšľaného účelu a odôvodnene predvídateľného použitia produktu s digitálnymi prvkami, ktoré zo základných požiadaviek uvedených v časti I prílohy I sa na tento produkt s digitálnymi prvkami vzťahujú a ako sa tieto požiadavky implementujú.
34. Ak výsledok tohto posúdenia rizík preukáže, že produkt s digitálnymi prvkami už obsahuje primerané a účinné bezpečnostné opatrenia zamerané na riešenie príslušných rizík, výrobca sa môže spoliehať na tieto existujúce opatrenia na preukázanie súladu s CRA. CRA sama o sebe neukladá povinnosť zavádzať nové bezpečnostné prvky ani prepracovať návrh produktu s digitálnymi prvkami, ak to nie je potrebné na riešenie zistených rizík.
35. Výrobca však naďalej podlieha povinnostiam stanoveným v CRA. Medzi ne patrí zabezpečenie toho, aby sa pred uvedením produktu s digitálnymi prvkami na trh vykonal príslušný postup posudzovania zhody, bolo vypracované EÚ vyhlásenie o zhode a bolo umiestnené označenie CE. Splnenie týchto požiadaviek je nezávislé od toho, či návrh produktu s digitálnymi prvkami vyžadoval úpravu v dôsledku posúdenia rizika. V prípade produktov s digitálnymi prvkami, ktoré boli navrhnuté pred dátumom začatia uplatňovania CRA, ale uvedené na trh po tomto dátume, ak výrobca nemôže preukázať, ako bolo posúdenie rizík zohľadnené počas fázy návrhu a vývoja produktu s digitálnymi prvkami, povinnosť podľa článku 13 ods. 2 by sa mala chápať tak, že od výrobcov sa vyžaduje, aby vykonali posúdenie kybernetickobezpečnostného rizika a na tomto základe preukázali, že produkt s digitálnymi prvkami obsahuje primerané bezpečnostné opatrenia s cieľom minimalizovať kybernetickobezpečnostné riziká, predchádzať incidentom a minimalizovať ich dopad, a to aj v súvislosti so zdravím a bezpečnosťou

používateľov.

36. V súlade s tým sa produkty s digitálnymi prvkami navrhnuté pred začatím uplatňovania CRA môžu uvádzať na trh podľa CRA bez nutnosti ich prepracovania, za predpokladu, že výrobca môže prostredníctvom posúdenia kybernetickobezpečnostných rizík a technickej dokumentácie preukázať, že produkt s digitálnymi prvkami dosahuje primeranú úroveň kybernetickej bezpečnosti s ohľadom na jeho zamýšľaný účel a odôvodnene predvídateľné použitie a spĺňa základné požiadavky kybernetickej bezpečnosti.
37. Okrem toho je užitočné objasniť uplatňovanie povinností v oblasti posudzovania zhody pre výrobcov produktov s digitálnymi prvkami, ktoré sa uvádzajú na trh po začatí uplatňovania CRA, ale sú vyrobené v súlade s typom alebo modelom navrhnutým a vyvinutým pred týmto dátumom. V súlade s článkom 13 ods. 12 je výrobca povinný prostredníctvom príslušného postupu posudzovania zhody preukázať, že jeho produkt s digitálnymi prvkami je v súlade s príslušnými základnými požiadavkami, a príslušné dôkazy o tom zahrnúť do technickej dokumentácie produktu (bod 6 prílohy VII).
38. Uplatňovanie týchto požiadaviek je však potrebné vykladať s ohľadom na posúdenie kybernetickobezpečnostného rizika a profil kybernetickobezpečnostného rizika produktu s digitálnymi prvkami. Najmä v prípade produktov s digitálnymi prvkami navrhnutých pred dátumom začatia uplatňovania CRA (ale uvedených na trh po tomto dátume), na ktoré sa vzťahujú postupy posudzovania zhody podľa článku 32 ods. 1, ak posúdenie rizika preukáže, že produkt s digitálnymi prvkami už obsahuje primerané a účinné bezpečnostné opatrenia zamerané na riziká daného produktu, povinnosť predložiť dôkazy v rámci postupu posudzovania zhody by sa nemala chápať tak, že od výrobcu sa vyžaduje, aby predložil výsledky skúšok zahŕňajúce pôvodné fázy návrhu a vývoja takýchto produktov s digitálnymi prvkami. To by nebolo potrebné, keďže by to neprispievalo k zvýšeniu bezpečnosti samotného produktu s digitálnymi prvkami. Ak by napriek tomu boli skúšky potrebné, od výrobcov sa neočakáva, že predložia dôkazy o skúškach vykonaných na všetkých variantoch produktov, ale môžu takéto skúšky zoskupiť v rámci skupín produktov s digitálnymi prvkami, ako sa ďalej uvádza v oddiele 7.4 *Opätovné použitie posúdení rizík a dokumentácie o zhode pre skupiny produktov s digitálnymi prvkami*.
39. Výrobca by však mal predložiť dôkazy o tom, ako dodržiava postupy na riešenie zraniteľností stanovené v časti II prílohy I, mal by aktualizovať svoje posúdenie rizika v súlade s článkom 13 ods. 3, ako aj plniť všetky ostatné povinnosti stanovené v CRA, vrátane poskytovania informácií a pokynov používateľom v súlade s článkom 13 ods. 18.

*Príklad 12: Výrobca uvádza na trh mikrokontrolér, ktorý bol navrhnutý a vyvinutý pred dátumom začatia uplatňovania CRA. Mikrokontrolér je určený na integráciu do radu elektronických produktov s digitálnymi prvkami, vrátane produktov s digitálnymi prvkami s funkcionalitami pripojiteľnosti.*

*Pred uvedením nových kusov mikrokontroléra na trh po začatí uplatňovania CRA výrobca vykoná posúdenie kybernetickobezpečnostného rizika v súlade s článkom 13 ods. 2. Na základe zamýšľaného účelu mikrokontroléra a jeho odôvodnene*

*predvídateľného použitia výrobca identifikuje relevantné kybernetickobezpečnostné riziká, ako je neoprávnený prístup, manipulácia so softvérom alebo údajmi a zneužitie dostupných rozhraní.*

*Výsledok posúdenia rizík ukazuje, že mikrokontrolér v pôvodnej podobe už obsahuje primerané a účinné bezpečnostné opatrenia zamerané na identifikované riziká. Výrobca preto dospeje k záveru, že produkt s digitálnymi prvkami spĺňa príslušné základné požiadavky uvedené v časti I prílohy I a že nie je potrebný žiadny nový návrh ani zavedenie dodatočných bezpečnostných funkcionalít.*

*Ak nie je možné preukázať, ako sa posúdenie kybernetickobezpečnostného rizika zohľadnilo počas pôvodnej fázy návrhu a vývoja, výrobca zdokumentuje aktuálne posúdenie kybernetickobezpečnostného rizika a vysvetlí, ako existujúci návrh a opatrenia zmierňujú identifikované riziká. Výrobca nie je povinný znovu vytvárať historickú dokumentáciu o návrhu alebo testovaní, keďže by to neprispelo k zvýšeniu kybernetickej bezpečnosti produktu s digitálnymi prvkami. Ak je viacero variantov mikrokontroléra založených na rovnakom návrhu a majú rovnaký profil kybernetickobezpečnostného rizika, výrobca sa môže opierať aj o reprezentatívne dôkazy týkajúce sa príslušnej skupiny produktov.*

*Výrobca tiež zabezpečuje súlad s požiadavkami na riešenie zraniteľností stanovenými v časti II prílohy I, a to aj prostredníctvom udržiavania procesov na riešenie a odstraňovanie zraniteľností a prostredníctvom priebežného preskúmania posúdenia kybernetickobezpečnostného rizika v súlade s článkom 13 ods. 3.*

*Za týchto okolností sa mikrokontrolér navrhnutý pred dátumom uplatňovania CRA môže uviesť na trh bez prepracovania, ak výrobca prostredníctvom posúdenia kybernetickobezpečnostného rizika a technickej dokumentácie preukáže, že dosahuje primeranú úroveň kybernetickej bezpečnosti s ohľadom na svoj zamýšľaný účel a odôvodnene predvídateľné použitie a spĺňa príslušné základné požiadavky.*

### 3. Slobodný softvér a softvér s otvoreným zdrojovým kódom

40. Ako sa uvádza v časti 2.1 *Uvedenie na trh*, CRA sa vzťahuje na produkty s digitálnymi prvkami, ktoré sa v rámci obchodnej činnosti po prvýkrát sprístupňujú na trhu EÚ (t. j. „uvádzajú sa na trh“), ako aj na akýkoľvek následný prípad, ktorý predstavuje sprístupnenie toho istého produktu s digitálnymi prvkami na trhu. Modrá príručka (časť 2.2) objasňuje, že pod pojmom „obchodná činnosť“ sa rozumie poskytovanie tovaru za odplatu alebo bezodplatne v kontexte súvisiacom s podnikaním a možno ju posudzovať len individuálne v každom jednotlivom prípade, pričom sa zohľadňuje pravidelnosť dodávok, vlastnosti produktu, zámary dodávateľa atď.
41. Dodávka v rámci obchodnej činnosti sa vyznačuje radom okolností, ktoré sú podrobne zdokumentované v Modrej príručke a pripomenuté v odôvodnení č. 15 rozhodnutia CRA. Medzi ne môže patriť priame účtovanie ceny, ako aj „účtovanie ceny za služby technickej podpory, ak nejde len o náhradu skutočných nákladov, so zámerom speňažiť, napríklad poskytnutím softvérovej platformy, prostredníctvom ktorej výrobca speňažuje iné služby, vyžadovaním použitia spracovania osobných údajov ako podmienky z iných dôvodov než výlučne na zlepšenie bezpečnosti, kompatibility alebo interoperability softvéru, alebo prijatím darov presahujúcich náklady spojené s návrhom, vývojom a poskytovaním produktu s digitálnymi prvkami“ (odôvodnenie 15)<sup>11</sup>.
42. CRA však uznáva špecifiká rôznych spôsobov vývoja a zverejňovania „slobodného softvéru a softvéru s otvoreným zdrojovým kódom“ (FOSS) a ponúka určité usmernenia, ktoré pomáhajú určiť, či je FOSS produktom s digitálnymi prvkami uvádzaným na trh (t. j. v rámci obchodnej činnosti) v zmysle CRA. Ako sa vysvetľuje v odôvodnení 18, „samotné okolnosti, za ktorých bol produkt s digitálnymi prvkami vyvinutý, alebo spôsob financovania vývoja by sa [...] preto nemali zohľadňovať pri určovaní toho, či ide o činnosť obchodnej alebo neobchodnej povahy“. Konkrétnejšie, „by sa poskytovanie produktov s digitálnymi prvkami považovanými za slobodný softvér a softvér s otvoreným zdrojovým kódom, ktoré ich výrobcovia nespeňažujú, nemalo považovať za obchodnú činnosť, aby sa zabezpečilo jasné rozlíšenie medzi fázou vývoja a fázou dodávky“.
43. Je preto užitočné:
- i) objasniť, čo je FOSS;
  - ii) kedy sa považuje za spadajúci do zodpovednosti fyzickej alebo právnickej osoby;
  - iii) uviesť príklady, ktoré pomôžu zainteresovaným stranám pochopiť, kedy distribúcia FOSS predstavuje uvedenie na trh.

---

<sup>11</sup> Treba tiež pripomenúť, že hoci sa produkty s digitálnymi prvkami často speňažujú (aj) prostredníctvom spracúvania osobných údajov, ochrana osobných údajov je základným právom, a preto osobné údaje nemožno považovať za tovar, ako sa uvádza v odôvodnení 24 smernice Európskeho parlamentu a Rady 2019/770 z 20. mája 2019 o určitých aspektoch týkajúcich sa zmlúv o dodávke digitálneho obsahu a digitálnych služieb, Ú. v. EÚ L 136, 22.5.2019, s. 1–27, ELI: <http://data.europa.eu/eli/dir/2019/770/oj>.

Ak sa FOSS neuvádza na trh, nespadá do pôsobnosti CRA a pokiaľ subjekt, ktorý ho zverejňuje, nie je právnickou osobou, ktorá spĺňa definíciu „správcu softvéru s otvoreným zdrojovým kódom“ (ďalej len „správca“) podľa článku 3 ods. 14. V takom prípade sa na neho vzťahujú iba povinnosti stanovené v článku 24.

44. Článok 3 ods. 48 definuje FOSS ako „softvér, ktorého zdrojový kód je voľne dostupný a ktorý je vytvorený na základe bezplatnej a otvorenej licencie, ktorá udeľuje všetky práva na voľný prístup k nemu, jeho použiteľnosť, modifikovateľnosť a redistribúciu“. Hoci tieto usmernenia neuvádzajú konkrétne licencie základe bezplatnej a otvorenej licencie, ktoré sú zlučiteľné s definíciou stanovenou v článku 3 ods. 48, zo znenia tohto ustanovenia vyplýva, že na účely CRA sa za FOSS považuje iba softvér, ktorý kumulatívne spĺňa dve podmienky:
- i) softvér musí byť sprístupnený na základe bezplatnej a otvorenej licencie, ktorá udeľuje všetky práva na voľný prístup k nemu uvedených v článku 3 ods. 48;
  - ii) jeho zdrojový kód musí byť verejne zdieľaný.
45. Požiadavka, aby licencia zabezpečovala, že softvér bude „voľne prístupný, použiteľný, modifikovateľný a redistribuovateľný“, odráža tradičné chápanie FOSS, a to, že používatelia musia mať prístup k zdrojovému kódu, môžu ho používať bez neprimeraných obmedzení, môžu upravovať a redistribuovať jeho pôvodné alebo upravované verzie. Prístup k zdrojovému kódu je preto nevyhnutnou podmienkou na uplatňovanie ostatných práv: bez prístupu k zdrojovému kódu nie je prakticky možné softvér upravovať ani zmysluplne opätovne využívať.
46. Avšak v článku 3 ods. 48 nejde len o odkaz na licenčné podmienky, keďže výslovne vyžaduje, aby bol zdrojový kód „verejne zdieľaný“. Pojem „verejne zdieľaný“ znamená, že zdrojový kód musí byť sprístupnený verejnosti (buď „na vyššej úrovni“, alebo „na nižšej úrovni“), a nie len poskytovaný na obmedzenom alebo podmienenom základe. V súlade s tým sa softvér distribuovaný na základe licencie na slobodný softvér a softvér s otvoreným zdrojovým kódom, ktorého zdrojový kód je však zdieľaný (alebo je povolené ho zdieľať) len s platiacimi zákazníkmi alebo obmedzenou skupinou používateľov, nepovažuje za FOSS v zmysle článku 3 ods. 48. Na účely CRA by sa preto za FOSS mal považovať iba softvér, ktorého zdrojový kód je verejne dostupný a je licencovaný na základe licencie na slobodný softvér a softvér s otvoreným zdrojovým kódom, ktorá udeľuje úplný súbor práv uvedených v článku 3 ods. 48.

### 3.1. Určenie, či je slobodný softvér a softvér s otvoreným zdrojovým kódom v zodpovednosti daného subjektu

47. CRA ukladá kľúčové povinnosti hospodárskym subjektom, ktoré dodávajú produkty s digitálnymi prvkami na trh EÚ. Výrobcu definuje ako fyzickú alebo právnickú osobu, ktorá dodáva produkt s digitálnymi prvkami pod svojím menom alebo ochrannou známkou a ktorá tak koná v rámci obchodnej činnosti (čím ho uvádza na trh). Podobne je dovozcom fyzická alebo právnická osoba so sídlom v EÚ, ktorá dodáva produkt s digitálnymi prvkami od osoby so sídlom mimo EÚ a ktorá tak koná v rámci obchodnej činnosti (čím ho uvádza na trh). Povinnosti správcov sa vzťahujú na právnickú osobu,

ktorá dodáva FOSS určený na obchodné účely<sup>12</sup>, ale neuvádza ho na trh v zmysle CRA.

48. Preto na určenie, či fyzická alebo právnická osoba uvádza FOSS na trh EÚ, je najprv potrebné objasniť, či táto fyzická alebo právnická osoba skutočne dodáva FOSS. Na správne stanovenie príslušných povinností podľa CRA je nevyhnutné určiť, či fyzická alebo právnická osoba skutočne vykonáva činnosť dodávania FOSS. Ako sa pripomína v odôvodnení 18, CRA sa totiž nevzťahuje na fyzické alebo právnické osoby, ktoré prispievajú zdrojovým kódom k produktom s digitálnymi prvkami spĺňajúcimi kritériá FOSS, za ktoré nenesú zodpovednosť.
49. Vzhľadom na špecifiká vývoja FOSS, ktorý často zahŕňa viacerých prispievateľov, decentralizované modely spolupráce a oddelenie prispievania od rozhodovania, je užitočné objasniť, že FOSS sa považuje „v zodpovednosti“ fyzických alebo právnických osôb, ktoré ho zverejňujú a vykonávajú primárnu kontrolu nad jeho vývojom, vydaniami a rozhodnutiami o distribúcii (často označované ako „udržiavatelia“). Osoby, ktoré prispievajú zdrojovým kódom, ale nemajú kontrolu nad vydaniami, plánmi vývoja ani rozhodnutiami o riadení, sa považujú za „prispievateľov“; v takýchto prípadoch nie je FOSS v ich zodpovednosti, hoci do neho prispeli kódom. Samotná existencia technických oprávnení, ako je prístup na odosielanie zmien (commit), nestačí na to, aby sa stanovilo, že FOSS je v zodpovednosti danej osoby; zodpovednosť spočíva na tých, ktorí FOSS zverejňujú a kontrolujú.

*Príklad 13: Samostatný vývojár alebo zamestnanec spoločnosti odošle do projektu FOSS žiadosť o „pull“ alebo „merge“ obsahujúcu bezpečnostnú opravu alebo nový prvok. Udržiavatelia projektu kód preskúmajú, prijímú a zlúčia do hlavného repozitára, následne ho zahrnú do novej verzie. V tomto scenári je osoba, ktorá podala žiadosť o „pull“, „prispievateľom“ a nepodlieha CRA. Hoci táto osoba prispela zdrojovým kódom, nevykonáva primárnu kontrolu nad vývojom, vydaniami ani rozhodnutiami o distribúcii.*

## 3.2. Určenie, či je slobodný softvér a softvér s otvoreným zdrojovým kódom uvádzaný na trh EÚ

50. Akonáhle sa zistí, že za FOSS zodpovedá fyzická alebo právnická osoba, je potrebné určiť, či táto osoba tento softvér dodáva v rámci obchodnej činnosti, čím dochádza k jeho uvedeniu na trh.

### 3.2.1. Účtovanie ceny

51. Ak fyzická alebo právnická osoba, ktorá dodáva FOSS, účtuje cenu za samotný softvér (napr. účtovaním ceny za vopred skompilované binárne súbory), táto osoba uvádza na trh produkt s digitálnymi prvkami. Osoba, ktorá uvádza FOSS na trh, je preto výrobcom podľa CRA.
52. Výrobcovia FOSS často poskytujú bezplatné verzie tohto softvéru (často nazývané „komunitné“ verzie), ktorých zdrojový kód je (takmer) identický s platenou verzou.

---

<sup>12</sup> Ide o nevyhnutnú, ale nie postačujúcu podmienku na to, aby sa právnická osoba mohla považovať za správcu softvéru s otvoreným zdrojovým kódom, keďže definícia uvedená v článku 3 ods. 14 stanovuje ďalšie podmienky, ktoré musí právnická osoba spĺňať, aby sa mohla považovať za správcu.

Tieto produkty s digitálnymi prvkami sú však odlišné produkty: platená verzia je nejakým spôsobom speňažovaná (napr. buď účtovaním ceny, alebo inými prostriedkami, ako sa uvádza v tejto časti) a preto sa považuje za uvedenú na trh, čo vyvoláva povinnosti výrobcu. Verzia poskytovaná bezplatne (alebo komunitná verzia) nie je speňažovaná, a preto sa na účely CRA nepovažuje za uvedenú na trh. To platí aj v prípade, ak je platená verzia „vylepšenou“ obchodnou verzou, ktorá rozširuje zdrojový kód verzie poskytovanej bezplatne alebo túto verziu začleňuje do širšieho produktu s digitálnymi prvkami (napr. ako v prípade modelu „open-core“).

53. Ak je poskytovateľom komunitnej verzie právnická osoba, táto právnická osoba podlieha povinnostiam správcov aj v súvislosti s verzou, ktorú poskytuje bezplatne (komunitná verzia). Ak je poskytovateľom fyzická osoba, verzia poskytovaná bezplatne (komunitná verzia) nespadá do pôsobnosti CRA.

### 3.2.2. Speňažovanie iných služieb alebo vyžadovanie spracúvania osobných údajov

54. Fyzická alebo právnická osoba, ktorá zverejňuje FOSS, môže tento softvér zároveň uvádzať na trh (t. j. poskytovať ho v rámci obchodnej činnosti), ak poskytuje softvér, prostredníctvom ktorého zarába na iných produktoch s digitálnymi prvkami alebo službách, alebo ak ako podmienku používania vyžaduje spracúvanie osobných údajov z iných dôvodov, ako je výlučne zlepšenie bezpečnosti, compatibility alebo interoperability softvéru.

*Príklad 14: Fyzická alebo právnická osoba zverejní slobodnú aplikáciu typu „marketplace“ s otvoreným zdrojovým kódom. Aplikácia je k dispozícii bezplatne a umožňuje používateľom prostredníctvom nej nakupovať tovary alebo služby. Aplikácia umožňuje osobe, ktorá ju zverejnila, zarábať na iných produktoch s digitálnymi prvkami a službách ponúkaných prostredníctvom nej (napr. prostredníctvom reklám, provízií alebo poplatkov za predplatné). Aplikácia sa preto považuje za uvedenú na trh v rámci obchodnej činnosti.*

*Príklad 15: Fyzická alebo právnická osoba zverejní slobodnú aplikáciu typu VPN s otvoreným zdrojovým kódom. Aplikácia je k dispozícii bezplatne, umožňuje však používateľom platiť za prístup k dodatočným serverom alebo vyhradeným IP adresám. Táto aplikácia umožňuje danej osobe zarábať na iných službách ponúkaných prostredníctvom nej, a preto sa považuje za uvedenú na trh v rámci obchodnej činnosti.*

*Príklad 16: Fyzická alebo právnická osoba zverejňuje slobodnú aplikáciu s otvoreným zdrojovým kódom na sledovanie fyzickej kondície. Aplikácia je k dispozícii bezplatne, jej používanie je však podmienené spracúvaním osobných údajov používateľov na účely, ako je cieľená reklama alebo analýza, ktoré nesúvisia s bezpečnosťou, kompatibilitou alebo interoperabilitou softvéru. Keďže aplikácia vyžaduje takéto spracúvanie údajov ako podmienku používania, považuje sa za uvedenú na trh v rámci obchodnej činnosti.*

### 3.2.3. Podporné služby

55. Samotná skutočnosť, že fyzická alebo právnická osoba, ktorá zverejňuje FOSS, ponúka aj súvisiace platené podporné služby, ešte sama o sebe neznamena, že produkt

s digitálnymi prvkami sa dodáva v rámci obchodnej činnosti. Podporné služby môžu zahŕňať činnosti, ako je poradenstvo, školenia alebo odborné služby súvisiace s používaním, dokumentáciou, konfiguráciou a nasadením softvéru zo strany zákazníka.

56. Rozhodujúcim faktorom je, či je prístup k samotnému FOSS (t. j. poskytovanie produktu s digitálnymi prvkami), vrátane jeho údržby podmienený odmenou, a nie len samotnou ponukou odborných služieb týkajúcich sa voľne dostupného produktu s digitálnymi prvkami, ako sa uvádza v odôvodnení 18 CRA („by sa poskytovanie produktov s digitálnymi prvkami považovanými za slobodný softvér a softvér s otvoreným zdrojovým kódom, ktoré ich výrobcovia nespĺňajú, nemalo považovať za obchodnú činnosť“). Ak je možné FOSS bezplatne stiahnuť a nainštalovať a používatelia si môžu voľiteľne zvoliť samostatný nákup odborných služieb, tento FOSS sa nepovažuje za uvedený na trh.
57. Naopak, v niektorých prípadoch je prístup ku konkrétnej verzii produktu s digitálnymi prvkami, vrátane určitých výhod, ako je technická pomoc alebo optimalizácia výkonu, podmienený odmenou. V takýchto prípadoch ide o speňažené poskytovanie produktu s digitálnymi prvkami v rámci obchodnej činnosti, a preto sa považuje za uvedenie na trh. Patrí sem aj situácia, keď je platená edícia alebo podniková verzia sprístupnená na základe obchodnej zmluvy, bez ohľadu na to, či je funkčne ekvivalentný softvér k dispozícii aj bezplatne na základe licencie na slobodný softvér a softvér s otvoreným zdrojovým kódom.

*Príklad 17: Fyzická alebo právnická osoba zverejňuje slobodný operačný systém s otvoreným zdrojovým kódom a ponúka platenú verziu tohto operačného systému, ktorá zahŕňa podporné služby, ako je technická pomoc alebo optimalizácia výkonu. Platená verzia operačného systému sa považuje za uvedenú na trh v rámci obchodnej činnosti.*

*Príklad 18: Fyzická alebo právnická osoba zverejňuje slobodný nástroj príkazového riadka s otvoreným zdrojovým kódom. Nástroj je voľne dostupný a ktokoľvek si ho môže stiahnuť a nainštalovať. Uvedená fyzická alebo právnická osoba samostatne ponúka odborné služby, ako sú voľiteľné poradenské služby zamerané na školenie používateľov a podporu pri inštalácii a používaní nástroja. Tento FOSS sa nepovažuje za uvedený na trh v zmysle CRA.*

58. Najmä v prípade fyzických osôb, ktoré zverejňujú FOSS, by ponuka technickej pomoci priamo spojená s prístupom k produktu s digitálnymi prvkami stále nespĺňala kritériá obchodnej činnosti, ak, ako sa uvádza v odôvodnení č. 15 CRA, účtovaná cena slúži iba na pokrytie skutočných nákladov. Medzi takéto skutočné náklady patria rôzne náklady súvisiace s návrhom, vývojom a údržbou daného softvéru, vrátane primeraných životných nákladov danej osoby. Preto sa fyzická osoba, ktorá zverejňuje FOSS a ponúka technickú pomoc s cieľom pokryť svoje náklady a získať primeranú odmenu, nesmie na základe tohto samotného faktu považovať za osobu uvádzajúcu tento softvér na trh EÚ.
59. Fyzická alebo právnická osoba, ktorá poskytuje technickú pomoc súvisiacu so softvérom FOSS, za ktorý nenesie zodpovednosť, sa nepovažuje za subjekt uvádzajúci tento softvér na trh, pokiaľ táto osoba v rámci poskytovania takejto pomoci podstatne

upraví softvér FOSS v súlade s článkom 22.

*Príklad 19: Poskytovateľ služieb nezverejňuje FOSS, ale pomáha zákazníkovi s jeho inštaláciou na lokálnom serveri zákazníka. Robí tak bez toho, aby vykonal podstatnú úpravu tohto FOSS. Poskytovateľ služieb sa preto nepovažuje za subjekt uvádzajúci FOSS na trh.*

### 3.2.4. Dary

60. Fyzické alebo právnické osoby, ktoré zverejňujú projekty FOSS, bežne poskytujú používateľom tohto softvéru možnosti dobrovoľne prispieť finančnou sumou, aby poďakovali vydavateľom projektu a zároveň zabezpečili, že projekt bude naďalej aktívne udržiavaný.
61. Ako sa uvádza v odôvodnení č. 15 CRA, „prijímanie darov bez úmyslu dosiahnuť zisk by sa nemalo považovať za obchodnú činnosť“. Samotná skutočnosť, že je zahrnutý odkaz na platformu na prijímanie darov alebo podobné nástroje na zbieranie darov, by sa nemala považovať za úmysel dosiahnuť zisk, a to ani v prípade, ak suma vyzbieraná prostredníctvom darov presahuje samotné náklady spojené s návrhom, vývojom a poskytovaním produktu s digitálnymi prvkami. To zahŕňa primeranú odmenu pre prispievateľov zamestnaných právnickou osobou a/alebo primerané životné náklady fyzickej osoby. Dary sa vzhľadom na svoju povahu v čase menia, a preto je potrebné pri posudzovaní, či sa FOSS speňažený výlučne prostredníctvom darov považuje za uvedený na trh, postupovať s určitou mierou flexibility. Je preto nepravdepodobné, že by sa FOSS podporovaný výlučne prostredníctvom darov považoval za uvedený na trh v zmysle CRA.

*Príklad 20: Fyzická alebo právnická osoba zverejní nástroj FOSS vo verejnom online repozitári, čím umožní komukoľvek stiahnuť, používať, upravovať a ďalej šíriť tento nástroj na základe bezplatnej a otvorenej licencie. Vydavateľ vyzýva používateľov, aby prostredníctvom darcovskej platformy poskytovali dobrovoľné dary na podporu ďalšieho vývoja a údržby projektu. Prístup k softvéru, jeho zdrojovému kódu a jeho aktualizáciám nie je podmienený poskytnutím daru. Tento FOSS sa nepovažuje za dodávaný v rámci obchodnej činnosti a nepovažuje sa za uvedený na trh v zmysle CRA.*

62. Existujú však prípady, keď sa FOSS podporovaný prostredníctvom darov môže považovať za uvedený na trh. Ide o prípady, keď na základe celkového posúdenia okolností sú dary de facto rovnocenné s účtovaním ceny za prístup k produktu s digitálnymi prvkami alebo k niektorým jeho funkcionalitám. Môže to platiť najmä vtedy, ak je prístup k FOSS, k základným funkcionalitám alebo k aktualizáciám v praxi podmienený poskytnutím daru, alebo ak sú dary spojené so zmluvnými výhodami alebo exkluzívnymi výhodami, ktoré presahujú výhody pre komunitu.

*Príklad 21: Fyzická alebo právnická osoba uverejňuje softvérový produkt s digitálnymi prvkami na základe licencie na slobodný softvér a softvér s otvoreným zdrojovým kódom, ale poskytuje verzie na stiahnutie a bezpečnostné aktualizácie iba používateľom, ktorí poskytnú dar. Používatelia, ktorí dar neposkytnú, nemajú prístup k aktuálnej verzii softvéru.*

*V tomto prípade sú dary de facto podmienkou prístupu k produktu s digitálnymi*

prvkami, a preto sa rovnajú účtovaniu ceny. Tento FOSS sa preto považuje za uvedený na trh v zmysle CRA.

*Príklad 22: Fyzická alebo právnická osoba sprístupňuje zdrojový kód FOSS verejnosti, ale poskytuje vopred skompilované binárne súbory, pravidelné aktualizácie a zaručené bezpečnostné opravy len darcom. V tomto prípade sú dary spojené s prístupom k podstatným aspektom produktu s digitálnymi prvkami a predstavujú odmenu za dodanie tohto produktu. Tento FOSS sa preto považuje za uvedený na trh v rámci obchodnej činnosti.*

### 3.2.5. Financovanie slobodného softvéru a softvéru s otvoreným zdrojovým kódom

63. Samotná skutočnosť, že tretia strana zaplatila za vývoj FOSS, sponzorovala ho alebo inak financovala, sama o sebe neurčuje, či je tento FOSS uvedený na trh. V ekosystéme FOSS je bežnou praxou, že samostatní vývojári, nadácie alebo komunity dostávajú finančné prostriedky od spoločností, verejných orgánov alebo iných sponzorov s cieľom pracovať na konkrétnych prvkoch, odstraňovať chyby alebo udržiavať kritické komponenty. Toto financovanie môže mať mnoho foriem, vrátane grantov, odmien za nájdenie chýb, sponzorstva, zmlúv o poskytovaní služieb alebo platených vývojárskych prác.
64. Ako už bolo pripomenuté, v odôvodnení č. 18 CRA sa objasňuje, že samotné okolnosti, za ktorých bol produkt s digitálnymi prvkami vyvinutý, alebo spôsob financovania tohto vývoja, by sa nemali zohľadňovať pri určovaní obchodného charakteru danej činnosti.
65. Preto v prípade, že je FOSS otvorene zdieľaný a voľne dostupný pre všetkých na prístup, používanie, úpravy a ďalšie šírenie, skutočnosť, že komerčný subjekt mohol za tento projekt zaplatiť, by nemala prispievať k určovaniu, či je tento softvér uvedený na trh. V skutočnosti, ak sa tento FOSS inak nespeňažuje, nemal by sa považovať za uvedený na trh. Ak spoločnosť, ktorá financovala vývoj FOSS (rovnako ako akákoľvek iná spoločnosť), integruje tento FOSS do svojho produktu s digitálnymi prvkami, táto spoločnosť je povinná postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5 CRA.

*Príklad 23: Samostatný vývojár zverejní projekt FOSS a aktívne ho udržiava. Výrobca A požiada samostatného vývojára, aby do daného FOSS pridal konkrétny prvok, a tento vývoj financuje. Vývojár pridá tento prvok do zdrojového kódu FOSS, otvorene ju zdieľa a sprístupňuje ju všetkým na prístup, používanie, úpravy a ďalšie šírenie. Nepovažuje sa, že by tento samostatný vývojár uviedol daný FOSS na trh. Ak výrobca integruje FOSS do svojho produktu s digitálnymi prvkami, musí vykonať náležitú starostlivosť v súlade s článkom 13 ods. 5.*

### 3.2.6. Neziskové subjekty zriadené na dosiahnutie neziskových cieľov

66. Ak je právnická osoba, ktorá zverejňuje FOSS, nezisková organizácia „zriadená tak, aby sa zabezpečilo, že všetky príjmy po odpočítaní nákladov sa použijú na dosiahnutie neziskových cieľov“ (odôvodnenie 18 CRA), FOSS, ktoré zverejňuje, sa nepovažuje za uvedený na trh. Ak táto právnická osoba spĺňa definíciu „správcu“, podlieha príslušným

povinnosti (článok 24 CRA).

*Príklad 24: Právnická osoba zverejňuje slobodný prehliadač s otvoreným zdrojovým kódom, ktorý je priamo speňažovaný prostredníctvom partnerstiev s vyhľadávačmi, avšak všetky jej výnosy po odpočítaní nákladov sa používajú na neziskové ciele. Prehliadač sa nepovažuje za uvedený na trh v zmysle CRA. Právnická osoba, ktorá ho zverejňuje, podlieha povinnostiam platným pre správcov.*

### 3.2.7. Integrácia inými výrobcami

67. V niektorých prípadoch je FOSS uverejnený jasne identifikovateľnou fyzickou alebo právnickou osobou, ale tento FOSS je „určený na integráciu inými výrobcami do ich vlastných produktov s digitálnymi prvkami“. V takýchto prípadoch sa tento FOSS nepovažuje za uvedený na trh EÚ, pokiaľ ho nespeňažuje aj osoba, ktorá ho uverejňuje (t. j. pôvodný výrobca), v súlade s predchádzajúcimi časťami týchto usmernení.
68. Ak sa tento FOSS neuvádza na trh, právnická osoba, ktorá ho zverejňuje, by podliehala povinnostiam správcov, ak poskytuje podporu na trvalej báze v súlade s definíciou pojmu „správca“.

*Príklad 25: Právnická osoba zverejňuje knižnicu FOSS na vytváranie používateľských rozhraní. Poskytovanie tejto knižnice nespeňažuje, ale integruje ju do jedného zo svojich produktov s digitálnymi prvkami (ktorý je následne uvedený na trh). Knižnica sa nepovažuje za uvedenú na trh v zmysle CRA, je však určená na integráciu do produktov s digitálnymi prvkami. Právnická osoba, ktorá ju zverejňuje, je jej správcou.*

*Príklad 26: Právnická osoba uvádza na trh operačný systém a zároveň zverejňuje knižnicu FOSS, ktoré slúžia ako referenčné implementácie pre používateľov tohto operačného systému. Právnická osoba nespeňažuje knižnicu FOSS, ktoré sú určené na integráciu do iných produktov s digitálnymi prvkami. Právnická osoba, ktorá ich zverejňuje, je správcou týchto knižníc FOSS.*

### 3.3. Správcovia softvéru s otvoreným zdrojovým kódom

69. CRA zavádza novú právnu kategóriu „správcu softvéru s otvoreným zdrojovým kódom „vzhľadom na význam mnohých produktov s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, pre kybernetickú bezpečnosť, ktoré sa zverejňujú, ale nesprístupňujú na trhu v zmysle [CRA]“ (odôvodnenie 19 CRA).
70. V niektorých prípadoch je FOSS uverejnený, ale nie je sprístupnený na trhu v zmysle CRA právnickou osobou, ktorej „účelom alebo cieľom je systematicky a trvalo podporovať vývoj [FOSS] [...] určených na obchodné činnosti, a ktorá zabezpečuje životaschopnosť týchto produktov“ (článok 3 ods. 14 CRA). V takýchto prípadoch sa na túto právnickú osobu vzťahujú povinnosti správcov.
71. Správca je definovaný ako „právnická osoba, ktorá nie je výrobcom“, pretože výrobca je podľa definície fyzická alebo právnická osoba, ktorá uvádza produkty s digitálnymi prvkami na trh („uvádza ich na trh“) pod vlastným menom alebo ochrannou známkou. Právnická osoba môže byť správcou iba v prípade produktov s digitálnymi prvkami, ktoré spĺňajú podmienky FOSS a ktoré sú uverejnené, ale nie sú sprístupnené na trhu

v zmysle CRA. Pojem správca sa preto vzťahuje na konkrétne prípady FOSS, ktoré „sú v konečnom dôsledku určený na obchodné činnosti, napríklad na integráciu do komerčných služieb alebo do speňažovaných produktov s digitálnymi prvkami.“ (odôvodnenie 19 CRA<sup>13</sup>), ale nie sú sprístupnené na trhu v zmysle CRA, a pre ktoré právnická osoba zverejňujúca daný FOSS zabezpečuje systematickú podporu.

72. Skutočnosť, že právnická osoba je správcom jedného konkrétneho FOSS, neznamená, že je nevyhnutne správcom aj iných FOSS, ktoré zverejňuje. Podobne skutočnosť, že právnická osoba je výrobcom jedného konkrétneho FOSS, neznamená, že nemôže byť správcom iných FOSS. To zahŕňa aj poskytovanie „komunitných“ verzií toho istého FOSS, ako je opísané v oddiele 3.2.1 *Stanovenie ceny*.
73. Právnická osoba môže teda byť súčasne správcom jedného konkrétneho FOSS (pričom správca systematicky poskytuje podporu na trvalej báze a zabezpečuje životaschopnosť softvéru) a výrobcom iného konkrétneho FOSS (pričom ho uvádza na trh). Inými slovami, od tej istej právnickej osoby sa môže vyžadovať, aby plnila rôzne úlohy v rámci rôznych projektov FOSS.
74. Pre každý konkrétny FOSS, ktorý zverejňuje, bude právnická osoba musieť zistiť, či sa tento FOSS považuje za uvedený na trh v zmysle CRA. Ak áno, stáva sa táto právnická osoba výrobcom daného softvéru. Ak sa FOSS nepovažuje za uvedený na trh, právnická osoba môže byť jeho správcom, ak je softvér určený na obchodné účely a ak ho právnická osoba udržiava v súlade s definíciou správcu<sup>14</sup>.

### 3.3.1. Trvalá podpora a zabezpečenie životaschopnosti FOSS

75. V odôvodnení č. 19 sa vysvetľuje, že poskytovanie trvalej podpory vývoju produktu s digitálnymi prvkami môže zahŕňať (okrem iného):
  - i) hosting a riadenie platforiem spolupráce pri vývoji softvéru;
  - ii) hosting zdrojového kódu alebo softvéru;
  - iii) správu alebo riadenie produktov s digitálnymi prvkami, ktoré sa považujú za FOSS;
  - iv) riadenie vývoja takýchto produktov s digitálnymi prvkami.
76. To môže byť napríklad prípad právnickej osoby, ktorá vyvíja FOSS na integráciu do svojich vlastných produktov s digitálnymi prvkami a následne ho zverejňuje bez toho, aby ho uvádzala na trh. Táto otázka je rozoberaná aj v časti 3.2.7 *Integrácia inými výrobcami*. V tomto prípade nie je právnická osoba výrobcom softvéru, ale môže byť jeho správcom. Okrem toho, ako bolo vysvetlené aj v predchádzajúcich častiach, právnická osoba, ktorá zverejňuje bezplatnú (alebo komunitnú) verziu a speňažovanú verziu toho istého FOSS, sa považuje za správcu bezplatnej (alebo komunitnej) verzie a za výrobcu speňažovanej verzie.
77. Podobne je právnická osoba, ktorá speňažuje FOSS, ale je neziskovou organizáciou, ktorej výnosy po odpočítaní nákladov sa používajú na dosiahnutie neziskových cieľov

<sup>13</sup> Tento pojem je obsiahnutý aj vo formulácii „určený na obchodné účely“, ktorá je súčasťou definície pojmu „správca softvéru s otvoreným zdrojovým kódom“ uvedenej v článku 3 ods. 14 CRA.

<sup>14</sup> Právnická osoba tiež nemusí podliehať žiadnym povinnostiam podľa CRA v prípadoch, keď: (i) konkrétny FOSS nie je uvedený na trh v zmysle CRA; a (ii) právnická osoba nespĺňa definíciu správcu v súvislosti s týmto konkrétnym FOSS.

(a preto sa jej FOSS neuvádza na trh v zmysle CRA, ako sa uvádza v oddiele 3.2.6 *Neziskové organizácie*), správcom FOSS, ktorý zverejňuje.

78. Okrem toho niektoré nadácie ponúkajú platformy pre spoluprácu s rôznymi formami riadenia, ktoré výrobcami umožňujú pravidelne prispievať k vývoju FOSS a/alebo ktoré sú pravidelne financované výrobcami. Takéto nadácie sa majú považovať za správcov v súvislosti s konkrétnym FOSS, ktorý je určený na obchodné činnosti a pre ktorý nadácia poskytuje trvalú podporu. Ako sa však vysvetľuje v oddiele 3.3 „*Správcovia softvéru s otvoreným zdrojovým kódom*“, takáto nadácia nemusí podliehať žiadnym povinnostiam podľa CRA v súvislosti s iným konkrétnym FOSS, ktorý hostuje, a to v prípadoch, keď neposkytuje systematickú podporu pre konkrétny FOSS, nezabezpečuje jeho životaschopnosť a/alebo ak tento konkrétny softvér nie je určený na obchodné činnosti.
79. Druh „trvalej podpory“, ktorú nadácie a podobné organizácie poskytujú konkrétnym projektom FOSS, sa môže výrazne líšiť. Niektoré právnické osoby napríklad poskytujú iba netechnickú podporu, ako je správa značky projektov, stanovenie pravidiel riadenia, organizovanie komunitných podujatí alebo zbieranie darov. Iné subjekty poskytujú aj základnú IT infraštruktúru potrebnú na prevádzku projektu, napríklad hosting repozitárov zdrojového kódu, poskytovanie systémov na správu verzií alebo generovanie podpisových kľúčov. Ďalšie subjekty idú vo forme poskytovanej podpory ešte ďalej a aktívne prispievajú k projektu technickými zdrojmi, napríklad zamestnávaním vývojárov, koordináciou vývojových prác, preskúmaním alebo zlučovaním kódu, riadením vydávania nových verzií alebo vybavovaním hlásení o zraniteľnostiach a bezpečnostných záplat. Hoci všetky právnické osoby, ktoré spĺňajú podmienky na to, aby boli považované za správcov podľa CRA, sú povinné dodržiavať povinnosti uvedené v článku 24 ods. 1 a 2, rozsah, v akom sa na tieto právnické osoby vzťahujú povinnosti stanovené v článku 14 ods. 1, odsekoch 3 a 8 vzťahujú na tieto právnické osoby, závisí od druhu podpory, ktorú poskytujú, v súlade s článkom 24 ods. 3.
80. Napríklad správca, ktorý poskytuje iba netechnickú podporu, sa podľa definície nezúčastňuje na vývoji produktu s digitálnymi prvkami, a preto nie je povinný hlásiť aktívne zneužívané zraniteľnosti. Takýto správca tiež neposkytuje žiadne sieťové a informačné systémy na vývoj takýchto produktov s digitálnymi prvkami, a preto nie je povinný hlásiť závažné incidenty agentúre ENISA a tímom CSIRT ani postihnutým používateľom. Ak sa však správca dozvie o aktívne zneužívanej zraniteľnosti (napr. prostredníctvom hlásenia z externých zdrojov, ako sú výskumní pracovníci), mal by túto informáciu zdieľať so správcami produktu s digitálnymi prvkami v súlade so svojou politikou kybernetickej bezpečnosti. Udržovatelia produktov s digitálnymi prvkami a/alebo udržiavatelia by mali tiež zvážiť dobrovoľné nahlásenie tohto zraniteľného miesta v súlade s článkom 15.
81. Na druhej strane, ak správca poskytuje základnú IT infraštruktúru pre určité produkty s digitálnymi prvkami, je povinný v súlade s článkom 14 ods. 3 oznámiť agentúre ENISA a CSIRT akékoľvek závažné incidenty súvisiace s touto infraštruktúrou, ktoré majú vplyv na bezpečnosť produktov s digitálnymi prvkami. V prípade potreby je tiež povinný informovať všetkých používateľov (napr. prostredníctvom všeobecného oznámenia).

Ako bolo uvedené v predchádzajúcom bode, hoci správca nie je povinný hlásiť aktívne zneužívané zraniteľnosti, o ktorých sa dozvie, mal by podporovať správne zaobchádzanie so zraniteľnosťami a mal by zvážiť dobrovoľné hlásenie v súlade s článkom 15.

82. Nakoniec, ak správca poskytuje aj technické zdroje pre konkrétne produkty s digitálnymi prvkami, je povinný:
  - i) v súlade s článkom 14 ods. 1 oznámiť aktívne zneužívané zraniteľnosti, o ktorých sa dozvie;
  - ii) v prípade potreby informovať všetkých používateľov. V rozsahu, v akom má správca aj priamy vzťah s dotknutými používateľmi, je povinný informovať ich priamo v súlade s článkom 14 ods. 8.
83. Ak subjekt prestane poskytovať systematickú podporu na trvalej báze pre konkrétny FOSS, môže prestať spĺňať definíciu správcu a preto už nemusí podliehať príslušným povinnostiam. V takýchto prípadoch sa tomuto subjektu odporúča jasne oznámiť zmenu svojho statusu v súvislosti s týmto konkrétnym FOSS.
84. V určitých situáciách sa subjekt, ktorý bol správcom konkrétneho projektu, môže rozhodnúť tento projekt priamo speňažiť, čím uvedie produkt s digitálnymi prvkami na trh a vznikajú mu tým povinnosti výrobcu podľa CRA. Za takýchto okolností sa tento subjekt kvalifikuje ako výrobca produktu s digitálnymi prvkami odo dňa, keď ho uvedie na trh (nie však v súvislosti s predchádzajúcimi verziami, pri ktorých pôsobil ako správca).

### 3.4. Prispievatelia a následné využitie

85. Ako už bolo spomenuté v časti 3.1 *Určenie, či je slobodný softvér a softvér s otvoreným zdrojovým kódom* v zodpovednosti daného subjektu, CRA objasňuje, že sa nevzťahuje „a fyzické alebo právnické osoby, ktoré prispievajú zdrojovým kódom k produktu s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, za ktoré nenesú zodpovednosť“ (odôvodnenie 18).
86. Výrobcovia produktov s digitálnymi prvkami, ktorí integrujú komponenty FOSS do svojich vlastných produktov s digitálnymi prvkami, sa tiež nestávajú zodpovednými za individuálnu zhodu týchto komponentov s CRA, a to ani v prípade, ak výrobcovia prispievajú zdrojovým kódom k ich údržbe.
87. Podobne samotná skutočnosť, že výrobcovia integrujú komponenty FOSS do svojich vlastných (speňažovaných) produktov s digitálnymi prvkami, nemá žiadny vplyv na daný status komponentu FOSS podľa CRA. Správcovia komponentov FOSS, ktoré nie sú uvedené na trh, nemajú žiadne povinnosti voči iným subjektom, ktoré môžu takéto komponenty integrovať do svojich produktov s digitálnymi prvkami. To, či sa CRA vzťahuje na daný FOSS, závisí výlučne od toho, či ju fyzická alebo právnická osoba, ktorá ju zverejňuje, uvádza na trh.
88. Výrobcovia produktov s digitálnymi prvkami, ktorí integrujú komponenty FOSS, sú však povinní dodržiavať CRA v súvislosti so svojimi vlastnými produktmi s digitálnymi prvkami. V súlade s článkom 13 ods. 5 majú tiež povinnosť náležitej starostlivosti vo vzťahu ku komponentom FOSS, ktoré integrujú. Okrem toho sú povinní hlásiť

zraniteľnosti v integrovaných komponentoch a zdieľať bezpečnostné opravy v súlade s článkom 13 ods. 6. Ďalšie usmernenia k tejto téme nájdete v časti 9.2.1 Hlásenie vývojárom a zdieľanie bezpečnostných opráv.

### 3.5. Ilustratívne scenáre

89. Nižšie uvedené príklady sú čisto hypotetické a slúžia iba na ilustráciu rôznych prípadov, ako je vysvetlené v predchádzajúcich častiach.

*Príklad 27: Samostatný vývojár A vyvinul FOSS. Vývojár A tento FOSS uverejňuje pod svojím vlastným menom alebo ochrannou známkou, ale za jeho používanie neúčtuje žiadnu cenu. Softvér je otvorene zdieľaný a voľne dostupný pre všetkých na prístup, používanie, úpravy a ďalšie šírenie. Vývojár A tiež uvádza odkaz na platformu na zbieranie dobrovoľných darov.*

*Spoločnosti B, C a D integrujú tento FOSS do svojich vlastných produktov s digitálnymi prvkami. Na podporu priebežnej údržby poskytujú spoločnosti B, C a D vývojárovi A dobrovoľné príspevky. Tieto príspevky umožňujú vývojárovi A aktívne udržiavať projekt.*

*Tento FOSS nie je uvádzaný na trh v zmysle CRA. Vývojár A nemá podľa CRA žiadne povinnosti. Spoločnosti B, C a D sú povinné postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5 pri integrácii tohto FOSS do svojich vlastných produktov s digitálnymi prvkami.*

*Príklad 28: Nezisková nadácia F zverejňuje komponent FOSS na integráciu do iných komerčných produktov s digitálnymi prvkami. Nadácia F sa zaväzuje poskytovať tomuto FOSS trvalú podporu s cieľom zabezpečiť jeho životaschopnosť a prijatie. Spoločnosti A, B a C integrujú tento FOSS do svojich vlastných produktov s digitálnymi prvkami. Spoločnosti A a B dobrovoľne prispievajú časom niektorých svojich vývojárov na vývoj a údržbu projektov FOSS v rámci nadácie F, vrátane tohto FOSS.*

*Keďže nadácia F je neziskový subjekt zriadený tak, že jej výnosy po odpočítaní nákladov sa používajú na dosiahnutie neziskových cieľov, tento FOSS sa nepovažuje za uvedený na trh v zmysle CRA. Nadácia F je správcou FOSS a podlieha príslušným povinnostiam stanoveným v článku 24. Spoločnosti A, B a C sú povinné postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5 pri integrácii tohto FOSS do svojich vlastných produktov s digitálnymi prvkami.*

*Príklad 29: Spoločnosť A vyvinula komponent FOSS na integráciu do svojich vlastných produktov s digitálnymi prvkami. Tento FOSS tiež samostatne zverejňuje pod svojím vlastným názvom alebo ochrannou známkou a aktívne ho udržiava. Za jeho používanie však neúčtuje poplatky ani ho iným spôsobom nespeňažuje. Spoločnosti B, C a D integrujú tento FOSS do svojich vlastných produktov s digitálnymi prvkami a dobrovoľne venujú čas niektorých svojich vývojárov na jeho údržbu.*

*Tento FOSS sa nepovažuje za uvedený na trh v zmysle CRA. Spoločnosť A nie je jeho výrobcom, ale je jeho správcou. Spoločnosti B, C a D sú povinné pri integrácii FOSS do svojich vlastných produktov s digitálnymi prvkami postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.*

*Príklad 30: Spoločnosť A uverejňuje FOSS pod svojím vlastným názvom alebo ochrannou*

známkou a ponúka ho ako platenú verziu, ktorá zahŕňa určité výhody, ako je technická podpora alebo optimalizácia výkonu. Vývojári zo spoločností B, C a D prispievajú k údržbe tohto FOSS, ten však zostáva pod kontrolou spoločnosti A.

Spoločnosť A sa v súvislosti s týmto FOSS považuje za výrobcu<sup>15</sup>. Spoločnosti B, C a D nepodliehajú povinnostiam vyplývajúcim z CRA v súvislosti s týmto konkrétnym FOSS. Ak tento FOSS integrujú do svojich vlastných produktov s digitálnymi prvkami, sú povinné postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

*Príklad 31:* Spoločnosť A zverejňuje FOSS pod svojím vlastným názvom alebo ochrannou známkou a zabezpečuje jeho priebežnú údržbu s cieľom zabezpečiť jeho dlhodobú životaschopnosť, aby bolo možné tento softvér integrovať do produktov iných spoločností obsahujúcich digitálne prvky. Spoločnosť A neučtuje poplatky za jeho používanie, nespracúva osobné údaje, ktoré zhromažďuje prostredníctvom produktu obsahujúceho digitálne prvky, ani nepredáva podporné služby súvisiace so zverejnením FOSS.

Spoločnosť B prispieva kúskom kódu a časom vývojárov na údržbu daného FOSS, ale tento softvér komerčne nedistribuuje. Spoločnosť B ponúka služby technickej podpory nezávisle od distribúcie daného FOSS. Spoločnosť A sa považuje za správcu daného FOSS, zatiaľ čo spoločnosť B nemá voči tomuto FOSS žiadne povinnosti podľa CRA.

*Príklad 32:* Komponent FOSS zverejňuje neziskový subjekt zriadený tak, aby zabezpečil, že všetky výnosy po odpočítaní nákladov sa použijú na dosiahnutie neziskových cieľov. Tento subjekt poskytuje trvalú podporu s cieľom zabezpečiť dlhodobú životaschopnosť projektu. Údržba je financovaná z verejných zdrojov, napríklad z výskumných grantov. Ďalší vývoj, vrátane nových prvkov, je financovaný z darov a v rámci konkrétnych projektov realizovaných v partnerstve s výrobcami, ktorí tento FOSS integrujú do svojich produktov s digitálnymi prvkami. Takéto prvky sú začlenené do zdrojového kódu FOSS. Nezisková organizácia, ktorá uverejňuje FOSS, sa považuje za správcu daného komponentu FOSS. Výrobca, ktorý prispel k vývoju určitých prvkov, sa nestáva výrobcom daného komponentu FOSS. Ak výrobca integruje daný komponent FOSS do svojho vlastného produktu s digitálnymi prvkami, musí postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

*Príklad 33:* Nezisková organizácia zriadená tak, aby zabezpečila, že všetky výnosy po odpočítaní nákladov sa použijú na dosiahnutie neziskových cieľov, zverejňuje sadu na vývoj softvéru (SDK) FOSS a zabezpečuje jej priebežnú údržbu. Sada SDK je verejne zdieľaná a je voľne dostupná pre všetkých na prístup, používanie, úpravy a ďalšie šírenie. Financovanie sa zabezpečuje prostredníctvom členských príspevkov vyplácaných neziskovému subjektu a vývojári zamestnaní členskými organizáciami prispievajú kódom a ďalšími zdrojmi k vývoju SDK. Výrobcovia používajú SDK ako komponent na vytváranie iných produktov s digitálnymi prvkami.

Nezisková organizácia, ktorá túto sadu SDK zverejňuje, je jej správcou. Členovia nadácie nie sú zodpovední za súlad sady SDK s CRA. Ak výrobcovia používajú sadu SDK na výrobu svojich vlastných produktov s digitálnymi prvkami, musia postupovať

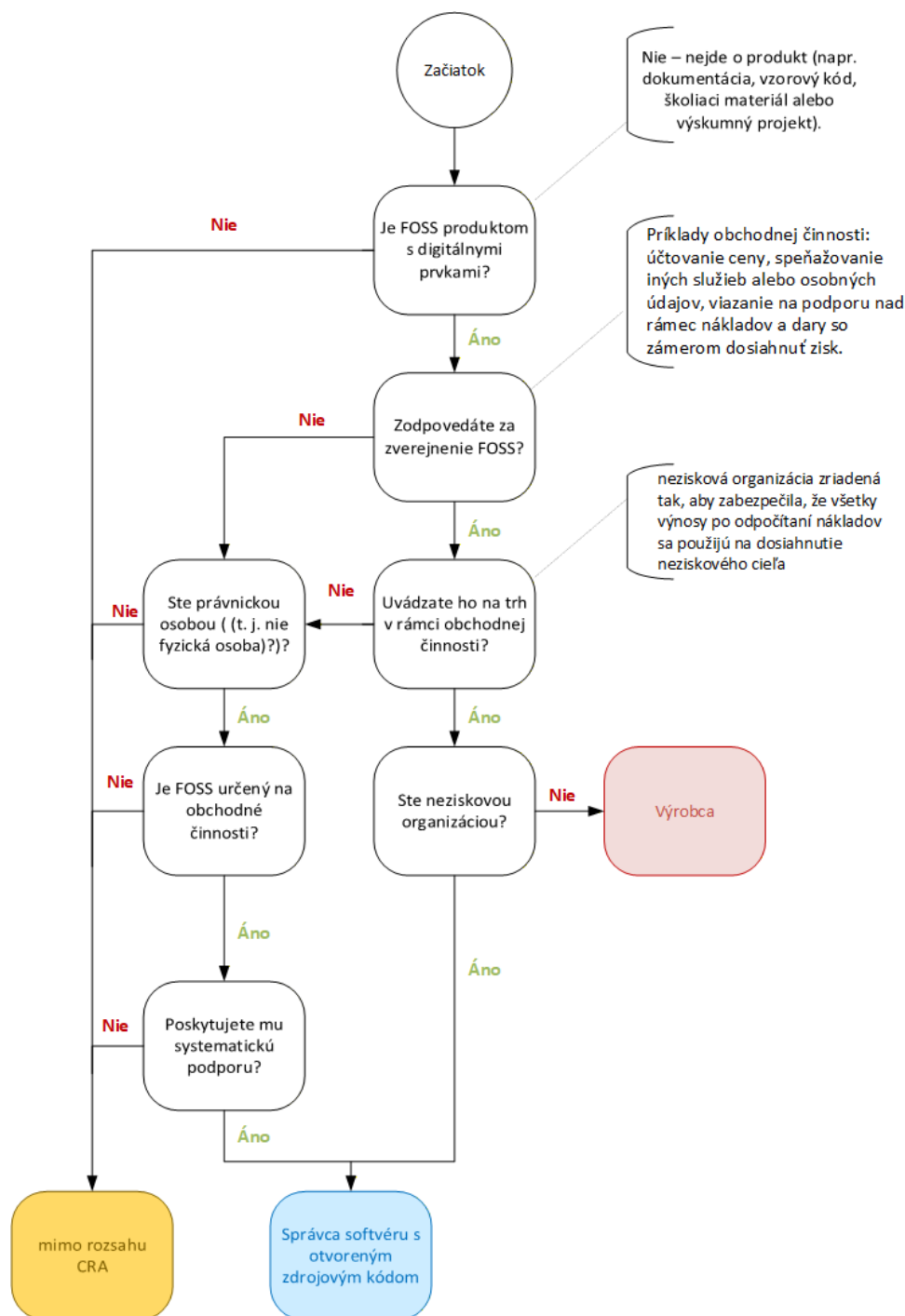
---

<sup>15</sup> Pokiaľ spoločnosť A nie je neziskovou organizáciou zriadenou tak, aby zabezpečovala, že všetky výnosy po odpočítaní nákladov sa použijú na dosiahnutie neziskových cieľov; v takom prípade by bola správcou daného FOSS.

s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

*Príklad 34: Samostatný vývojár zverejní knižnicu FOSS vo verejnom repozitári balíkov pre daný programovací jazyk a aktívne ju udržiava. Do dokumentácie balíka vývojár pridá odkaz na zbierku darov. Výrobca si túto knižnicu bezplatne stiahne z repozitára a integruje ju do svojho vlastného produktu s digitálnymi prvkami.*

*Samostatný vývojár ani repozitár balíkov nemajú podľa CRA žiadne povinnosti. Výrobca, ktorý knižnicu integruje, musí postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.*



Obrázok 1: Zjednodušený diagram uplatňovania CRA na slobodný softvér a softvér s otvoreným zdrojovým kódom

## 4. Podstatné úpravy a náhradné diely

90. Článok 3 ods. 30 CRA definuje „podstatnú úpravu“ ako zmenu produktu s digitálnymi prvkami po jeho uvedení na trh, ktorá:
91. ovplyvňuje súlad produktu s digitálnymi prvkami so základnými požiadavkami stanovenými v časti I prílohy I; alebo ktorá
- a. vedie k úprave zamýšľaného účelu, pre ktorý bol produkt s digitálnymi prvkami posudzovaný.
  - b. Pojem podstatnej úpravy je relevantný pre stanovenie povinností podľa CRA v mnohých prípadoch, vrátane týchto:
  - c. v súlade s článkom 21 sa dovozca alebo distribútor, ktorý vykoná podstatnú úpravu produktu s digitálnymi prvkami, ktorý je už uvedený na trh, považuje za jeho výrobcu;
  - d. v súlade s článkom 22 sa za výrobcu považuje akákoľvek fyzická alebo právnická osoba, ktorá vykoná podstatnú úpravu produktu s digitálnymi prvkami a uvedie ho na trh;
  - e. v súlade s článkom 69 ods. 2 sa za výrobcu považuje akákoľvek fyzická alebo právnická osoba, ktorá po 11. decembri 2027 vykoná podstatnú úpravu produktu s digitálnymi prvkami uvedeného na trh pred 11. decembrom 2027 a tento produkt uvedie na trh;
  - f. pre výrobcov produktov s digitálnymi prvkami uvedených na trh po 11. decembri 2027, s cieľom určiť, či produkt s digitálnymi prvkami musí prejsť novým postupom posudzovania zhody v dôsledku zmien vykonaných po tomto dátume, najmä vzhľadom na iteratívny charakter vývoja softvéru.
92. Preto je dôležité poskytnúť usmernenia, ktoré pomôžu hospodárskym subjektom pochopiť, kedy sa úpravy hardvéru alebo softvéru považujú za podstatné úpravy.

### 4.1. Fyzické opravy

93. Ako sa uvádza v odôvodnení 42 CRA, „ak produkt s digitálnymi prvkami podlieha „renovovaniu“, „údržbe“ a „oprave“ v zmysle vymedzenia v článku 2 bodoch 18, 19 a 20 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1781, nemusí to nevyhnutne viesť k podstatnej úprave produktu, napríklad ak sa zamýšľaný účel a funkcie nezmenia a neovplyvnená zostane aj úroveň rizika. Modernizácia produktu s digitálnymi prvkami výrobcom by mohla viesť k zmenám v návrhu a vývoji tohto produktu, a preto by mohla mať vplyv na jeho zamýšľaný účel a súlad s požiadavkami stanovenými v tomto nariadení“. Toto je v súlade s oddielom 2.1 Modrej príručky, v ktorej sa pripomína, že „produkt, ktorý prešiel významnými zmenami alebo generálnou opravou po uvedení do prevádzky, sa musí považovať za nový produkt, ak:
- i) došlo k úprave jeho pôvodnej výkonnosti, účelu alebo typu, pričom táto zmena nebola predpokladaná v pôvodnom posúdení rizika;
  - ii) zmenila sa povaha nebezpečenstva alebo sa zvýšila úroveň rizika vo vzťahu k príslušným harmonizačným právnym predpisom Únie; a
  - iii) produkt je sprístupnený na trhu (alebo uvedený do prevádzky, ak príslušné právne predpisy zahŕňajú do svojej pôsobnosti aj uvedenie do prevádzky).

Toto sa musí posudzovať individuálne v každom jednotlivom prípade, a to najmä s ohľadom na cieľ právnych predpisov a typ produktov, na ktoré sa dané právne predpisy vzťahujú“.

94. Úkony renovácie, údržby alebo opravy, ktoré vedú k fyzickým úpravám produktov s digitálnymi prvkami, ktoré už boli uvedené na trh, nemusia nevyhnutne predstavovať podstatné úpravy. Preto by sa malo vykonať posúdenie v jednotlivých prípadoch s cieľom zistiť, či takáto fyzická úprava ovplyvňuje súlad produktu s digitálnymi prvkami so základnými požiadavkami časti I prílohy I, alebo či vedie k zmene zamýšľaného účelu produktu, na ktorý sa vzťahuje posúdenie kybernetickobezpečnostného rizika.
95. Výmena chybných alebo opotrebovaných dielov za diely s lepšími vlastnosťami (napr. v dôsledku technického pokroku alebo preto, že starý diel sa už nevyrába) sama osebe nespôsobuje podstatnú úpravu opraveného produktu s digitálnymi prvkami. K tomu dochádza len vtedy, ak zmena výkonu alebo spôsobu fungovania opraveného produktu s digitálnymi prvkami:
- i) ovplyvňuje jeho súlad so základnými požiadavkami alebo
  - ii) vedie k zmene zamýšľaného účelu, ktorá nebola zahrnutá v posúdení rizika.

*Príklad 35: Výrobca počítačového servera vykoná opravu, pri ktorej vymení chybnú pamäť RAM za novú s lepším výkonom. Zhoda servera so základnými požiadavkami nie je ovplyvnená. Server má lepší výkon, ale jeho nový výkon zostáva v rámci zamýšľaného použitia servera, ako bolo zohľadnené v posúdení kybernetickobezpečnostných rizík. Počítačový server sa nepovažuje za podstatne upravený.*

## 4.2. Náhradné diely

96. V článku 2 ods. 6 CRA sa stanovuje, že náhradné diely určené na výmenu identických komponentov a vyrobené podľa rovnakých špecifikácií ako tieto komponenty nepodliehajú CRA. V odôvodnení 29 sa ďalej uvádza, že výnimka sa vzťahuje jednak na náhradné diely pre produkty s digitálnymi prvkami, ktoré boli uvedené na trh pred začatím uplatňovania CRA, a jednak na náhradné diely, ktoré už prešli postupom posudzovania zhody stanoveným v nariadení.
97. Výnimku uvedenú v článku 2 ods. 6 CRA treba chápať tak, že sa uplatňuje len vtedy, ak sa náhradný diel dodáva výlučne na účely opravy alebo predĺženia životnosti produktu s digitálnymi prvkami, ktorý bol už uvedený na trh (pred alebo po 11. decembri 2027). Ak sa produkt s digitálnymi prvkami dodáva ako samostatný produkt bez akejkoľvek súvislosti s údržbou alebo opravou už existujúceho produktu s digitálnymi prvkami, uvádza sa na trh v zmysle CRA a nemal by sa považovať za náhradný diel spadajúci do pôsobnosti článku 2 ods. 6. Účel údržby alebo opravy by mal byť zrejmý z kontextu dodávky, napríklad prostredníctvom identifikácie produktu s digitálnymi prvkami alebo skupiny produktov v objednávke alebo obchodnej ponuke, alebo prostredníctvom dodávky cez popredajné alebo servisné kanály. Podporné dôkazy v tomto zmysle by mali byť k dispozícii aj orgánom dohľadu nad trhom. Skutočnosť, že produkt s digitálnymi prvkami by sa z technického hľadiska mohol použiť na výmenu súčiastky, sama osebe nestačí na to, aby sa naň vzťahovala výnimka v prípade, že takéto prvky chýbajú.

98. Preto ak je náhradný diel identický so súčiastkou, ktorá je už súčasťou produktu s digitálnymi prvkami, ktorý bol uvedený na trh buď pred dátumom začatia uplatňovania CRA, alebo ktorý bol uvedený na trh v súlade s CRA, tento náhradný diel sám o sebe nepodlieha CRA.
99. Pri posudzovaní, či by sa náhradný diel mal považovať za identický so súčiastkou, by sa pozornosť mala zamerať na jeho funkčnú úlohu v produkte s digitálnymi prvkami a na vlastnosti, ktoré môžu byť relevantné pre kybernetickú bezpečnosť. Hoci je vždy potrebné posúdenie v jednotlivých prípadoch, rozdiely, ktoré neovplyvňujú bezpečnostné vlastnosti ani profil kybernetickobezpečnostného rizika súčiastky, samy osebe nebránia tomu, aby sa na tento náhradný diel vzťahoval článok 2 ods. 6 CRA.
100. Naopak, rozdiely vo vlastnostiach relevantných pre kybernetickú bezpečnosť komponentu, ako sú algoritmy, protokoly, kryptografické mechanizmy, prvky kontroly prístupu alebo iné vlastnosti súvisiace s bezpečnosťou, môžu znamenať, že nový diel nemožno považovať za identický s komponentom, ktorý má nahradiť.
101. Ak náhradná súčiastka nie je identická s pôvodnou súčiastkou, táto náhradná súčiastka predstavuje samostatný produkt s digitálnymi prvkami a preto podlieha CRA. V takýchto prípadoch sa musí posúdiť súlad so základnými požiadavkami s ohľadom na zamýšľaný účel náhradnej súčiastky. Osobitný význam má funkcia náhradnej súčiastky spočívajúca v zabezpečení kompatibility alebo interoperability s existujúcim produktom s digitálnymi prvkami, a to aj v prípade, ak ide o produkt s digitálnymi prvkami uvedený na trh pred začatím uplatňovania CRA. Ak nie je možné primerane splniť určité základné požiadavky z dôvodu tohto zamýšľaného účelu alebo technických obmedzení, výrobca to musí zohľadniť v posúdení rizík kybernetickej bezpečnosti a zaviesť primerané alternatívne alebo kompenzačné opatrenia na zmiernenie rizík, aby nedošlo k ohrozeniu bezpečnosti produktu s digitálnymi prvkami. Ako sa uvádza aj v časti 2.6 Zložité systémy, kľúčovú úlohu pri transparentnom opise zistených obmedzení, súvisiacich kybernetickobezpečnostných rizík a zavedených opatrení na zmiernenie rizík zohrávajú tak technická dokumentácia, ako aj informácie a pokyny pre používateľa. Ako sa vysvetľuje v časti 4.1 Fyzické opravy, výmena vadných dielov alebo opotrebovaných súčastí za diely s lepšími vlastnosťami sama o sebe nespôsobuje podstatnú úpravu opraveného produktu s digitálnymi prvkami.

*Príklad 36: Výrobca uviedol na trh EÚ prepojené riadiace jednotky. V jednom prípade bol ovládač uvedený na trh v roku 2026, pred dátumom uplatňovania CRA. V inom prípade bol ovládač uvedený na trh v roku 2028 v súlade s CRA. V roku 2028 došlo k poruche digitálneho komunikačného modulu v oboch typoch ovládačov. Výrobca dodáva ako náhradný diel výmenný modul, ktorý je identický a vyrobený podľa rovnakých špecifikácií ako originál.*

*V oboch prípadoch spadá náhradný modul do rozsahu pôsobnosti výnimky uvedenej v článku 2 ods. 6. Náhradný diel sám o sebe nepodlieha CRA, hoci ide o produkt s digitálnymi prvkami, pretože nahrádza identickú súčasť v produkte s digitálnymi prvkami. Oprava nepredstavuje podstatnú úpravu produktu s digitálnymi prvkami.*

*Príklad 37: Výrobca uviedol na trh EÚ v roku 2026 pripojený priemyselný regulátor, a to pred dátumom uplatňovania CRA. V roku 2028 došlo k poruche komunikačného čipu*

*v tomto regulátore. Keďže výrobca tento čip už nevyrába, dodáva ako náhradný diel novší čip s rovnocennou funkcionalitou, avšak s odlišnou kryptografickou implementáciou a aktualizovaným mechanizmom bezpečného spustenia, s cieľom zachovať kompatibilitu a nepretržitú prevádzku.*

*V tomto prípade nemožno náhradný čip považovať za identický, keďže rozdiely v kryptografickej implementácii a mechanizme bezpečného spúšťania ovplyvňujú vlastnosti čipu v oblasti kybernetickej bezpečnosti. Preto sa naň nevzťahuje výnimka podľa článku 2 ods. 6 a predstavuje produkt s digitálnymi prvkami, na ktorý sa vzťahuje CRA. Súlad náhradného dielu sa musí posudzovať s ohľadom na jeho zamýšľaný účel, vrátane jeho úlohy pri zabezpečovaní interoperability s produktom s digitálnymi prvkami uvedeným na trh pred začatím uplatňovania CRA.*

*Príklad 38: Výrobca uvedie na trh v roku 2028 inteligentný regulátor budov v súlade s CRA. V roku 2029 dôjde k poruche bezdrôtového modulu v tomto regulátore. Keďže výrobca tento modul už nevyrába, dodá ako náhradný diel nový modul, ktorý plní rovnakú funkciu s využitím rovnakých komunikačných protokolov a bezpečnostných mechanizmov, je však založený na inej sade čipov a má aktualizovaný firmvér, ktorý nemení vlastnosti, ktoré môžu byť relevantné pre kybernetickú bezpečnosť.*

*V tomto prípade možno náhradný modul považovať za identický. Na modul sa preto vzťahuje výnimka podľa článku 2 ods. 6 a nepodlieha CRA.*

102. Výnimka pre náhradné diely sa uplatňuje bez ohľadu na to, či náhradný diel nahrádza súčasť v rámci produktu s digitálnymi prvkami, alebo či nahrádza kompletný produkt s digitálnymi prvkami, ktorý sám tvorí súčasť väčšieho produktu, a to aj v prípade, ak je tento väčší produkt s digitálnymi prvkami zložený z viacerých integrovaných súčastí, za predpokladu, že náhradný diel je konkrétne dodávaný ako náhradný diel, ako je vysvetlené v predchádzajúcich odsekoch.

*Príklad 39: V roku 2027 uvedie výrobca na trh systém priemyselnej automatizácie, ktorý obsahuje programovateľný logický kontrolér (PLC) ako jednu zo svojich zložiek. V roku 2031 dôjde k poruche centrálnej procesorovej jednotky (CPU) PLC. Výrobca ponúka dve možnosti opravy: i) dodanie náhradnej jednotky CPU, ktorú možno považovať za identickú s pôvodne nainštalovanou CPU; alebo ii) dodanie kompletného náhradného PLC, ktoré možno považovať za identické s pôvodne nainštalovaným PLC. V oboch prípadoch sa náhradný diel dodáva prostredníctvom kanála popredajného servisu výrobcu ako náhradný diel a priemyselný automatizačný systém, pre ktorý je náhradný diel určený, je jasne identifikovaný. V oboch prípadoch spadá náhradný diel do rozsahu výnimky uvedenej v článku 2 ods. 6, bez ohľadu na to, či sa náhrada týka súčasti v rámci PLC, alebo PLC ako celku.*

### 4.3. Aktualizácie softvéru ako podstatné úpravy

103. Vývoj softvéru má iteratívny charakter, pričom softvérové produkty s digitálnymi prvkami, ktoré sú už uvedené na trh, sa často a priebežne aktualizujú. V tejto súvislosti je užitočné poskytnúť ďalšie usmernenia na určenie, kedy sa má softvér považovať za podstatne upravený. Takéto usmernenia majú najmä pomôcť výrobcovi softvérových produktov s digitálnymi prvkami, ktorí vykonávajú zmeny na svojich vlastných produktoch, určiť, či tieto zmeny predstavujú podstatnú úpravu.

104. V odôvodnení č. 39 sa uvádza, že produkt s digitálnymi prvkami je podstatne upravený vtedy, ak zmena ovplyvňuje úroveň kybernetickobezpečnostného rizika a ak výrobca takéto zmenené alebo dodatočné riziko nezohľadnil vo svojom posúdení rizík a následne ani pri implementácii základných požiadaviek. Výrobca by preto mal v jednotlivých prípadoch posúdiť, či aktualizácia softvéru prináša nové alebo zvýšené kybernetickobezpečnostné riziká a či sa takéto riziká už zohľadnili v jeho posúdení rizík.
105. Ak výrobca zavedie do produktu s digitálnymi prvkami nové funkcionality, ktoré majú za následok zmenu zamýšľaného účelu produktu ako celku, je pravdepodobné, že výrobca takéto zmeny nezohľadnil vo svojom posúdení rizík. Za takýchto okolností by sa táto zmena vo všeobecnosti považovala za podstatnú úpravu.

*Príklad 40: Výrobca uvádza na trh riadiaci panel, ktorý zbiera údaje zo strojov a zobrazuje trendy a výstrahy, pričom nemá možnosť tieto stroje ovládať. Výrobca následne vyvinie novú verziu tohto riadiaceho panela, do ktorej zavedie funkcionality, ktoré mu umožňujú ovládať stroje, a to aj prostredníctvom úpravy prevádzkových parametrov a reštartovania strojov po poruchových stavoch. V dôsledku týchto zmien sa zamýšľaný účel riadiaceho panela posunul nad rámec toho, čo bolo predpokladané v posúdení rizík, a to z riadiaceho panela na produkt s digitálnymi prvkami určeným na vykonávanie prevádzkovej kontroly nad inými zariadeniami. Riadiaci panel bol preto podstatne upravený.*

*Príklad 41: Výrobca uvádza na trh spotrebiteľskú softvérovú aplikáciu určenú na organizovanie a zobrazovanie osobných údajov, ako sú e-maily, správy alebo dokumenty, a na podporu základných funkcií vyhľadávania a filtrovania. Výrobca následne zavádza aktualizáciu, ktorá umožňuje aplikácii automaticky analyzovať obsah používateľa s cieľom vytvárať profily správania a prijímať automatizované rozhodnutia ovplyvňujúce prioritizáciu, potláčanie alebo odporúčanie obsahu bez zásahu používateľa. V dôsledku tejto zmeny sa zamýšľaný účel softvéru mení z nástroja na správu informácií ovládaného používateľom na automatizovaný systém rozhodovania, čo nebolo zahrnuté v posúdení rizík. Aplikácia bola preto podstatne upravená.*

106. Zároveň je však možné, že výrobca postupne zavádza nové funkcionality, ktoré už boli zahrnuté v jeho posúdení rizík, alebo ktoré samy osebe nemenia profil kybernetickobezpečnostného rizika produktu s digitálnymi prvkami. Tak tomu môže byť napríklad v prípade, ak výrobca predpokladal vývoj týchto funkcionalít, už opísal a posúdil súvisiace riziká a zaviedol primerané zmierňujúce opatrenia na zabezpečenie trvalej zhody so základnými požiadavkami. Tak tomu môže byť aj v prípade, ak nové funkcionality nezavádzajú zmeny, ktoré by so sebou prinášali nové alebo zvýšené riziká. Aktualizácie tohto charakteru by sa preto nemali považovať za podstatné úpravy, keďže nezvyšujú kybernetickobezpečnostné riziko a následne nemenia spôsob plnenia základných požiadaviek.

*Príklad 42: Aplikácia na zasielanie správ je pôvodne uvedená na trh s funkcionalitou obmedzenou na zasielanie správ medzi dvoma osobami. Posúdenie rizika výrobcu zahŕňa neskoršie zavedenie skupinového zasielania správ, vrátane napríklad zvýšenej zložitosti smerovania správ. V následnej aktualizácii výrobca pridáva funkcionality skupinového chatu spolu s nástrojmi na správu a moderovanie, ktoré boli už*

*v pôvodnom návrhu predpokladané a posúdené. Aktualizácia zavádza funkcionality, ktoré spadajú do rozsahu pôvodného zamýšľaného účelu a posúdenia rizika. Aplikácia na zasielanie správ preto nebola podstatne upravená.*

*Príklad 43: Systém monitorovania výroby sa uvádza na trh s povolenými riadiacimi panelmi len na čítanie, pričom prvky automatizovaného riadenia sú prítomné v architektúre systému, ale zostávajú deaktivované. Posúdenie rizík výrobcu výslovne zahŕňa budúcu aktiváciu automatizovaných regulačných slučiek, vrátane kybernetickobezpečnostných rizík spojených s riadením v uzavretej slučke, ako aj bezpečnostných opatrení, ako sú mechanizmy ručného prebratia riadenia operátorom a stavy zabezpečené proti zlyhaniu. V neskoršej aktualizácii výrobca aktivuje prvky automatizovaného riadenia a bezpečnostné opatrenia tak, ako bolo pôvodne posúdené. Systém monitorovania výroby preto nebol podstatne upravený.*

107. Naopak, aj obmedzené alebo zdanlivo menej významné nové funkcionality môžu so sebou priniesť závažné kybernetickobezpečnostné riziká, ktoré ovplyvňujú súlad so základnými požiadavkami. Posúdenie podstatnej úpravy by sa preto nemalo zakladať na rozsahu alebo zložitosti zmeny, ale na jej potenciálnom nepriaznivom vplyve na profil kybernetickobezpečnostného rizika produktu s digitálnymi prvkami a následne na plnenie základných požiadaviek.

*Príklad 44: Výrobca zavádza aktualizáciu softvérovej aplikácie, ktorou pridáva prvok „zapamätať si ma“ alebo prvok trvalého prihlásenia, ktorá lokálne ukladá autentizačné tokeny s cieľom zvýšiť pohodlie používateľa. Hoci je rozsah tejto funkcionality obmedzený, prináša nové riziká súvisiace s krádežou tokenov, neoprávneným prístupom a prevzatím relácie, ktoré neboli zohľadnené v posúdení rizík. Aktualizácia preto ovplyvňuje súlad so základnými požiadavkami. Softvérová aplikácia bola podstatne upravená.*

*Príklad 45: Výrobca pridáva do existujúceho softvérového produktu s digitálnymi prvkami nový prvok protokolovania a diagnostiky, ktorá umožňuje export podrobných systémových protokolov na účely riešenia problémov. Hoci sa táto funkcionality javí ako menej významná, vedie k zberu a ukladaniu citlivých prevádzkových údajov v nezašifrovanom formáte, čím vznikajú riziká zverejnenia údajov, ktoré neboli predtým posúdené ani zmiernené. Táto zmena môže preto mať významný vplyv na profil kybernetickobezpečnostných rizík produktu s digitálnymi prvkami. Softvérový produkt s digitálnymi prvkami bol podstatne upravený.*

108. V súlade s odôvodnením č. 39 CRA sa bezpečnostné aktualizácie vo všeobecnosti nepovažujú za podstatné úpravy, keďže ich primárnym účelom je znížiť úroveň kybernetickobezpečnostného rizika spojeného s produktom s digitálnymi prvkami. Bezpečnostná aktualizácia, ktorá neupravuje zamýšľaný účel daného produktu a nezavádza nové kybernetickobezpečnostné riziká, by sa preto nemala považovať za podstatnú úpravu, a to ani v prípade, ak táto aktualizácia môže priniesť významné technické zmeny. To platí aj v prípadoch, keď sú určité funkcionality upravené alebo obmedzené výlučne za účelom zmiernenia zistených zraniteľností a zabezpečenia pokračujúceho súladu so základnými požiadavkami.

*Príklad 46: Výrobca nasadí bezpečnostnú aktualizáciu s cieľom odstrániť zraniteľnosť v kódovej základni produktu s digitálnymi prvkami opravou chyby autentizácie vstupných údajov, ktorá by mohla viesť k pretečeniu vyrovnávacej pamäte, alebo opravou logickej chyby umožňujúcej obídenie overovania totožnosti prostredníctvom nesprávneho overovania relácie. Aktualizácia upravuje vnútornú implementáciu softvéru bez toho, aby ovplyvnila zamýšľaný účel daného produktu alebo zaviedla nové riziko. Cieľom takejto aktualizácie je výlučne znížiť kybernetickobezpečnostné riziko. Bezpečnostná aktualizácia by sa nemala považovať za podstatnú úpravu.*

*Príklad 47: Výrobca zavádza bezpečnostnú aktualizáciu, ktorá posilňuje existujúce bezpečnostné konfigurácie, napríklad sprísnením pravidiel firewallu, deaktiváciou nepoužívaných sieťových portov, zmenou predvolených zásad pre heslá správcov alebo zavedením povinnej viacfaktorovej autentizácie tam, kde bola táto funkcionality už k dispozícii alebo sa s ňou počítalo. Hoci aktualizácia môže ovplyvniť spôsob, akým používatelia konfigurujú produkt s digitálnymi prvkami alebo k nemu pristupujú, nemení jeho zamýšľaný účel a slúži výlučne na posilnenie jeho bezpečnostnej úrovne. Bezpečnostná aktualizácia by sa nemala považovať za podstatnú úpravu.*

*Príklad 48: Výrobca uvádza na trh softvérový produkt s digitálnymi prvkami, ktorý zabezpečuje komunikáciu pomocou konfigurovateľného šifrovacieho rámca podporujúceho viacero kryptografických algoritmov a veľkostí kľúčov, ako je opísané v technickej dokumentácii produktu a v posúdení rizík. Posúdenie rizík zahŕňa všetky kryptografické možnosti poskytované v produkte s digitálnymi prvkami a predpokladá budúce vyradenie určitých algoritmov z používania. Posúdenie rizík zahŕňa aj zmierňujúce opatrenia, ako napríklad kryptografickú agilitu, internú správu kľúčov a testovanie kompatibility. V reakcii na nové kryptografické usmernenia výrobca nasadí bezpečnostnú aktualizáciu, ktorá deaktivuje zastaraný algoritmus a aktivuje silnejšiu, už podporovanú alternatívu, bez zavedenia nových externých závislostí alebo zmeny tokov údajov. Keďže aktualizácia implementuje bezpečnostné opatrenie, ktoré bolo predpokladané a posúdené ako súčasť pôvodného návrhu, a nezavádza nové kybernetickobezpečnostné riziká, táto bezpečnostná aktualizácia by sa nemala považovať za podstatnú úpravu.*

109. Naopak, bezpečnostná aktualizácia sa môže považovať za podstatnú úpravu, ak napriek svojmu bezpečnostnému cieľu vedie k tomu, že zamýšľaný účel produktu s digitálnymi prvkami je upravený nad rámec toho, čo bolo pôvodne predpokladané, alebo ak prináša nové alebo zvýšené kybernetickobezpečnostné riziká. Tak tomu môže byť napríklad prípad, keď aktualizácia podstatne mení hranice daného produktu alebo štruktúru závislostí spôsobom, ktorý nebol predpokladaný v posúdení rizík, napr. podstatnou zmenou tokov údajov alebo pridaním nových externých rozhraní.

*Príklad 49: Výrobca uvádza na trh softvérový produkt s digitálnymi prvkami, ktorý má slúžiť na lokálne šifrovanie súborov uložených na zariadení používateľa, čím umožňuje používateľom šifrovať a dešifrovať súbory podľa potreby. Po zistení zraniteľnosti v procese šifrovania výrobca nasadí bezpečnostnú aktualizáciu, ktorá odstraňuje funkcionality lokálneho šifrovania a namiesto toho vyžaduje, aby boli všetky súbory nahrané, uložené a spracované prostredníctvom šifrovacej služby na diaľku*

prevádzkovej výrobcou. V dôsledku tejto zmeny produkt s digitálnymi prvkami už nevykonáva lokálne šifrovanie tak, ako bolo pôvodne zamýšľané, ale funguje ako služba šifrovania na diaľku a spracovania údajov. Hoci je aktualizácia zavedená z bezpečnostných dôvodov, zásadným spôsobom mení zamýšľaný účel daného produktu spôsobom, ktorý nebol predpokladaný v posúdení rizík, a preto sa považuje za podstatnú úpravu.

*Príklad 50: Výrobca uvádza na trh softvérový produkt s digitálnymi prvkami, ktorý na zabezpečenie komunikácie medzi komponentmi produktu s digitálnymi prvkami využíva zavedený šifrovací protokol a interne spravovaný životný cyklus kľúčov. V reakcii na novo zistené kryptografické slabiny výrobca zavádza bezpečnostnú aktualizáciu, ktorá nahrádza existujúci šifrovací mechanizmus iným protokolom vyžadujúcim použitie externej služby správy kľúčov prevádzkovej treťou stranou. V dôsledku tejto zmeny sa podstatne menia závislosti a toky údajov produktu s digitálnymi prvkami, čím sa zavádzajú nové externé rozhrania a závislosť od služieb tretích strán, ktoré neboli zohľadnené v posúdení rizík. Hoci je aktualizácia motivovaná bezpečnostnými dôvodmi, prináša nové kybernetickobezpečnostné riziká, a preto sa považuje za podstatnú úpravu.*

110. Ako sa uvádza v bode 104 vyššie, to, či aktualizácia softvéru predstavuje podstatnú úpravu, by sa malo posudzovať individuálne v každom jednotlivom prípade. Pri vykonávaní tohto posúdenia môžu výrobcovia zvážiť, bez toho, aby bol tento zoznam vyčerpávajúci, či aktualizácia softvéru:
- a. zavádza nové vektory hrozieb, ako sú dodatočné rozhrania, komunikačné kanály, prostredia na spúšťanie alebo externé závislosti, prostredníctvom ktorých by sa mohli hrozby prejaviť;
  - b. umožňuje nové scenáre útokov, vrátane napríklad nových spôsobov, ktorými by mohlo dôjsť k neoprávnenému prístupu, manipulácii, zasahovaniu alebo zneužitiu produktu s digitálnymi prvkami alebo údajov, ktoré tento produkt spracúva;
  - c. mení pravdepodobnosť predtým identifikovaných scenárov útokov, napríklad znížením úsilia alebo odborných znalostí potrebných na ich zneužitie, zvýšením vystavenia nedôveryhodným subjektom alebo oslabením existujúcich ochranných opatrení;
  - d. mení potenciálny dopad predtým identifikovaných scenárov útokov, vrátane napríklad rozsahu dotknutých údajov alebo funkcií, závažnosti prevádzkových, bezpečnostných alebo ekonomických dôsledkov, alebo schopnosti zistiť incident, zabrániť jeho šíreniu alebo sa z neho zotaviť.
111. V niektorých prípadoch aktualizácia softvéru nezavádza nové vektory hrozieb, neumožňuje nové scenáre útokov a podstatne nemení pravdepodobnosť ani dopad predtým identifikovaných scenárov útokov. To môže naznačovať, že aktualizácia nezavádza nové ani zvýšené kybernetickobezpečnostné riziká, za predpokladu, že predpoklady a zmierňujúce opatrenia, na ktorých sa zakladalo posúdenie rizík, zostávajú platné a účinné. Je preto pravdepodobné, že aktualizácia nespĺňa kritériá podstatnej úpravy.

112. Naopak, aktualizácia softvéru môže priniesť nové vektory hrozieb, umožniť nové scenáre útokov alebo podstatne zmeniť pravdepodobnosť alebo dopad existujúcich scenárov útokov. V takýchto prípadoch by výrobca mal opätovne posúdiť kybernetickobezpečnostné riziká produktu s digitálnymi prvkami a určiť, či sa naďalej spĺňajú základné požiadavky, vrátane toho, či aktualizácia prináša nové alebo zvýšené riziká, ktoré neboli predpokladané v posúdení rizík.
113. To, či aktualizácia softvéru spĺňa kritériá podstatnej úpravy, je relevantné pri určovaní, či sa uplatňujú určité povinnosti podľa CRA, ako je uvedené v bode 91. Bez ohľadu na túto kvalifikáciu však výrobcovia naďalej nesú zodpovednosť za zabezpečenie bezpečnosti aktualizácií softvéru a svojho produktu s digitálnymi prvkami počas obdobia podpory v súlade s požiadavkami na riešenie zraniteľností stanovenými v časti II prílohy I k CRA. Okrem toho, bez ohľadu na to, či sa aktualizácie softvéru považujú za podstatné úpravy alebo nie, výrobcovia sú povinní udržiavať posúdenie rizík a technickú dokumentáciu presné, úplné a neustále aktuálne v súlade s článkom 13 ods. 7 a článkom 31 ods. 2.

#### 4.4. Dôsledky podstatnej úpravy

114. Dôsledky podstatnej úpravy vykonanej iným subjektom ako pôvodným výrobcom produktu s digitálnymi prvkami, ktorý je už uvedený na trhu, sú upravené v článkoch 21 a 22 CRA. Článok 21 sa týka dovozcov a distribútorov, zatiaľ čo článok 22 sa týka akejkoľvek fyzickej alebo právnickej osoby inej ako výrobcu, dovozcu alebo distribútor.
115. Ak podstatnú úpravu vykoná pôvodný výrobca produktu s digitálnymi prvkami, dôsledky vyplývajú zo všeobecne ustanoveného pojmu podstatnej úpravy uvedeného v odôvodnení 41 CRA a sú podrobnejšie rozpracované v oddiele 2.1 Modrej príručky. V tejto časti sa uvádza, že produkt, ktorý bol po uvedení na trh podrobený významným zmenám alebo generálnej oprave, sa považuje za nový produkt, ak došlo k úprave jeho pôvodnej výkonnosti, účelu alebo typu, ak sa zmenila povaha nebezpečenstva alebo sa zvýšila úroveň rizika a ak je produkt s digitálnymi prvkami sprístupnený na trhu.
116. Všeobecne uznávaným dôsledkom je preto to, že ak sa úprava produktu s digitálnymi prvkami kvalifikuje ako podstatná úprava a upravený produkt s digitálnymi prvkami je sprístupnený na trhu, na účely CRA sa s ním má zaobchádzať ako s novým produktom s digitálnymi prvkami. V dôsledku toho sprístupnenie podstatne upraveného produktu na trhu predstavuje nové uvedenie na trh. To platí bez ohľadu na to, či sa podstatná úprava vykonáva pôvodným výrobcom alebo inou osobou. S cieľom zabezpečiť jednotné a primerané uplatňovanie CRA vo vzťahu k rôznym kategóriám subjektov, ktoré môžu vykonať podstatnú úpravu, nasledujúce pododdiely upravujú povinnosti osoby vykonávajúcej podstatnú úpravu v prípade, že sa podstatne upravený produkt s digitálnymi prvkami uvedie na trh. Dôsledky pre obdobie podpory produktu s digitálnymi prvkami sú upravené v oddiele 5 „Obdobie podpory“.

##### 4.4.1. Podstatné úpravy vykonané inou osobou ako pôvodným výrobcom

117. V súlade s článkami 21 a 22, ak podstatnú úpravu produktu s digitálnymi prvkami, ktorý je už uvedený na trh, vykoná fyzická alebo právnická osoba iná ako výrobca produktu s digitálnymi prvkami, osoba, ktorá vykoná podstatnú úpravu a uvedie upravený

produkt s digitálnymi prvkami na trh, sa považuje za výrobcu upraveného produktu s digitálnymi prvkami, bez ohľadu na to, či sa táto osoba podieľala na pôvodnom návrhu alebo na uvedení tohto produktu na trh.

118. Článok 22 ďalej objasňuje, že osoba vykonávajúca úpravu podlieha povinnostiam stanoveným v článkoch 13 a 14 iba v súvislosti s tou časťou produktu s digitálnymi prvkami, ktorej sa podstatná úprava týka, ak táto úprava nemá vplyv na kybernetickú bezpečnosť produktu s digitálnymi prvkami ako celku.
119. Ak podstatná úprava ovplyvňuje súlad so základnými požiadavkami, ale nemá negatívny vplyv na kybernetickú bezpečnosť produktu s digitálnymi prvkami ako celku, osoba vykonávajúca úpravu podlieha ustanoveniam článku 13 (vrátane povinnosti zabezpečiť súlad so základnými požiadavkami a vykonať postup posudzovania zhody) a článku 14 (povinnosti podávať správy) iba vo vzťahu k tej časti produktu s digitálnymi prvkami, ktorá bola podstatne upravená<sup>16</sup>. Okrem toho sa povinnosti pôvodného výrobcu podľa CRA naďalej vzťahujú na pôvodný produkt s digitálnymi prvkami uvedený na trh, čím sa zabezpečuje kontinuita pri riešení zraniteľností a dodržiavanie požiadaviek v prípade nezmenených častí.
120. Prípád podstatnej úpravy by sa nemal zamieňať s prípadmi integrácie, pri ktorých osoba montuje komponenty (vrátane ich prípadnej úpravy) do nového produktu s digitálnymi prvkami, ktorý sama uvádza na trh. V takýchto prípadoch integrátor neupravuje produkt s digitálnymi prvkami, ktorý už na trh uviedol iný výrobca; skôr uvádza nový produkt s vlastnými digitálnymi prvkami na trh. Integrátor je na účely CRA výrobcom tohto nového produktu s digitálnymi prvkami a je povinný dodržiavať nariadenie v plnom rozsahu, pokiaľ ide o produkt s digitálnymi prvkami ako celok. Ak výrobca integruje komponenty, na ktoré sa vzťahuje CRA, môže sa spoliehať na činnosti zamerané na zabezpečenie zhody vykonávané výrobcami týchto komponentov, aby uľahčil vlastné dodržiavanie CRA.

*Príklad 51: Spoločnosť nakupuje hotové moduly mikrokontrolérov a komponenty pre pripojenie od tretích dodávateľov, vyvíja vlastný firmvér a súbor senzorov a montuje ich do prepojeného poľnohospodárskeho monitorovacieho produktu s digitálnymi prvkami, ktorý uvádza na trh pod vlastným menom. Hoci spoločnosť upravila základné moduly mikrokontrolérov a skombinovala ich s inými komponentmi, nejde o podstatnú úpravu produktu s digitálnymi prvkami, ktorý je už uvedený na trh; skôr uvádza na trh nový produkt s digitálnymi prvkami. Spoločnosť je výrobcom poľnohospodárskeho monitorovacieho zariadenia na účely CRA a je povinná dodržiavať nariadenie v súvislosti s poľnohospodárskym monitorovacím zariadením ako celkom.*

121. Ak podstatná úprava vykonaná inou osobou ako pôvodným výrobcom negatívne ovplyvňuje kybernetickú bezpečnosť produktu s digitálnymi prvkami ako celku,

---

<sup>16</sup> V súlade s oddielom 2.1 Modrej príručky „nie je potrebné opakovať skúšky a vypracúvať novú dokumentáciu v súvislosti s aspektmi, na ktoré nemá úprava vplyv. Je na fyzickej alebo právnickej osobe, ktorá vykonáva zmeny alebo dáva vykonať zmeny na produkte, aby preukázala, že nie je potrebné aktualizovať všetky prvky technickej dokumentácie. Fyzická alebo právnická osoba, ktorá vykonáva zmeny na produkte alebo dáva vykonať zmeny na produkte, nesie zodpovednosť za zhodu upraveného produktu a vyhotoví vyhlásenie o zhode, aj keď využíva existujúce skúšky a technickú dokumentáciu“.

napríklad preto, že úprava už nie je zameraná ani obmedzená na konkrétnu súčiastku alebo subsystém, upravený produkt s digitálnymi prvkami uvedený na trh by sa mal považovať za nový produkt s digitálnymi prvkami, na ktorý sa v plnom rozsahu vzťahuje CRA. V takýchto prípadoch sa zmenil celkový profil kybernetickobezpečnostného rizika daného produktu a úpravu nie je možné posúdiť bez zohľadnenia produktu s digitálnymi prvkami ako celku. Osoba vykonávajúca úpravu podlieha povinnostiam výrobcu stanoveným v článkoch 13 a 14, pokiaľ ide o upravený produkt s digitálnymi prvkami ako celok.

#### 4.4.2. Podstatné úpravy vykonané pôvodným výrobcom

122. Ak podstatnú úpravu vykoná pôvodný výrobca, a to aj v kontexte iteratívneho vývoja softvérových produktov s digitálnymi prvkami, tento výrobca zostáva výrobcom na účely CRA. Podstatne upravený produkt s digitálnymi prvkami sa však považuje za produkt novo uvedený na trh.
123. V súlade s oddielom 2.1 Modrej príručky môže pôvodný výrobca, ktorý uvádza podstatne upravený produkt s digitálnymi prvkami na trh, opätovne použiť existujúcu dokumentáciu a testy pre tie aspekty produktu s digitálnymi prvkami, ktoré nie sú podstatnou úpravou ovplyvnené. Najmä v prípade, ak výrobca uvádza na trh podstatne upravené verzie toho istého produktu s digitálnymi prvkami, mal by sa postup posudzovania zhody zamerať na podstatne upravené časti produktu s digitálnymi prvkami. Podobne, ak sa vykonáva posudzovanie zhody treťou stranou, orgán posudzovania zhody by mal svoje posudzovanie zamerať na podstatne upravené časti. V prípade nezmenených častí produktu s digitálnymi prvkami môže opätovne použiť existujúcu dokumentáciu a výsledky skúšok.
124. Úvahy o proporcionalite uvedené v predchádzajúcej podsekcii sa rovnako vzťahujú na podstatné úpravy vykonané pôvodným výrobcom produktu s digitálnymi prvkami uvedeného na trh pred 11. decembrom 2027. Takáto podstatná úprava vykonaná pôvodným výrobcom sama o sebe nevyžaduje, aby výrobca uviedol celý produkt s digitálnymi prvkami, ktorý bol uvedený na trh pred týmto dátumom, do plného súladu s CRA, pokiaľ táto úprava negatívne neovplyvňuje kybernetickú bezpečnosť produktu s digitálnymi prvkami ako celku. Ak úprava neovplyvňuje kybernetickú bezpečnosť produktu s digitálnymi prvkami ako celku, povinnosti pôvodného výrobcu v súvislosti s touto úpravou by sa mali obmedziť na podstatne upravené časti.

## 5. Obdobie podpory

125. Článok 13 ods. 8 CRA vyžaduje, aby výrobcovia stanovili obdobie podpory, počas ktorého sa zraniteľnosti produktu s digitálnymi prvkami, vrátane jeho komponentov, riešia účinne a v súlade so základnými požiadavkami stanovenými v časti II prílohy I. Obdobie podpory odzrkadľuje časové obdobie, počas ktorého sa predpokladá, že sa produkt s digitálnymi prvkami bude používať (predpokladá čas používania), a malo by sa stanoviť s ohľadom na kritériá uvedené v článku 13 ods. 8, najmä na primerané očakávania používateľov, povahu produktu s digitálnymi prvkami vrátane jeho zamýšľaného účelu, ako aj na príslušné právo Únie, ktorým sa stanovuje životnosť produktov s digitálnymi prvkami<sup>17</sup>. Celkovo sa tieto kritériá majú zohľadňovať spôsobom, ktorý zabezpečí proporionalitu pri určovaní obdobia podpory.
126. Článok 13 ods. 8 ďalej vyžaduje, aby obdobie podpory trvalo najmenej päť rokov, pokiaľ sa nepredpokladá, že produkt s digitálnymi prvkami bude v prevádzke menej ako päť rokov, pričom v takom prípade sa obdobie podpory zhoduje s predpokladaným časom používania. Minimálne obdobie podpory preto slúži iba ako ochranné opatrenie, ktoré zabezpečuje, že zraniteľnosti sa riešia počas dostatočne dlhého obdobia, pričom výrobcom umožňuje zohľadniť produkty s digitálnymi prvkami, ktorých predpokladaný čas používania je skutočne kratší. Odôvodnenie 60 poskytuje v tomto ohľade ďalšie usmernenia a objasňuje, že produkty s digitálnymi prvkami, u ktorých sa odôvodnene predpokladá, že budú v prevádzke dlhšie ako päť rokov, by mali mať zodpovedajúcim spôsobom dlhšie obdobia podpory. Obdobie podpory v dĺžke piatich rokov sa preto nemá považovať za predvolené pre všetky produkty s digitálnymi prvkami. Výrobca by namiesto toho mal určiť primerané obdobie podpory s ohľadom na kritériá uvedené v článku 13 ods. 8.
127. Článok 13 ods. 19 vyžaduje, aby výrobcovia v čase nákupu jasným a zrozumiteľným spôsobom uviedli dátum ukončenia obdobia podpory (aspoň mesiac a rok). Vyžaduje tiež, aby výrobcovia po uplynutí obdobia podpory zobrazili používateľom oznámenie, ak je to technicky realizovateľné vzhľadom na povahu produktu s digitálnymi prvkami. Cieľom tejto povinnosti je zabezpečiť transparentnosť pre používateľov, pokiaľ ide o dĺžku trvania, počas ktorej možno predpokladať bezpečnostnú podporu.
128. V prípade softvérových produktov s digitálnymi prvkami, ktoré sa často vyvíjajú a uvádzajú na trh postupne a pri ktorých sa v priebehu času môžu na trh často uvádzať podstatne upravené verzie, je potrebné obdobie podpory chápať s ohľadom na tento model vývoja. Každá podstatne upravená verzia softvérového produktu s digitálnymi prvkami uvádzaná na trh musí mať deklarované obdobie podpory, ktoré je v súlade s článkom 13 ods. 8. To zahŕňa minimálne obdobie podpory v dĺžke najmenej piatich rokov, pokiaľ nie je preukázateľne kratší predpokladaný čas používania danej verzie, ako tiež upresnené v odôvodnení 60. *Časť 5.1 „Podstatné úpravy a obdobie podpory“*

---

<sup>17</sup> Medzi ďalšie kritériá, ktoré sa môžu zohľadniť v súlade s článkom 13 ods. 8, patria obdobia podpory produktov s digitálnymi prvkami ponúkajúcimi podobnú funkcionality, ktoré uvádzajú na trh iní výrobcovia, dostupnosť prevádzkového prostredia, obdobia podpory integrovaných komponentov, ktoré zabezpečujú základné funkcie a pochádzajú od tretích strán, ako aj príslušné usmernenia poskytnuté skupinou pre administratívnu spoluprácu CRA (ADCO) a Komisiou.

dalej upresňuje, že ak podstatná úprava nevedie k zmenám faktorov, ktoré pôvodne určovali predpokladaný čas používania produktu s digitálnymi prvkami, pôvodné obdobie podpory zostáva nezmenené (t. j. vrátane prípadov, keď zostávajúce obdobie podpory je kratšie ako päť rokov).

129. Článok 13 ods. 10 poskytuje flexibilitu pre softvérové produkty s digitálnymi prvkami tým, že umožňuje výrobcovi za určitých podmienok zabezpečiť súlad s požiadavkou na riešenie zraniteľností stanovenou v bode 2 časti II prílohy I (riešenie a odstraňovanie zraniteľností) iba pre verziu softvérového produktu s digitálnymi prvkami, ktorá bola ako posledná uvedená na trh. Toto je povolené v prípade, ak používatelia predtým uvedených verzií majú bezplatný prístup k verzii, ktorá bola ako posledná uvedená na trh, a nevznikajú im dodatočné náklady na prispôbienie hardvérového a softvérového prostredia, v ktorom používajú pôvodnú verziu daného produktu.
130. Na účely článku 13 ods. 10 by sa pojem „dodatočné náklady“ mal vykladať prakticky a primerane, s prihliadnutím na bežné a predpokladané postupy pri údržbe a prevádzke softvéru. Nezahŕňa primerané prevádzkové úsilie, ktoré je neoddeliteľnou súčasťou inštalácie aktualizácií softvéru alebo udržiavania bezpečného prevádzkového prostredia, ako je čas personálu, rutinné testovanie, úpravy konfigurácie alebo aktualizácie základných softvérových závislostí, ktoré sú potrebné na riešenie komponentov na konci životnosti alebo známych bezpečnostných zraniteľností. Naopak, „dodatočné náklady“ sa týkajú záťaží, ktoré presahujú to, čo sa bežne dá predpokladať v súvislosti s aktualizáciami softvéru, ako je povinný nákup nového hardvéru, výmena infraštruktúry alebo zásadné zmeny prevádzkového prostredia.
131. V prípade neustále sa vyvíjajúcich softvérových produktov s digitálnymi prvkami môžu výrobcovia uvádzať na trh postupne podstatne upravené verzie v relatívne krátkych intervaloch a očakávať, že používatelia budú pravidelne vykonávať aktualizácie. V takýchto prípadoch musí deklarované obdobie podpory pre každú podstatne upravenú verziu spĺňať požiadavky článku 13 ods. 8 v čase jej uvedenia na trh. Inými slovami, výrobca musí pre túto podstatne upravenú verziu deklarovať nové obdobie podpory. Výrobcovia sa však môžu opierať o článok 13 ods. 10 a prestať riešiť a odstraňovať zraniteľnosti v starších verziách, akonáhle budú môcť používatelia bezplatne a bez dodatočných nákladov, ako je uvedené vyššie, prejsť na novšiu verziu, aj keď to bude mať za následok skrátenie skutočného obdobia podpory pre tieto staršie verzie<sup>18</sup>. Výrobca naďalej podlieha ostatným požiadavkám na riešenie zraniteľností uvedeným v časti II prílohy I, ako aj oznamovacím povinnostiam podľa článku 14. Ako sa vysvetľuje aj v odôvodnení 40, tieto požiadavky zahŕňajú okrem iného všetky následné podstatne upravené verzie softvérového produktu s digitálnymi prvkami, ktoré sú uvedené na trh na trhu:
- i) dodržiavanie politiky koordinovaného zverejňovania zraniteľností

---

<sup>18</sup> Je potrebné pripomenúť, že článok 13 ods. 19 vyžaduje, aby výrobcovia, ak je to technicky realizovateľné vzhľadom na povahu produktu s digitálnymi prvkami, zobrazili používateľom oznámenie, v ktorom ich informujú, že ich produkt s digitálnymi prvkami dosiahol koniec obdobia podpory. Ak sa teda riešenie a odstraňovanie zraniteľností pre staršie verzie ukončí, predpokladá sa, že používatelia, ktorí neprešli na najnovšiu verziu, budú informovaní, ak je to technicky realizovateľné.

- ii) opatrenia na uľahčenie zdieľania informácií o potenciálnych zraniteľnostiach<sup>19</sup>.

*Príklad 52: Výrobca uvedie na trh EÚ model smartfónu a vyhlási obdobie podpory v dĺžke X rokov odo dňa uvedenia na trh, počas ktorého bude poskytovať bezpečnostné aktualizácie riešiace zraniteľnosti. Počas tohto obdobia výrobca vydáva pravidelné softvérové aktualizácie a podstatne upravené verzie operačného systému, ktoré si používatelia môžu nainštalovať bezplatne bez potreby nového hardvéru.*

*Výrobca môže v súlade s článkom 13 ods. 10 riešiť a odstraňovať zraniteľnosti v najnovšej verzii operačného systému sprístupnenej pre daný model smartfónu za predpokladu, že staršie verzie je možné aktualizovať bezplatne a bez dodatočných nákladov. Počas trvania obdobia podpory sa na výrobcu naďalej vzťahujú ostatné požiadavky na riešenie zraniteľností, ako napríklad koordinované zverejňovanie zraniteľností a opatrenia na zdieľanie informácií.*

*Príklad 53: Výrobca uvádza na trh podnikový softvérový produkt s digitálnymi prvkami a každých niekoľko mesiacov vydáva podstatne upravené verzie, ktoré odrážajú vylepšenia v oblasti bezpečnosti, nové prvky a kompatibilitu s aktualizovanými operačnými systémami a platformami. Každá verzia sa uvádza na trh s deklarovaným obdobím podpory v súlade s článkom 13 ods. 8. Výrobca očakáva, že používatelia budú pravidelne vykonávať aktualizácie v rámci bežnej prevádzky, a poskytuje bezplatný prístup k najnovšej verzii. Inštalácia aktualizácií môže vyžadovať primerané prevádzkové úsilie, ako je testovanie alebo úpravy konfigurácie, nevyžaduje však dodatočné náklady, ako je nákup nového hardvéru alebo zásadné zmeny infraštruktúry. V tejto súvislosti sa výrobca môže opierať o článok 13 ods. 10 a prestať riešiť a odstraňovať zraniteľnosti v starších verziách, akonáhle si používatelia môžu aktualizovať na najnovšiu verziu, pričom naďalej spĺňa ostatné požiadavky na riešenie zraniteľností pre všetky následné podstatne upravené verzie.*

## 5.1. Podstatné úpravy a obdobie podpory

132. Ako sa uvádza v oddiele 4.4 „Dôsledky podstatnej úpravy“, ak sa úprava produktu s digitálnymi prvkami kvalifikuje ako podstatná úprava a upravený produkt s digitálnymi prvkami sa uvádza na trh, na účely CRA sa s ním zaobchádza ako s novým produktom a samotný akt uvedenia podstatne upraveného produktu s digitálnymi prvkami na trh predstavuje nové uvedenie na trh. Je preto užitočné objasniť vplyv, ktorý má toto nové uvedenie na trh na obdobie podpory podstatne upraveného produktu s digitálnymi prvkami.
133. Obdobie podpory podstatne upraveného produktu s digitálnymi prvkami by sa malo určiť s ohľadom na predpokladaný čas používania daného produktu, a to na základe kritérií stanovených v článku 13 ods. 8 CRA. Podstatná úprava by preto mala vyžadovať opätovné posúdenie na základe týchto kritérií, ale automaticky nevedie k obnoveniu alebo dokonca predĺženiu obdobia podpory. Rozhodujúca je otázka, či podstatná

---

<sup>19</sup> Je potrebné poznamenať, že ak môžu používatelia bez dodatočných nákladov prejsť na najnovšiu verziu softvéru, výrobcovia sa napriek tomu môžu rozhodnúť naďalej riešiť a odstraňovať zraniteľnosti v starších verziách tohto softvéru, a to aj za úhradu alebo na základe iných komerčných dohôd. CRA nevyžaduje, aby výrobcovia poskytovali bezpečnostné aktualizácie pre takéto staršie verzie bezplatne.

úprava ovplyvňuje faktory, ktoré pôvodne určili predpokladaný čas používania daného produktu, a tým aj pôvodné obdobie podpory.

134. Ak podstatná úprava tieto faktory neovplyvňuje, kritériá stanovené v článku 13 ods. 8 naďalej uvádzajú rovnaký predpokladaný čas používania, ako bol pôvodne stanovený, a obdobie podpory upraveného produktu s digitálnymi prvkami by sa malo zosúladiť so zostávajúcim predpokladaným časom používania produktu, ako bol pôvodne uvedený na trh. To bude zvyčajne platiť v prípadoch, keď bol predpokladaný čas používania stanovený predovšetkým na základe faktorov, ktoré úprava nemení, ako je fyzická životnosť hardvérových komponentov, pričom podstatná úprava sa týka iba funkcionality softvéru alebo back-endových služieb.

*Príklad 54: Výrobca uvedie na trh robotický vysávač s predpokladaným časom používania X rokov, stanoveným na základe povahy produktu s digitálnymi prvkami, vrátane fyzickej životnosti a charakteristík opotrebenia hardvérových komponentov, a so zreteľom na primerané očakávania používateľov, pokiaľ ide o životnosť daného produktu. Výrobca stanoví obdobie podpory na X rokov. Po Y rokoch výrobca vydá aktualizáciu softvéru, ktorá spĺňa kritériá podstatnej úpravy, pričom pridáva nové režimy čistenia a navigačné prvky. Aktualizácia softvéru nemá vplyv na fyzickú životnosť hardvéru a nemení primerané očakávania používateľov, pokiaľ ide o životnosť daného produktu. Kritériá podľa článku 13 ods. 8 preto naďalej uvádzajú rovnaký predpokladaný čas používania. Obdobie podpory upraveného produktu s digitálnymi prvkami zodpovedá zostávajúcemu predpokladanému času používania, ako bolo pôvodne stanovené.*

*Príklad 55: Výrobca uvádza na trh komplexný priemyselný stroj s digitálnymi prvkami, ktorého cloudové back-endové riešenie slúži na spracovanie údajov na diaľku. Predpokladaný čas používania je X rokov, stanovený na základe primeraných očakávaní používateľov a povahy produktu s digitálnymi prvkami, ako je fyzická životnosť hardvéru stroja a predpokladané opotrebenie. Obdobie podpory je stanovené tak, aby zodpovedalo tomuto predpokladanému času používania, t. j. X rokov. Po uplynutí Y rokov výrobca prekonštruje cloudové zázemie (riešenie spracovania údajov na diaľku) a zavedie nové rozhrania API a toky údajov spôsobom, ktorý sa považuje za podstatnú úpravu produktu s digitálnymi prvkami, avšak nemení povahu tohto produktu ani neovplyvňuje očakávania používateľov. Kritériá uvedené v článku 13 ods. 8 preto naďalej uvádzajú ten istý predpokladaný čas používania. Obdobie podpory upraveného produktu s digitálnymi prvkami zodpovedá zostávajúcemu predpokladanému času používania, ako bolo pôvodne stanovené.*

135. Ak podstatná úprava ovplyvňuje faktory, ktoré pôvodne určovali predpokladaný čas používania produktu s digitálnymi prvkami, výrobca by mal prepočítať obdobie podpory tak, aby odrážalo nový predpokladaný čas používania, pričom by mal primerane uplatniť kritériá uvedené v článku 13 ods. 8. Tak tomu môže byť napríklad v prípade modernizačných úprav hardvéru, ktoré predlžujú prevádzkovú životnosť daného produktu, alebo v prípade podstatného preprogramovania alebo prepísania základného softvéru daného produktu, ktoré podstatne mení jeho predpokladaný čas

používania<sup>20</sup>.

*Príklad 56: Výrobca uvádza na trh programovateľný logický kontrolér (PLC) s predpokladaným časom používania X rokov, stanovenou predovšetkým na základe povahy produktu s digitálnymi prvkami a životnosti príslušného hardvéru. Obdobie podpory je stanovená zodpovedajúcim spôsobom. Niekoľko rokov po prvotnom uvedení na trh výrobca vykoná podstatnú úpravu spočívajúcu vo výmene vstavanej výpočtovej platformy PLC, vrátane procesora, pamäte a prostredia pre beh aplikácií, za komponenty novej generácie navrhnuté pre výrazne dlhšiu prevádzkovú životnosť. V dôsledku tejto úpravy sa menia primerané očakávania používateľov a povaha produktu s digitálnymi prvkami: používateľ PLC môže teraz primerane očakávať, že PLC zostane v produktívnom používaní aj po uplynutí pôvodne deklarovaného predpokladaného času používania, a to vďaka novej výpočtovej platforme. Kritériá uvedené v článku 13 ods. 8 preto naznačujú dlhší predpokladaný čas používania a výrobca podľa toho prepočíta obdobie podpory pre dané konkrétne PLC.*

---

<sup>20</sup> Je potrebné pripomenúť, že, ako sa uvádza v oddiele 4.1 „Fyzické opravy“, renovačné, údržbárske alebo opravárenské činnosti sa vo všeobecnosti nepovažujú za podstatné úpravy.

## 6. Dôležité a kritické produkty s digitálnymi prvkami

136. V článku 7 ods. 1 CRA sa stanovuje, že produkty s digitálnymi prvkami, ktoré majú základnú funkčnosť kategórie produktov uvedenej v prílohe III k nariadeniu, sa považujú za „dôležité produkty s digitálnymi prvkami“. Príloha III ďalej rozdeľuje dôležité produkty s digitálnymi prvkami na triedu I a triedu II. Podobne článok 8 ods. 1 stanovuje, že produkty s digitálnymi prvkami, ktoré majú základnú funkčnosť kategórie produktov uvedenej v prílohe IV k CRA, sa považujú za „kritické produkty s digitálnymi prvkami“<sup>21</sup>.
137. Klasifikácia produktu s digitálnymi prvkami ako dôležitého alebo kritického, alebo naopak ako produktu patriaceho do „default“ kategórie<sup>22</sup>, je relevantná pri určovaní postupu posudzovania zhody, ktorý musí výrobca v súlade s článkom 32 dodržať, skôr než môže tento produkt s digitálnymi prvkami uviesť na trh. Je potrebné poznamenať, že produkty s digitálnymi prvkami v „default“ kategórii sa môžu vždy spoliehať na postup vnútornej kontroly založený na module A („samoposúdenie“)<sup>23</sup>. Dôležité produkty s digitálnymi prvkami triedy I alebo II a kritické produkty s digitálnymi prvkami podliehajú prísnejšiemu postupu posudzovania zhody. To sa nevzťahuje na dôležité produkty s digitálnymi prvkami triedy I alebo II, ktoré spĺňajú podmienky slobodného softvéru a softvéru s otvoreným zdrojovým kódom a ktoré sa uvádzajú na trh, pri ktorých môžu výrobcovia v súlade s článkom 32 ods. 5 postupovať podľa postupov platných pre „default“ kategóriu.
138. Pojem „základná funkčnosť“ je preto pre výrobcu kľúčový pri určovaní uplatniteľného režimu posudzovania zhody. Tento pojem však nie je v nariadení o posudzovaní zhody výslovne definovaný. Produkty s digitálnymi prvkami môžu plniť celý rad funkcií, z ktorých niektoré môžu byť doplnkové vo vzťahu k základnej funkčnosti daného produktu, a nemali by mať vplyv na klasifikáciu produktu ako produkt v kategórii „default“/dôležitý produkt triedy I/dôležitý produkt triedy II/kritický produkt. Je preto užitočné poskytnúť ďalšie usmernenia, ktoré pomôžu výrobcovi správne vykonávať príslušné postupy posudzovania zhody a ktoré pomôžu orgánom dohľadu nad trhom zabezpečiť harmonizované uplatňovanie nariadenia o posudzovaní zhody v celej EÚ.

### 6.1. Základná funkčnosť

139. Základná funkčnosť produktu s digitálnymi prvkami sa vzťahuje na hlavné prvky a technické schopnosti daného produktu, bez ktorých by nemohol plniť svoj zamýšľaný účel. Je možné ju posúdiť s ohľadom na konkrétny kontext a podmienky používania daného produktu, pričom sa zohľadňujú okrem iného informácie, ktoré výrobca uvádza v návode na použitie, propagačných alebo predajných materiáloch a vyhláseniach, ako

<sup>21</sup> Vykonávacie nariadenie Komisie (EÚ) č. 2025/2392 stanovuje technický popis kategórií dôležitých a kritických produktov

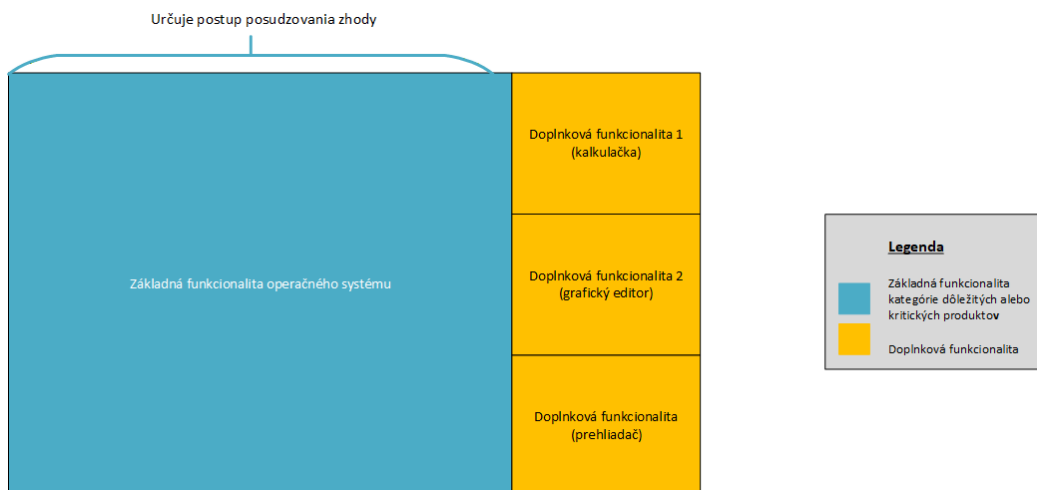
<sup>22</sup> Pojem „default“ kategória nie je v CRA definovaný. Použitie tohto pojmu v tomto dokumente sa vzťahuje na produkty s digitálnymi prvkami, ktoré nemajú základnú funkčnosť kategórie produktov uvedenej v prílohách III alebo IV k CRA a ktoré sa preto riadia režimom posudzovania zhody stanoveným v článku 32 ods. 1.

<sup>23</sup> Výrobca sa však vždy môže rozhodnúť uplatniť prísnejší postup posudzovania zhody, ako je stanovené v článku 32 ods. 1.

aj v technickej dokumentácii.

*Príklad 57: Softvérový produkt s digitálnymi prvkami poskytuje abstrakčnú vrstvu nad základným hardvérom a riadi vykonávanie softvérových komponentov. Medzi jeho hlavné prvky patrí inicializácia hardvéru a periférnych zariadení, správa procesov a pamäte, riadenie vstupov a výstupov, plánovanie, pridelovanie zdrojov a sprístupňovanie systémových služieb a aplikačných programových rozhraní (API), prostredníctvom ktorých aplikácie interagujú s hardvérovými a softvérovými zdrojmi zariadenia. V technickej dokumentácii sa uvádza, že produkt s digitálnymi prvkami koordinuje výpočtové zdroje, vynucuje systémové konfigurácie a poskytuje štandardizované rozhrania pre softvérové moduly a pripojené periférie. Výrobca zdôrazňuje, že vďaka týmto schopnostiam môže platforma slúžiť ako centrálné softvérové prostredie, v ktorom môžu aplikácie spoľahlivo bežať. Produkt s digitálnymi prvkami má základnú funkcionality operačného systému, ako je opísané v prílohe I bode 11 vykonávacieho nariadenia (EÚ) 2025/2392.*

140. Funkcionalita produktu s digitálnymi prvkami je zriedka obmedzená výlučne na jeho základnú funkcionality, keďže produkty s digitálnymi prvkami často – ak nie vždy – plnia dodatočné funkcie, ktoré neprispievajú k základnej funkcionality produktu. Môže to zahŕňať aj začlenenie komponentov, ktoré samy osebe majú funkcionality iného dôležitého alebo kritického produktu s digitálnymi prvkami. Skutočnosť, že produkt s digitálnymi prvkami plní iné alebo dodatočné funkcie, ako sú uvedené v technických popisoch dôležitých alebo kritických produktov s digitálnymi prvkami, však sama osebe nebráni tomu, aby produkt mal jednu takúto základnú funkcionality.



Obrázok 2: Ilustrácia toho, ako základná funkcionality, a nie doplnkové funkcionality, určuje uplatniteľný postup posudzovania zhody

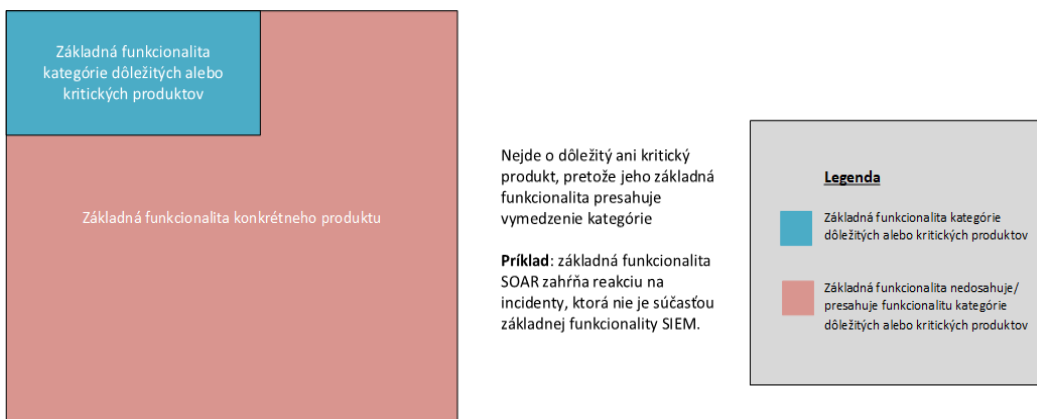
141. Produkt s digitálnymi prvkami môže byť schopný plniť funkcie kategórie dôležitých alebo kritických produktov, napriek tomu však mať základnú funkcionality odlišnú od funkcionality takejto kategórie produktov. V takýchto prípadoch by sa daný produkt s digitálnymi prvkami nepovažoval za dôležitý alebo kritický produkt s digitálnymi prvkami. Ako sa výslovne uvádza v článku 7 ods. 1 CRA pre dôležité produkty s digitálnymi prvkami (a pri uplatnení tej istej logiky na kritické produkty s digitálnymi prvkami) samotná integrácia dôležitého alebo kritického produktu s digitálnymi

prvkami ešte sama o sebe nespôsobuje, že sa produkt s digitálnymi prvkami stáva dôležitým alebo kritickým produktom s digitálnymi prvkami.

*Príklad 58: Smartfón obsahuje operačný systém, ktorý poskytuje funkcionality opísané v prílohe I bode 11 vykonávacieho nariadenia (EÚ) 2025/2392. Hoci operačný systém umožňuje správu hardvérových zdrojov a spúšťanie softvérových aplikácií, smartfón ako celok má odlišnú základnú funkcionality (napr. umožňovať používateľom komunikovať a získavať prístup k informáciám a službám). Samotná integrácia operačného systému neznamená, že smartfón má základnú funkcionality operačného systému.*

142. Niektoré produkty s digitálnymi prvkami môžu byť podobné dôležitej alebo kritickej kategórii produktov alebo môžu patriť do tej istej všeobecnej skupiny produktov, avšak ich základná funkcionality môže podstatne presahovať alebo podstatne zaostávať za základnou funkcionality danej kategórie. To neplatí v prípade, ak produkt s digitálnymi prvkami obsahuje dodatočné funkcionality, ktoré iba dopĺňajú alebo vylepšujú základnú funkcionality, ktorá sama o sebe zodpovedá základnej funkcionality dôležitej alebo kritickej kategórie produktov; v takýchto prípadoch si produkt s digitálnymi prvkami zachováva základnú funkcionality danej kategórie a je podľa toho zaradený. Toto posúdenie by sa malo zakladať na hlavných prvkoch a technických schopnostiach daného produktu, posudzovaných objektívne s ohľadom na jeho zamýšľaný účel, a nie na spôsobe, akým je produkt s digitálnymi prvkami opisovaný alebo uvádzaný na trh, ak tento popis neodzrkadľuje skutočné technické charakteristiky produktu.

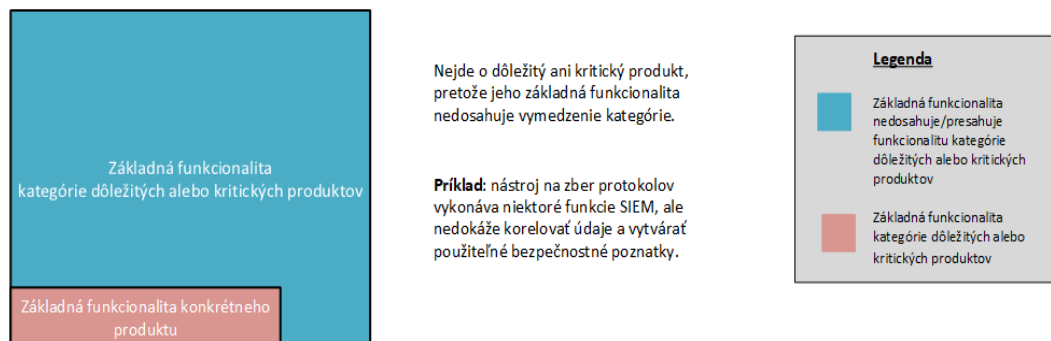
*Príklad 59: Softvér na koordináciu, automatizáciu a reakciu v oblasti bezpečnosti (SOAR) má často schopnosť vykonávať funkcie produktov s digitálnymi prvkami v kategórii „systémov na riadenie bezpečnostných informácií a udalostí (SIEM)“, t. j. zbierať údaje z viacerých zdrojov, analyzovať a korelovať tieto údaje a prezentovať ich ako informácie využiteľné na účely súvisiace s bezpečnosťou. Základná funkcionality tohto softvéru však podstatne presahuje funkcionality systému SIEM, pričom zahŕňa služby, ako je reakcia na incidenty, ako kľúčové prvky svojich technických schopností. Softvér SOAR sa preto vo všeobecnosti nepovažuje za produkt s základnou funkcionality systémov SIEM.*



Obrázok 3: Ilustrácia základnej funkcionality produktu s digitálnymi prvkami, ktorá podstatne presahuje definíciu kategórie dôležitých alebo kritických produktov

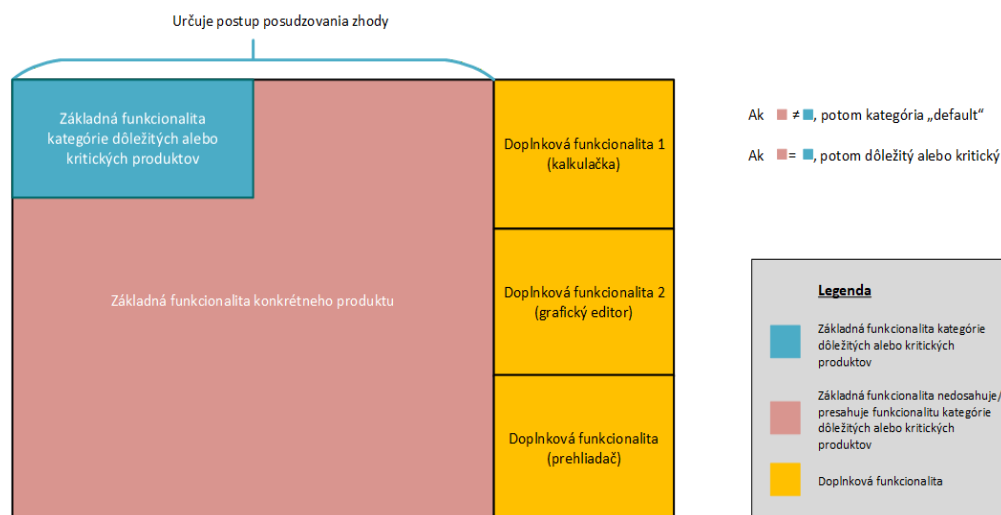
*Príklad 60: Niektoré nástroje na zber a vizualizáciu protokolov majú schopnosť načítavať údaje z protokolov a zobrazovať základné riadiace panely s udalosťami*

systému. Hoci tieto nástroje môžu podporovať činnosti v oblasti monitorovania bezpečnosti, ich základná funkcionálna nedosahuje úroveň systémov SIEM, keďže nevykonávajú koreláciu údajov ani neposkytujú využiteľné bezpečnostné informácie. Preto sa vo všeobecnosti nepovažuje, že takéto nástroje majú základnú funkcionálnu systémov SIEM.



Obrázok 4: Ilustrácia základnej funkcionality produktu s digitálnymi prvkami, ktorá výrazne nespĺňa definíciu kategórie dôležitých alebo kritických produktov

143. Výrobca nesmie nesprávne uvádzať základnú funkcionálnu svojho produktu s digitálnymi prvkami tak, aby sa vyhol režimu posudzovania zhody uplatniteľnému na dôležité alebo kritické produkty s digitálnymi prvkami, napr. tým, že nadmerne zdôrazňuje alebo bagatelizuje úlohu určitých funkcionálov, čím produkt podstatne prekračuje alebo nedosahuje danú základnú funkcionálnu. Tak by to bolo napríklad v prípade, ak existujú zjavné nezrovnalosti medzi propagačnými materiálmi, návodmi na použitie a technickou dokumentáciou.
144. Produkt s digitálnymi prvkami nesmie mať na účely určenia uplatniteľného režimu posudzovania zhody viac ako jednu základnú funkcionálnu. V súlade s prílohou VII CRA sú výrobcovia povinní v rámci technickej dokumentácie produktu opísať zamýšľaný účel svojho produktu s digitálnymi prvkami a postup posudzovania zhody, ktorý dodržali. Základná funkcionálna produktu by preto mala byť jasne identifikovaná. To umožňuje správne určenie príslušného režimu posudzovania zhody a umožňuje orgánom dohľadu nad trhom vykonávať dohľad a kontrolovať, či sa nariadenie správne uplatňuje.



Obrázok 5: Ilustrácia toho, ako základná funkcionálna konkrétneho produktu s digitálnymi prvkami určuje triedu produktu, a tým aj príslušný postup posudzovania zhody

145. Niektoré produkty s digitálnymi prvkami sa uvádzajú na trh ako samostatné produkty s digitálnymi prvkami, ale skladajú sa z odlišných modulov so samostatnými funkcionalitami. Ak výrobca tieto moduly uvádza na trh aj samostatne, napríklad v prípade, že sa ponúkajú na samostatný nákup, na základe licencie alebo predplatného, tieto moduly samy osebe predstavujú samostatné produkty s digitálnymi prvkami. Ako také sa majú klasifikovať na základe ich príslušných základných funkcionalít (a preto podliehajú príslušnému režimu posudzovania zhody na základe základnej funkcionalít každého modulu). Tým nie sú dotknuté moduly dodávané výlučne ako súčasti integrovaného produktu s digitálnymi prvkami, ktoré nie sú sprístupňované samostatne; v takýchto prípadoch sa základná funkcionalita určuje na úrovni integrovaného produktu s digitálnymi prvkami.

*Príklad 61: Výrobca uvádza na trh jednotný bezpečnostný balík kombinujúci viacero modulov, vrátane modulu SIEM, systému detekcie narušenia a analytického modulu. Výrobca ponúka tieto moduly aj v rámci samostatných predplatných. V tomto scenári je každý modul samostatným produktom s digitálnymi prvkami a klasifikuje sa na základe svojej vlastnej základnej funkcionality. Modul SIEM podlieha režimu posudzovania zhody pre dôležité produkty s digitálnymi prvkami triedy I, keďže jeho základnou funkcionalitou je funkcionalita „systémov riadenia bezpečnostných informácií a udalostí (SIEM)“. Systém detekcie narušení podlieha režimu posudzovania zhody pre dôležité produkty s digitálnymi prvkami triedy II, keďže jeho základnou funkcionalitou je funkcionalita „firewallov, systémov detekcie a prevencie narušení“. Analytický modul podlieha režimu posudzovania zhody pre „default“ produkty s digitálnymi prvkami, keďže jeho základná funkcionalita nepatrí do kategórie dôležitých ani kritických produktov.*

146. Nedodržanie povinností stanovených v článku 32 CRA môže viesť k udeleniu správnych pokút v súlade s článkom 64 ods. 3.

## 6.2. Posudzovanie zhody dôležitých a kritických produktov s digitálnymi prvkami

147. Akonáhle výrobca určí základnú funkcionalitu svojho produktu s digitálnymi prvkami, musí vykonať jeden z príslušných postupov posudzovania zhody. Výrobca musí zabezpečiť, aby produkt s digitálnymi prvkami ako celok spĺňal základné požiadavky, pričom musí primerane zohľadniť bezpečnosť komponentov alebo funkcionalít, ktoré sú do neho integrované.
148. Prísnejší postup posudzovania zhody za účasti tretej strany (na základe modulu B+C, modulu H alebo schém certifikácie kybernetickej bezpečnosti) je povinný pre dôležité produkty s digitálnymi prvkami triedy II (s výnimkou tých, ktoré spĺňajú podmienky pre voľne dostupný a softvér s otvoreným zdrojovým kódom v súlade s článkom 32 ods. 5) a pre kritické produkty s digitálnymi prvkami<sup>24</sup>. Naopak, dôležité produkty s digitálnymi prvkami triedy I (s výnimkou tých, ktoré spĺňajú podmienky slobodného softvéru a softvéru s otvoreným zdrojovým kódom v súlade s článkom 32 ods. 5) musia prejsť

<sup>24</sup> To platí aj v prípade využitia európskej schémy certifikácie kybernetickej bezpečnosti s úrovňou záruky aspoň „významná“, keďže sa vyžaduje zapojenie certifikačného orgánu tretej strany.

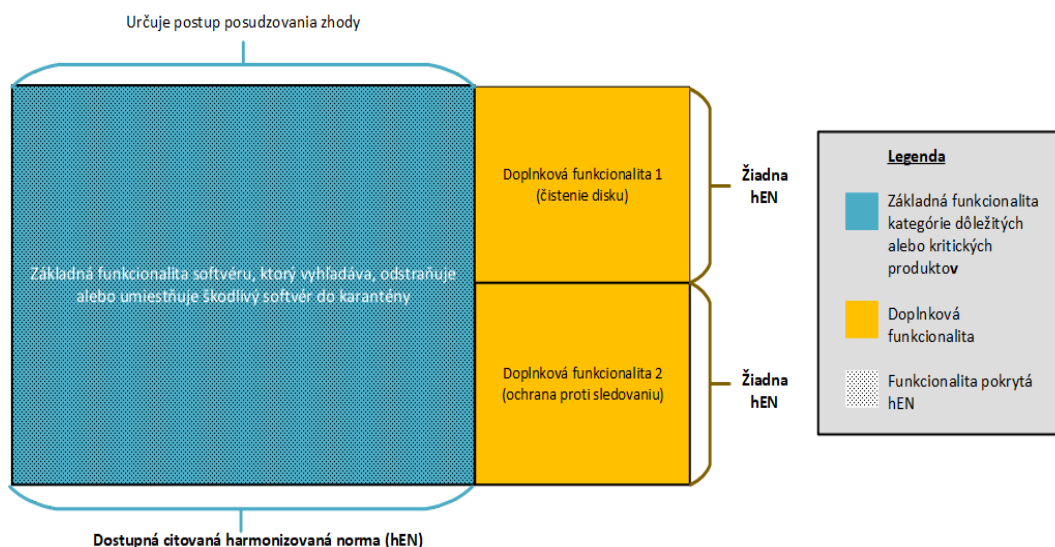
postupom posudzovania zhody vykonávaným treťou stranou len vtedy, ak výrobca neuplatnil alebo uplatnil len čiastočne príslušné harmonizované normy, na ktoré sa odkazuje v Úradnom vestníku Európskej únie (ďalej len „harmonizované normy“), spoločné špecifikácie alebo európske schémy certifikácie kybernetickej bezpečnosti aspoň na úrovni záruky „významná“<sup>25</sup>.

149. Preto, aby sa dôležitý produkt s digitálnymi prvkami triedy I mohol podrobiť postupu vnútornej kontroly,
- i) musia sa uplatniť všetky príslušné požiadavky príslušnej harmonizovanej normy; a
  - ii) rozsah pôsobnosti normy musí pokrývať aspoň všetky kybernetickobezpečnostné riziká spojené so základnou funkcionalitou daného produktu.
150. Rozsah pôsobnosti produktu s digitálnymi prvkami môže byť širší, než stanovuje príslušná harmonizovaná norma, a takéto dodatočné funkcie môžu predstavovať odlišné alebo dodatočné kybernetickobezpečnostné riziká. Výrobca je vždy povinný vykonať posúdenie rizík podľa článku 13 ods. 2 a mal by preto overiť, či uplatnenie harmonizovanej normy pokrýva všetky riziká spojené s produktom s digitálnymi prvkami. Ak uplatnenie normy nepokrýva všetky riziká, výrobca by mal inými prostriedkami zabezpečiť, aby jeho produkt s digitálnymi prvkami spĺňal základné požiadavky.
151. Ak teda výrobca dôležitého produktu s digitálnymi prvkami triedy I uplatnil príslušnú harmonizovanú normu, ktorá pokrýva riziká spojené so základnou funkcionalitou tohto produktu, môže sa rozhodnúť využiť postup vnútornej kontroly na preukázanie zhody svojho produktu. V rámci činností posudzovania zhody bude výrobca naďalej povinný preukázať, že sú riešené všetky riziká týkajúce sa jeho produktu s digitálnymi prvkami. Ak teda existuje rozdiel medzi rozsahom pôsobnosti harmonizovanej normy a rozsahom produktu s digitálnymi prvkami ako celku, výrobca musí aj naďalej zdokumentovať, aké dodatočné opatrenia zaviedol na riešenie týchto rizík.

*Príklad 62: Antivírusový softvér má základnú funkcionalitu softvéru, ktorý vyhľadáva, odstraňuje alebo umiestňuje do karantény škodlivý softvér, ako je opísané v prílohe I bod 4 vykonávacieho nariadenia (EÚ) 2025/2392. Tento produkt s digitálnymi prvkami obsahuje aj ďalšie prvky, a to konkrétne funkciu čistenia disku a funkciu proti sledovaniu, ktorá chráni používateľa pri prehliadaní webu. Výrobca vykonáva posúdenie rizík, ktoré sa vzťahuje na celý produkt s digitálnymi prvkami, vrátane základnej funkcionality antivírusového softvéru, funkcie čistenia disku a funkcie proti sledovaniu. Uplatňuje harmonizovanú normu, ktorá sa vzťahuje na riziká spojené so základnou funkcionalitou antivírusového softvéru, a dodatočné opatrenia na riešenie rizík vyplývajúcich z dodatočných funkcií. Výrobca môže na účely posúdenia zhody využiť postup vnútornej kontroly, ktorý sa vzťahuje na produkt s digitálnymi prvkami ako celok, vrátane funkcií čistenia disku a ochrany proti sledovaniu.*

---

<sup>25</sup> V záujme stručnosti sa zvyšná časť tejto časti vzťahuje iba na harmonizované normy, na ktoré boli uverejnené odkazy v Úradnom vestníku Európskej únie. Tieto usmernenia sa však vzťahujú aj na spoločné špecifikácie prijaté v súlade s článkom 27 ods. 2 a na európske schémy certifikácie kybernetickej bezpečnosti, ak to Komisia stanoví prostredníctvom delegovaných aktov v súlade s článkom 27 ods. 9.



Obrázok 6: Ilustrácia toho, ako použitie citovanej harmonizovanej normy, ktorá sa vzťahuje iba na základnú funkcionálnu, určuje platný postup posudzovania zhody

152. To platí aj v prípade, ak produkt s digitálnymi prvkami integruje dodatočnú funkciu, ktorá je sama osebe funkciou iného dôležitého alebo kritického produktu s digitálnymi prvkami. V skutočnosti je to základná funkcionálna produktu s digitálnymi prvkami ako celku, a nie funkcionálna integrovaných komponentov posudzovaná izolovane, ktorá určuje, či produkt s digitálnymi prvkami patrí do kategórie dôležitých alebo kritických produktov (a teda aj príslušný režim posudzovania zhody). Napríklad ak má produkt s digitálnymi prvkami základnú funkcionálnu dôležitého produktu s digitálnymi prvkami triedy I, tento produkt ako celok podlieha režimu posudzovania zhody uplatniteľnému na dôležité produkty s digitálnymi prvkami triedy I, hoci obsahuje zložku, ktorá je sama osebe kritickým produktom s digitálnymi prvkami. V týchto prípadoch, keď výrobca uplatňuje harmonizovanú normu pokrývajúcu riziká spojené so základnou funkcionálnou daného produktu, môže využiť postup vnútornej kontroly.

*Príklad 63: Hardvérový produkt s digitálnymi prvkami má základnú funkcionálnu smerovača, ako je opísané v prílohe I bode 12 vykonávacieho nariadenia (EÚ) 2025/2392. Tento produkt s digitálnymi prvkami obsahuje aj ďalšie funkcionality, vrátane funkcií firewallu, keďže integruje komponent firewallu. Výrobca vykonáva posúdenie rizík, ktoré sa vzťahuje na produkt s digitálnymi prvkami v celom jeho rozsahu, vrátane základnej funkcionality smerovača a funkcionality firewallu. Uplatňuje harmonizovanú normu, ktorá pokrýva riziká spojené so základnou funkcionálnou smerovača, a dodatočné opatrenia na riešenie rizík vyplývajúcich z dodatočných funkcií. Výrobca môže napríklad použiť harmonizovanú normu pre brány firewall na pokrytie rizík spojených s funkcionálnou firewall. Výrobca môže pri posudzovaní zhody využiť postup vnútornej kontroly, ktorý sa vzťahuje na produkt s digitálnymi prvkami ako celok, vrátane funkcionality firewall.*

### 6.3. Dôsledky pre predpoklad zhody

153. V článku 27 ods. 1 CRA sa stanovuje, že u produktov s digitálnymi prvkami a procesov zavedených výrobcom, ktoré sú v súlade s harmonizovanými normami alebo ich

časťami, ktorých odkazy boli uverejnené v *Úradnom vestníku Európskej únie (OJEU)*, sa predpokladá, že sú v súlade so základnými požiadavkami CRA, na ktoré sa vzťahujú uvedené normy alebo ich časti<sup>26</sup>. Článok 27 ods. 5 rozširuje tú istú predpoklad zhody na produkty s digitálnymi prvkami a procesmi zavedenými výrobcom, ktoré sú v súlade so spoločnými špecifikáciami prijatými Komisiou prostredníctvom vykonávacích aktov, a článok 27 ods. 8 stanovuje predpoklad zhody pre produkty s digitálnymi prvkami a procesmi zavedenými výrobcom, pre ktoré bolo vydané EÚ vyhlásenie o zhode alebo certifikát v rámci európskej schémy certifikácie kybernetickej bezpečnosti prijatej podľa nariadenia (EÚ) 2019/881, ak to bolo špecifikované prostredníctvom delegovaných aktov v súlade s článkom 27 ods. 9<sup>27</sup>.

154. Preto ak výrobca uplatnil harmonizovanú normu, na ktorú sa odkazuje v Úradnom vestníku EÚ, požíva predpoklad zhody pre riziká, na ktoré sa táto norma vzťahuje. Tak tomu môže byť napríklad v prípade, ak uvedená harmonizovaná norma rieši všetky riziká spojené so základnou funkcionalitou produktu s digitálnymi prvkami a neexistujú žiadne ďalšie funkcionality, ktoré by predstavovali kybernetickobezpečnostné riziká. Predpokladá sa napríklad, že Harmonizovaná norma pre smerovače bude riešiť aspoň riziká spojené so základnou funkcionalitou týchto produktov s digitálnymi prvkami. Ak takýto produkt neobsahuje žiadne dodatočné funkcionality alebo ak tieto dodatočné funkcionality nepredstavujú riziká, ktoré norma nerieši, produkt s digitálnymi prvkami môže využívať predpoklad zhody.
155. V prípadoch uvedených v bodoch 151 a 152 môže výrobca použiť postup vnútornej kontroly, pretože harmonizovaná norma pokrýva riziká spojené so základnou funkcionalitou produktu s digitálnymi prvkami. Produkty s digitálnymi prvkami opísané v týchto príkladoch však môžu mať širší rozsah pôsobnosti než harmonizované normy a dodatočné funkcionality môžu predstavovať kybernetickobezpečnostné riziká, ktoré táto harmonizovaná norma nerieši. Tieto produkty s digitálnymi prvkami preto nemusia mať nárok na predpoklad zhody, pokiaľ ide o tieto dodatočné funkcionality.

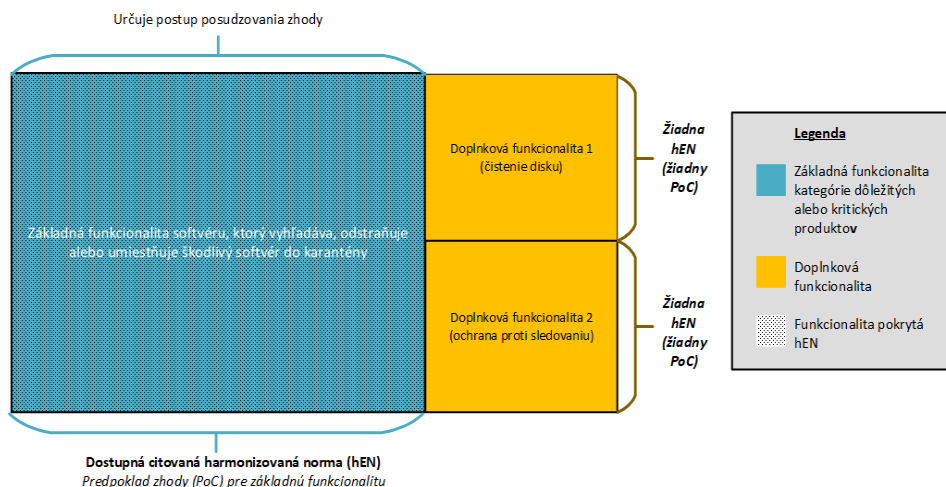
*Príklad 64: Antivírusový softvér má základnú funkcionalitu softvéru, ktorý vyhľadáva, odstraňuje alebo izoluje škodlivý softvér, a riziká spojené s touto základnou funkcionalitou sú pokryté harmonizovanou normou. Tento produkt s digitálnymi prvkami obsahuje aj dodatočné funkcionality, a to konkrétne funkciu čistenia disku a funkcionalitu proti sledovaniu, ktorá chráni používateľa pri prehliadaní webu, pričom riziká spojené s týmito funkcionalitami nie sú pokryté harmonizovanou normou. Ak sa uplatňuje harmonizovaná norma, výrobca môže na posúdenie zhody využiť postup vnútornej kontroly. Bude mať nárok na predpoklad zhody v súvislosti s rizikami*

---

<sup>26</sup> Ako sa jasne uvádza v oddiele 4.1.2.2 Modrej príručky, „v právnych predpisoch o harmonizácii týkajúcich sa rizík [...] výrobcovia vždy, aj pri používaní harmonizovaných noriem, ktorých odkazy sú uverejnené v Úradnom vestníku EÚ, nesú plnú zodpovednosť za posúdenie všetkých rizík svojho produktu s cieľom určiť, ktoré základné (alebo iné) požiadavky sú relevantné. Po tomto posúdení sa výrobca môže rozhodnúť uplatniť technické špecifikácie uvedené v harmonizovaných normách, na ktoré sa odkazuje v Úradnom vestníku EÚ, s cieľom zaviesť opatrenia na zníženie rizika, ktoré sú špecifikované v harmonizovaných normách“.

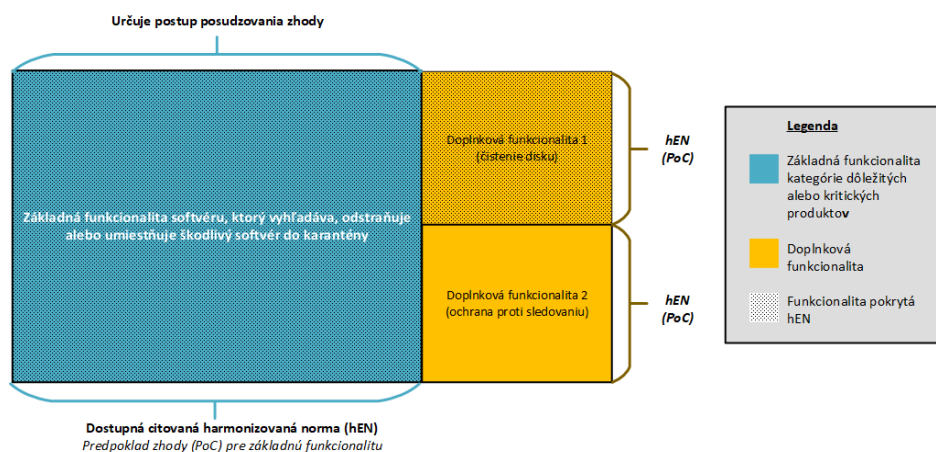
<sup>27</sup> Rovnako ako vyššie, v záujme stručnosti sa zvyšná časť tejto časti týka iba harmonizovaných noriem, na ktoré sa odkazuje v Úradnom vestníku EÚ. Tieto usmernenia sa však vzťahujú aj na spoločné špecifikácie a na európske schémy certifikácie kybernetickej bezpečnosti.

spojenými so základnou funkcionalitou daného produktu, nie však v súvislosti s rizikami spojenými s dodatočnými funkcionalitami.



Obrázok 7: Harmonizovaná norma poskytuje predpoklad zhody (PoC) pre základnú funkcionalitu, keďže rieši všetky riziká spojené s touto základnou funkcionalitou, nie však pre doplnkové funkcionality

Príklad 65: V rovnakom scenári ako v predchádzajúcom príklade bola harmonizovaná norma aktualizovaná tak, aby pokrývala aj riziká spojené s jednou z dodatočných funkcionalít, a to s funkciou čistenia disku, nie však s druhou (t. j. funkciou proti zanechávaniu stôp). Ak sa uplatňuje harmonizovaná norma, výrobca môže využiť postup vnútornej kontroly na posúdenie zhody. Bude mať prospech z predpokladu zhody v súvislosti s rizikami spojenými so základnou funkcionalitou daného produktu a s funkcionalitou čistenia disku, avšak nie v súvislosti s rizikami spojenými s funkcionalitou proti sledovaniu.



Obrázok 8: Harmonizovaná norma poskytuje predpoklad zhody (PoC) pre základnú funkcionalitu a doplnkovú funkcionalitu 1, keďže rieši všetky riziká spojené s týmito dvoma funkcionalitami, avšak nie pre doplnkovú funkcionalitu

## 7. Posúdenie kybernetickobezpečnostného rizika a integrácia produktov s digitálnymi prvkami a komponentov

### 7.1. O hodnotení a riešení kybernetickobezpečnostných rizík

156. Posúdenie kybernetickobezpečnostného rizika ustanovené v článku 13 ods. 2 CRA vyžaduje, aby výrobcovia identifikovali relevantné riziká a posúdili ich potenciálny vplyv na produkt s digitálnymi prvkami. Výrobcovia musia tiež zaviesť primerané opatrenia na riešenie týchto rizík v súlade so základnými požiadavkami uvedenými v prílohe I.
157. V rámci organizačného riadenia rizík sa riziká bežne hodnotia na základe kritérií prijateľnosti odvodených z vnútorných cieľov organizácie alebo jej ochoty podstupovať riziko. Naopak, podľa CRA by sa zostatkové kybernetickobezpečnostné riziko malo posudzovať s ohľadom na požiadavku, aby produkt s digitálnymi prvkami uvedený na trh zabezpečoval primeranú úroveň kybernetickej bezpečnosti na základe týchto rizík, pričom sa zohľadňuje jeho zamýšľaný účel a odôvodnene predvídateľné použitie.
158. V súlade s tým nie sú pri posudzovaní, či boli riziká primerane zohľadnené, relevantné vnútropodniková tolerancia výrobcu voči rizikám, jeho obchodná stratégia ani čisto nákladové hľadiská. Na účely článku 13 ods. 2 a 3 musia byť výrobcovia schopní určiť, či boli identifikované kybernetickobezpečnostné riziká dostatočne riešené prostredníctvom implementácie základných požiadaviek časti I prílohy I, s ohľadom na zamýšľaný účel, odôvodnene predvídateľné použitie a podmienky používania, vrátane, ak je to relevantné, prevádzkového prostredia (napríklad zamýšľaní používateľa produktu s digitálnymi prvkami) a aktív, ktoré majú byť chránené, pričom sa zohľadňuje predpokladaný čas používania produktu s digitálnymi prvkami.
159. Zvyškové kybernetickobezpečnostné riziko je neoddeliteľným výsledkom posúdenia rizika a riadenia rizika. Uznáva sa, že kybernetickobezpečnostné riziká nie je v praxi možné úplne eliminovať. Existencia zvyškového rizika však neznamená, že akékoľvek riziko možno akceptovať podľa uváženia výrobcu. Produkt s digitálnymi prvkami sa smie uviesť na trh len vtedy, ak sa reziduálne riziká po prijatí primeraných opatrení dostatočne riešia prostredníctvom splnenia základných požiadaviek, pričom sa zohľadňuje zamýšľaný účel a odôvodnene predvídateľné použitie produktu s digitálnymi prvkami.
160. V súlade s článkom 13 ods. 3 sú výrobcovia v prípade zistenia kybernetickobezpečnostných rizík povinní riešiť ich prostredníctvom primeraných opatrení, a to aj na úrovni produktu. V závislosti od okolností to môže zahŕňať napríklad zníženie plochy útoku, zavedenie technických ochranných opatrení, obmedzenie alebo prispôsobenie funkcionality alebo presnejšie vymedzenie zamýšľaného účelu produktu s digitálnymi prvkami. Výrobcovia môžu tiež prijať opatrenia na formovanie odôvodnene predvídateľného používania produktu s digitálnymi prvkami, napríklad prostredníctvom informovania o rizikách, usmerňovania používateľov alebo návrhu používateľského rozhrania, s cieľom nasmerovať správanie používateľov k bezpečným vzorom používania.

161. CRA neumožňuje prenášať kybernetickobezpečnostné riziko ani zodpovednosť na používateľov alebo tretie strany s cieľom kompenzovať nedostatky v návrhu produktu alebo ospravedlniť neriešenie kybernetickobezpečnostných rizík. Povinnosť uvádzať na trh bezpečný produkt s digitálnymi prvkami a preukázať zhodu so základnými požiadavkami zostáva na výrobcovi.
162. Informácie a pokyny poskytované používateľom sa môžu využiť na podporu bezpečného nasadenia a prevádzky produktu s digitálnymi prvkami, a to aj v prípadoch, keď sa výrobca rozhodol obmedziť zamýšľaný účel daného produktu na dôveryhodné prostredia, a na informovanie používateľov o zostatkových rizikách spôsobom, ktorý je primeraný povahe produktu s digitálnymi prvkami a jeho zamýšľaným používateľom.

*Príklad 66: Výrobca vyvíja priemyselný senzor určený na použitie v dôveryhodných prostrediach. Aby senzor správne plnil svoju funkcionality, výrobca nezavádza opatrenia na ochranu pred fyzickými útokmi na samotný senzor. S cieľom zmierniť súvisiace riziká identifikované v posúdení rizík výrobca obmedzuje zamýšľaný účel senzora výlučne na použitie v dôveryhodných prostrediach, kde je zabránené neoprávnenému fyzickému prístupu k produktu s digitálnymi prvkami. Informácie a pokyny pre používateľov poskytujú jasné informácie o týchto obmedzeniach používania snímača spôsobom, ktorý zodpovedá povahe produktu s digitálnymi prvkami a jeho zamýšľaným používateľom.*

*Príklad 67: Výrobca vyvíja softvérovú aplikáciu na profesionálne použitie na spravovaných stolných a mobilných zariadeniach. Aplikácia spracúva lokálne uložené citlivé údaje a obsah vytvorený používateľmi. Počas posúdenia rizík výrobca identifikuje riziko neoprávneného prístupu k takýmto údajom, ak sú uložené v čitateľnej podobe na zariadení. Namiesto navrhnutia a implementácie vlastného šifrovacieho mechanizmu priamo v aplikácii sa výrobca rozhodne spoľahnúť na funkcie šifrovania a správy kľúčov, ktoré natívne poskytuje operačný systém, na ktorom má aplikácia bežať, keďže vstavané kryptografické služby operačného systému sú vyspelé a pravidelne udržiavané.*

163. Ak posúdenie kybernetickobezpečnostného rizika identifikuje riziká, ktoré nie je možné primerane riešiť prostredníctvom vhodných opatrení, dodržanie CRA môže vyžadovať zmeny v návrhu, funkcionality alebo zamýšľanom účele produktu s digitálnymi prvkami. Úvahy týkajúce sa výlučne nákladov alebo obchodnej realizovateľnosti nepredstavujú dostatočný dôvod na to, aby sa takéto riziká neriešili, ak by to bránilo tomu, aby produkt s digitálnymi prvkami spĺňal základné požiadavky.

## 7.2. O navrhovaní, vývoji a výrobe produktov s digitálnymi prvkami takým spôsobom, aby zabezpečovali primeranú úroveň kybernetickej bezpečnosti na základe rizík

164. Základná požiadavka kybernetickej bezpečnosti uvedená v bode 1 časti I prílohy I k CRA stanovuje, že produkty s digitálnymi prvkami sa navrhujú, vyvíjajú a vyrábajú tak, aby zabezpečovali primeranú úroveň kybernetickej bezpečnosti na základe rizík.
165. Táto základná požiadavka je zameraná na riešenie všetkých

kybernetickobezpečnostných rizík, ktoré boli identifikované v rámci posúdenia kybernetickobezpečnostného rizika. Konkrétne zahŕňa kybernetickobezpečnostné riziká, ktoré nie sú inak primerane riešené v rámci implementácie základných požiadaviek časti I prílohy I, s výnimkou bodu (1). Táto základná požiadavka sa líši od zákonnej povinnosti vykonať posúdenie kybernetickobezpečnostného rizika, ktoré sa má vykonať podľa článku 13 ods. 2.

166. Ak sa všetky relevantné kybernetickobezpečnostné riziká kybernetickej bezpečnosti súvisiace s produktom s digitálnymi prvkami riešia zavedením primeraných opatrení na splnenie príslušných základných požiadaviek okrem bodu (1), základná požiadavka uvedená v bode (1) časti I prílohy I sa považuje za splnenú. Naopak, ak sa pri posúdení kybernetickobezpečnostných rizík zistia ďalšie riziká, ktoré nie sú týmito opatreniami plne pokryté, výrobcovia sú povinní zaviesť na produkte s digitálnymi prvkami primerané opatrenia na riešenie týchto rizík, aby produkt spĺňal základnú požiadavku uvedenú v bode (1) časti I prílohy I. V praxi sa vo väčšine prípadov predpokladá, že splnenie ostatných základných požiadaviek povedie k splneniu tejto požiadavky.

### 7.3. Posúdenie kybernetickobezpečnostného rizika a náležitá starostlivosť vo vzťahu k externým závislostiam a integrovaným komponentom

167. CRA stanovuje pre výrobcov dve odlišné, ale vzájomne sa dopĺňajúce povinnosti v súvislosti s riadením kybernetickobezpečnostných rizík. Po prvé, článok 13 ods. 2 vyžaduje, aby výrobcovia vykonali posúdenie kybernetickobezpečnostného rizika pre samotný produkt s digitálnymi prvkami. Po druhé, článok 13 ods. 5 ukladá povinnosť postupovať s náležitou starostlivosťou, pokiaľ ide o integrované komponenty. Tieto dve povinnosti sú spoločne navrhnuté tak, aby zabezpečili, že produkt s digitálnymi prvkami zostane bezpečný, a to aj v prípadoch, keď sa spolieha na riešenia spracovania údajov na diaľku, služby na diaľku alebo softvérové či hardvérové komponenty tretích strán.
168. Posúdenie kybernetickobezpečnostných rizík sa týka identifikácie a riadenia relevantných rizík, ktoré môžu ovplyvniť produkt s digitálnymi prvkami, vrátane rizík, ktoré majú pôvod mimo samotného produktu, ako sú externé siete, faktory prostredia alebo iné vonkajšie aspekty, ktoré by mohli ovplyvniť produkt s digitálnymi prvkami alebo na ktorých sa produkt spolieha. V prípade takýchto vonkajších rizík CRA nevyžaduje, aby výrobcovia kontrolovali alebo riadili vonkajšie prostredie. Od výrobcov sa skôr vyžaduje, aby takéto riziká identifikovali a zmierňovali ich prostredníctvom samotného návrhu a vývoja produktu s digitálnymi prvkami. To bude zahŕňať implementáciu príslušných základných požiadaviek stanovených v časti I prílohy I a v prípade potreby poskytovanie informácií a pokynov používateľom o rizikách súvisiacich s integráciou alebo nasadením.
169. Výrobca môže napríklad identifikovať riziko, že neoprávnené osoby môžu počas prevádzky produktu s digitálnymi prvkami získať prístup k back-endovým systémom, ktoré nie sú súčasťou samotného produktu s digitálnymi prvkami, a pokúsiť sa odoslať škodlivé príkazy do produktu s digitálnymi prvkami. Takéto back-endové systémy, ak nie sú navrhnuté a vyvinuté výrobcom alebo na jeho zodpovednosť, alebo ak

nepodporujú jednu z funkcií produktu s digitálnymi prvkami, nepredstavujú riešenia spracovania údajov na diaľku, a preto nespádajú do rozsahu pôsobnosti produktu s digitálnymi prvkami na účely CRA. CRA však vyžaduje, aby výrobca riešil riziko, ktoré môžu predstavovať, prostredníctvom opatrení na úrovni produktu, napríklad vyžadovaním kryptografického overovania príkazov na diaľku, overovaním integrity zmien konfigurácie alebo generovaním protokolov alebo výstrah týkajúcich sa bezpečnosti v prípade zistenia abnormálneho správania. Podobne, ak výrobca zistí riziko vyplývajúce z nedostupnosti takejto externej služby, napríklad v dôsledku výpadkov napájania alebo porúch infraštruktúry, CRA môže vyžadovať zmiernujúce opatrenia na úrovni produktu proti takýmto kybernetickobezpečnostným rizikám, napr. zabezpečenie toho, aby výpadok nespôsobil prechod produktu s digitálnymi prvkami do nezabezpečených stavov. V takýchto prípadoch CRA reguluje, ako produkt s digitálnymi prvkami reaguje na tieto vonkajšie riziká; neukladá povinnosti týkajúce sa organizácie, personálneho obsadenia ani prevádzky back-endovej infraštruktúry, ani túto infraštruktúru nepovažuje za súčasť produktu s digitálnymi prvkami.

170. Povinnosť náležitej starostlivosti sa týka prvkov, ktoré tvoria súčasť samotného produktu s digitálnymi prvkami, najmä integrovaných softvérových alebo hardvérových komponentov dodávaných treťou stranou. Výrobcovia sú povinní prijať primerané opatrenia na zabezpečenie toho, aby takéto komponenty nenarušili súlad produktu s digitálnymi prvkami so základnými požiadavkami. To je možné dosiahnuť len stanovením toho, čo produkt s digitálnymi prvkami vyžaduje od svojich komponentov na splnenie svojich cieľov v oblasti kybernetickej bezpečnosti, a overením na základe posúdenia rizík, či sú tieto komponenty v súlade s potrebami produktu, ako sa uvádza aj v odôvodnení 34.
171. V súlade so svojím posúdením kybernetickobezpečnostných rizík musí výrobca určiť požiadavky, ktoré by mala integrovaná súčiastka spĺňať. Ak sa napríklad produkt s digitálnymi prvkami spolieha na kryptografické funkcie, mechanizmy aktualizácie alebo bezpečnú komunikáciu, ktoré zabezpečuje určitá súčiastka, musí výrobca v rámci svojej náležitej starostlivosti identifikovať tieto potreby a overiť, či ich daná súčiastka spĺňa. Dôkazy na tento účel môžu pozostávať z dokumentácie získanej od výrobcu komponentu, ako sú technické špecifikácie, bezpečnostná dokumentácia alebo príslušná dokumentácia o zhode alebo o zabezpečení. V prípade potreby môže výrobca tiež vykonať testy s cieľom overiť, či tieto komponenty primerane plnia príslušné funkcie. Hoci náležitá starostlivosť predstavuje samostatnú zákonnú povinnosť, podporuje a posilňuje schopnosť výrobcu preukázať súlad so základnými požiadavkami na produkt s digitálnymi prvkami ako celok.
172. Pri posudzovaní rizík pre produkt s digitálnymi prvkami ako celok sa musia v rámci posúdenia kybernetickobezpečnostného rizika zohľadniť prvky mimo produktu, ako sú prvky prostredia, externá infraštruktúra, iné systémy alebo siete, a v prípade potreby sa musia riešiť prostredníctvom opatrení na úrovni produktu s cieľom zabezpečiť súlad produktu s digitálnymi prvkami so základnými požiadavkami. Súčasti, ktoré sú fyzicky alebo logicky integrované do produktu s digitálnymi prvkami, ale pochádzajú od tretej strany, sa musia takisto zohľadniť v rámci posúdenia rizík. Na účely zabezpečenia súladu

by ich však výrobca mal považovať za externé súčasti, ktorých vlastnosti sa overujú prostredníctvom náležitej starostlivosti pri integrácii, keďže výrobca ich pravdepodobne neprepracoval ani nevyvinul nanovo.

173. Rovnaká logika platí aj počas vývoja a integrácie komponentov. Ak výrobca vyvíja funkcionality sám, musí priamo implementovať základné požiadavky. Ak výrobca integruje komponenty vyvinuté inými subjektmi, musí prostredníctvom náležitej starostlivosti zabezpečiť, aby sa tieto komponenty mohli používať spôsobom, ktorý umožňuje, aby produkt s digitálnymi prvkami ako celok spĺňal požiadavky. V oboch prípadoch zostáva cieľ rovnaký: aby produkt s digitálnymi prvkami, tak ako je uvedený na trh, dosiahol primeranú úroveň kybernetickej bezpečnosti, ako to vyžaduje CRA, s prihliadnutím na riziká identifikované v posúdení kybernetickobezpečnostných rizík.

#### 7.4. Opätovné použitie posúdenia rizík a dokumentácie o zhode pre skupiny produktov s digitálnymi prvkami

174. Výrobcovia môžu uvádzať na trh produkty s digitálnymi prvkami, ktoré sú podobné, napríklad rôzne varianty, modely alebo konfigurácie tej istej skupiny produktov. Ak takéto produkty s digitálnymi prvkami majú spoločnú architektúru, návrh relevantný z hľadiska bezpečnosti, zamýšľaného účelu a sú vystavené rovnakým kybernetickobezpečnostným rizikám, CRA nevyžaduje, aby výrobcovia na účely posúdenia rizika a posúdenia zhody zaobchádzali s každým variantom ako s úplne samostatným produktom s digitálnymi prvkami.
175. V takýchto prípadoch, za predpokladu, že všetky príslušné varianty sú primerane pokryté z hľadiska relevantných rizík a základných požiadaviek, sa výrobcovia môžu opierať o:
- i) jedno posúdenie kybernetickobezpečnostného rizika vykonané v súlade s článkom 13 ods. 2 CRA;
  - ii) jeden súbor technickej dokumentácie; a
  - iii) jeden postup posudzovania zhody.

To tiež umožňuje vydanie jedného EÚ vyhlásenia o zhode pre skupinu produktov s digitálnymi prvkami, pokiaľ v ňom sú jasne identifikované varianty produktov, na ktoré sa vzťahuje.

176. Rozhodujúcim faktorom je, či sú rozdiely medzi variantmi relevantné z hľadiska kybernetickej bezpečnosti. Odchýlky, ktoré nemajú vplyv na vlastnosti produktu s digitálnymi prvkami z hľadiska kybernetickej bezpečnosti, ako sú rozdiely vo farbe, tvare, veľkosti pamäte alebo iné charakteristiky, ktoré nie sú relevantné z hľadiska bezpečnosti, nevyžadujú samostatné posúdenia rizík ani posúdenia zhody. Naopak, v niektorých prípadoch sa varianty môžu líšiť spôsobmi, ktoré ovplyvňujú implementáciu základných požiadaviek, napríklad prostredníctvom rôznych komunikačných rozhraní, softvérových balíkov, mechanizmov aktualizácie alebo pripojenia na diaľku. V takýchto prípadoch sa tieto rozdiely musia zohľadniť v posúdení rizika a v prípade potreby aj v posúdení zhody a v technickej dokumentácii.
177. Výrobcovia naďalej nesú zodpovednosť za to, aby posúdenie rizika a súvisiaca dokumentácia presne odrážali produkty s digitálnymi prvkami uvádzané na trh. Ak nový

variant prináša nové kybernetickobezpečnostné riziká alebo mení spôsob implementácie základných požiadaviek, existujúce posúdenie rizika a dokumentácia o zhode musia byť primerane aktualizované. Spoliehanie sa na jedno posúdenie zhody je možné len v rozsahu, v akom produkty s digitálnymi prvkami nevykazujú rozdiely, pokiaľ ide o ich vlastnosti v oblasti kybernetickej bezpečnosti.

## 8. Spracovanie údajov na diaľku

178. Článok 3 ods. 1 CRA definuje produkt s digitálnymi prvkami ako „softvérový alebo hardvérový produkt a jeho riešenia spracovania údajov na diaľku vrátane softvérových alebo hardvérových komponentov, ktoré sa uvádzajú na trh samostatne“. V tomto kontexte musí výrobca posudzovať produkt s digitálnymi prvkami ako celok, vrátane jeho riešení spracovania údajov na diaľku (RDPS). Napríklad pri preukazovaní toho, že produkt s digitálnymi prvkami spĺňa základné požiadavky uvedené v prílohe I, je potrebné zohľadniť riešenia spracovania údajov na diaľku (RDPS), a to už od posúdenia rizika (článok 13 ods. 2). To isté platí pri zohľadňovaní povinností počas životného cyklu, ako je hlásenie aktívne zneužívaných zraniteľností a závažných incidentov (článok 14).
179. Účelom týchto usmernení je poskytnúť výrobcovi ďalšiu podporu pri určovaní, či ich produkt s digitálnymi prvkami obsahuje riešenia spracovania údajov na diaľku (RDPS) v zmysle definície v CRA, a ako splniť svoje povinnosti v súvislosti s dodržiavaním predpisov v tejto oblasti. Po úvodnej analýze definícií a odôvodnení stanovených v CRA budú v týchto usmerneniach uvedené otázky, ktoré pomôžu výrobcovi objasniť, či ich produkt s digitálnymi prvkami obsahuje riešenia spracovania údajov na diaľku (pozri časť 8.1 *Čo sa považuje za riešenie spracovania údajov na diaľku pre produkt s digitálnymi prvkami?*). Následne sa budú podrobne rozoberať technické dôsledky riešení RDPS a spôsob posudzovania súladu so CRA (pozri časť 8.2 *Praktické a technické dôsledky riešení spracovanie údajov na diaľku a spoliehanie sa na riešenia tretích strán*).
180. V zásade článok 3 ods. 2 definuje pojem „spracovanie údajov na diaľku“ ako „spracovanie údajov na diaľku, pre ktoré je softvér navrhnutý a vyvinutý výrobcovi alebo na zodpovednosť výrobcu a ktorého neexistencia by bránila produktu s digitálnymi prvkami plniť jednu z jeho funkcií“. RDPS sa preto definuje ako softvérové prvky („časť elektronického informačného systému, ktorý pozostáva z počítačového kódu“, ako je definované v článku 3 ods. 4) spracovania údajov na diaľku. Jeho zámerom nie je zahrnúť do rozsahu pôsobnosti produktu s digitálnymi prvkami hardvér, na ktorom môže závisieť spracovanie údajov na diaľku.
181. Odôvodnenia 11 a 12 poskytujú ďalšie vysvetlenia o tom, ako by sa mal tento pojem interpretovať. Odôvodnenie 11 objasňuje, že cieľom zahrnutia riešení spracovania údajov na diaľku je, aby „boli takéto produkty primerane a v celom rozsahu zabezpečené ich výrobcami bez ohľadu na to, či sa údaje spracúvajú alebo uchovávajú lokálne na zariadení používateľa alebo na diaľku výrobcovi“. Uvádza sa v ňom tiež, že „požiadavky na riešenia spracovania údajov na diaľku, ktoré patria do rozsahu pôsobnosti tohto nariadenia, preto nezahŕňajú technické, prevádzkové ani organizačné opatrenia zamerané na riadenie rizík pre bezpečnosť sietí a informačných systémov výrobcovi ako celku.“
182. Z odôvodnenia č. 11 teda vyplýva, že zámerom nie je, aby sa požiadavky CRA vzťahovali na celú IT infraštruktúru organizácie, ale len na softvérové komponenty, ktoré umožňujú vykonávanie riešenia na spracovanie údajov. Napríklad interné systémy týkajúce sa vlastných ľudských zdrojov výrobcu, mzdového účtovníctva, riadenia vzťahov so zákazníkmi, procesov nepretržitej integrácie/nepretržitého dodávania (CI/CD) alebo distribúcie bezpečnostných aktualizácií do okrajových lokalít by sa nemali

považovať za riešenia spracovania údajov na diaľku (RDPS). Podobne systémy spojené s audítorskými a testovacími činnosťami, ako sú penetračné testovanie, vyhľadávanie hrozieb a red teaming, sú mimo rozsahu pôsobnosti produktu s digitálnymi prvkami, na ktorý sa vzťahuje CRA. Je dôležité poznamenať, že hoci vykonávanie účinných a pravidelných testov a preskúmaní bezpečnosti produktu s digitálnymi prvkami je základnou požiadavkou stanovenou v bode (3) časti II prílohy I k CRA, neznamená to, že takéto činnosti sa majú považovať za RDPS pre produkt s digitálnymi prvkami.

183. Odôvodnenie 12 sa zameriava na cloudové služby a podrobne rozoberá okolnosti, za ktorých by sa cloudové služby mohli považovať za RDPS. Odôvodnenie na záver pripomína, že služby cloud computingu a modely cloudových služieb spadajú do rozsahu pôsobnosti smernice (EÚ) 2022/2555 (NIS 2)<sup>28</sup>, ktorá stanovuje požiadavky na riadenie kybernetickobezpečnostných rizík pre poskytovateľov služieb cloud computingu. Tieto požiadavky sú ďalej špecifikované vykonávacím nariadením Komisie (EÚ) 2024/2690<sup>29</sup>.

## 8.1. Čo sa považuje za riešenie spracovania údajov na diaľku v prípade produktu s digitálnymi prvkami?

184. Definícia spracovania údajov na diaľku stanovená v článku 3 ods. 2 sa teda opiera o tri prvky:
- i) či sa spracovanie údajov vykonáva „na diaľku“;
  - ii) či by absencia takéhoto spracovania údajov zabránila produktu s digitálnymi prvkami plniť jednu z jeho funkcií; a
  - iii) či je softvér navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť.
- Nasledujúce tri podsekcie sa podrobnejšie zaoberajú každým z týchto prvkov.

### 8.1.1. Pojem „na diaľku“

185. Pojem „na diaľku“, na ktorý sa odvoláva článok 3 ods. 2, je relevantný, ale nestačí na určenie, či produkt s digitálnymi prvkami zahŕňa RDPS. Vzhľadom na rozmanitosť riešení, ktoré by mohli spadať pod tento pojem, navyše nie je možné poskytnúť vyčerpávajúcu definíciu pojmu „na diaľku“. Je potrebné, aby výrobca posúdil každý prípad individuálne.
186. V odôvodnení č. 11 CRA sa spomínajú údaje spracúvané alebo ukladané „na diaľku výrobcom“ na rozdiel od údajov spracúvaných alebo ukladaných „lokálne na zariadení používateľa“. Spracúvanie údajov na diaľku sa zvyčajne uskutočňuje mimo

---

<sup>28</sup> Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Únii, ktorou sa mení a dopĺňa nariadenie (EÚ) č. 910/2014 a smernicu (EÚ) 2018/1972 a ktorou sa zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2), Ú. v. EÚ L 333, 27.12.2022, s. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/2022-12-27>.

<sup>29</sup> Vykonávacie nariadenie Komisie (EÚ) 2024/2690 zo 17. októbra 2024, ktorým sa stanovujú pravidlá na uplatňovanie smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia riadenia kybernetickobezpečnostných rizík a ďalšie špecifikovanie prípadov, v ktorých sa incident považuje za významný, pokiaľ ide o poskytovateľov služieb DNS, registrov názvov TLD, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátových centier, poskytovateľov sietí na doručovanie obsahu, poskytovateľov spravovaných služieb, poskytovateľov spravovaných bezpečnostných služieb, poskytovateľov online trhovísk, online vyhľadávačov a platforiem sociálnych sietí, ako aj poskytovateľov dôveryhodných služieb, Ú. v. EÚ L, 2024/2690, 18.10.2024, ELI: [http://data.europa.eu/eli/reg\\_impl/2024/2690/oj](http://data.europa.eu/eli/reg_impl/2024/2690/oj).

používateľského prostredia produktu s digitálnymi prvkami alebo mimo prevádzkového prostredia organizácie (v prípade profesionálneho používateľa). To však nebráni tomu, aby sa spracúvanie uskutočňovalo aj v blízkosti zariadenia („na okraji“). Prenos údajov môže byť káblový (napr. ethernetový kábel) alebo bezdrôtový (napr. Wi-Fi, Bluetooth). Cloud computing, vrátane edge computingu, je typickým príkladom spracovania údajov prebiehajúceho „na diaľku“. Napríklad v prípade cloudovej funkcie, ku ktorej má používateľ prístup z mobilnej aplikácie, sa časť spracovania údajov uskutočňuje v cloude, mimo prostredia používateľa.

187. Je dôležité poznamenať, že riešenia spracovania údajov na diaľku (RDPS) nemusia byť nevyhnutne prevádzkované na cloudovej infraštruktúre tretej strany. Spracovanie údajov na diaľku bežiacie na lokálnych serveroch v priestoroch výrobcu môže tiež predstavovať RDPS. Inými slovami, riešenie prevádzkované v lokálnych priestoroch a v súkromnom cloude sa môže rovnako kvalifikovať ako RDPS ako riešenie prevádzkované vo verejnom cloude a mimo lokálnych priestorov.
188. Dve rozhodujúce a kumulatívne otázky, ktoré určujú, či spracovanie údajov spadá pod CRA ako riešenie spracovania údajov na diaľku, sú uvedené nižšie v oddieloch 8.1.2 a 8.2. Ak je odpoveď na obe otázky kladná, spracovanie údajov na diaľku spĺňa podmienky pre RDPS.

#### 8.1.2. Zabránila by absencia takéhoto spracovania údajov tomu, aby produkt s digitálnymi prvkami plnil jednu zo svojich funkcií?

189. Ako sa stanovuje v definícii pojmu „spracovanie údajov na diaľku“ uvedenej v článku 3 ods. 2, aby sa spracovanie údajov na diaľku kvalifikovalo ako RDPS, jeho absencia by musela zabrániť produktu s digitálnymi prvkami vykonávať jednu z jeho funkcií. Pojem „funkcie“ uvedený v tejto definícii nie je obmedzený na „základnú funkcionality“ alebo „zamýšľaný účel“ produktu s digitálnymi prvkami, keďže CRA takéto obmedzenie nestanovuje. Funkcie v rozsahu pôsobnosti CRA zahŕňajú jednak funkcie, ktoré priamo naplňujú zamýšľaný účel produktu s digitálnymi prvkami tak, ako ho vnímajú používatelia, a jednak funkcie, ktoré podporujú celkový výkon produktu.
190. Príklady funkcií, pri ktorých môže dochádzať k spracovaniu údajov na diaľku a ktoré by bránili produktu s digitálnymi prvkami vo vykonávaní jednej z jeho funkcií, zahŕňajú:
  - i) odosielanie príkazov do zariadenia;
  - ii) synchronizáciu súborov;
  - iii) registráciu používateľa;
  - iv) konfiguráciu (personalizáciu produktu s digitálnymi prvkami);
  - v) automatizovanú distribúciu aktualizácií, vrátane aktualizácií prvkov a bezpečnostných záplat;
  - vi) správu identít a prístupu.
191. V niektorých prípadoch môže používateľ funkciu využívať aj na diaľku, aj manuálne (napr. zapnutie žiarovky prostredníctvom aplikácie alebo manuálne). Existencia tejto možnosti nevyklučuje kvalifikáciu spracovania údajov súvisiaceho so vykonávaním funkcie na diaľku ako RDPS. Vykonávanie tejto funkcie na diaľku sa tiež považuje za súčasť funkcií, ktoré produkt s digitálnymi prvkami ponúka.

192. Naopak, ak absencia určitého spracovania údajov nebráni produktu s digitálnymi prvkami vo vykonávaní jednej z jeho funkcií, takéto spracovanie sa nepovažuje za RDPS v zmysle CRA. Patrí sem napríklad analýza telemetrických údajov na diaľku zhromaždených výlučne na štatistické účely alebo na účely budúceho vývoja produktu.
193. Avšak aj v prípade, že spracovanie údajov nepodporuje funkciu produktu s digitálnymi prvkami, výrobcovia môžu musieť zvážiť, či tieto komponenty na diaľku prinášajú riziko pre produkt s digitálnymi prvkami v rámci posúdenia kybernetickobezpečnostného rizika (napr. s ohľadom na prevádzkové prostredie produktu) a primerane tieto riziká zmierniť (napr. prostredníctvom opatrení na úrovni produktu).
194. Webové stránky predstavujú špecifický prípad, ktorý si zaslúži ďalšie objasnenie, ako sa vysvetľuje aj v *oddiele 2.1 Uvedenie na trh*. Webové stránky nespádajú do rozsahu pojmu RDPS, ak nepodporujú funkciu produktu s digitálnymi prvkami, ako sa vysvetľuje v odôvodnení 11 CRA. Na to, aby sa webová stránka považovala za spadajúcu do rozsahu pojmu RDPS, nestačí, aby obsahovala informácie o produkte s digitálnymi prvkami, a to ani v prípade, že produkt presmeruje na takúto webovú stránku. Napríklad presmerovanie používateľov na externú webovú stránku, ktorá poskytuje používateľom informácie a pokyny, nie je RDPS. Naopak, webová stránka môže spadať do rozsahu pojmu RDPS, ak umožňuje alebo podporuje funkciu produktu s digitálnymi prvkami. Napríklad autentifikačný portál, ktorý vydáva poverenia alebo tokeny potrebné na prevádzku produktu s digitálnymi prvkami, by sa považoval za RDPS (za predpokladu, že sú splnené aj ostatné kritériá definície).

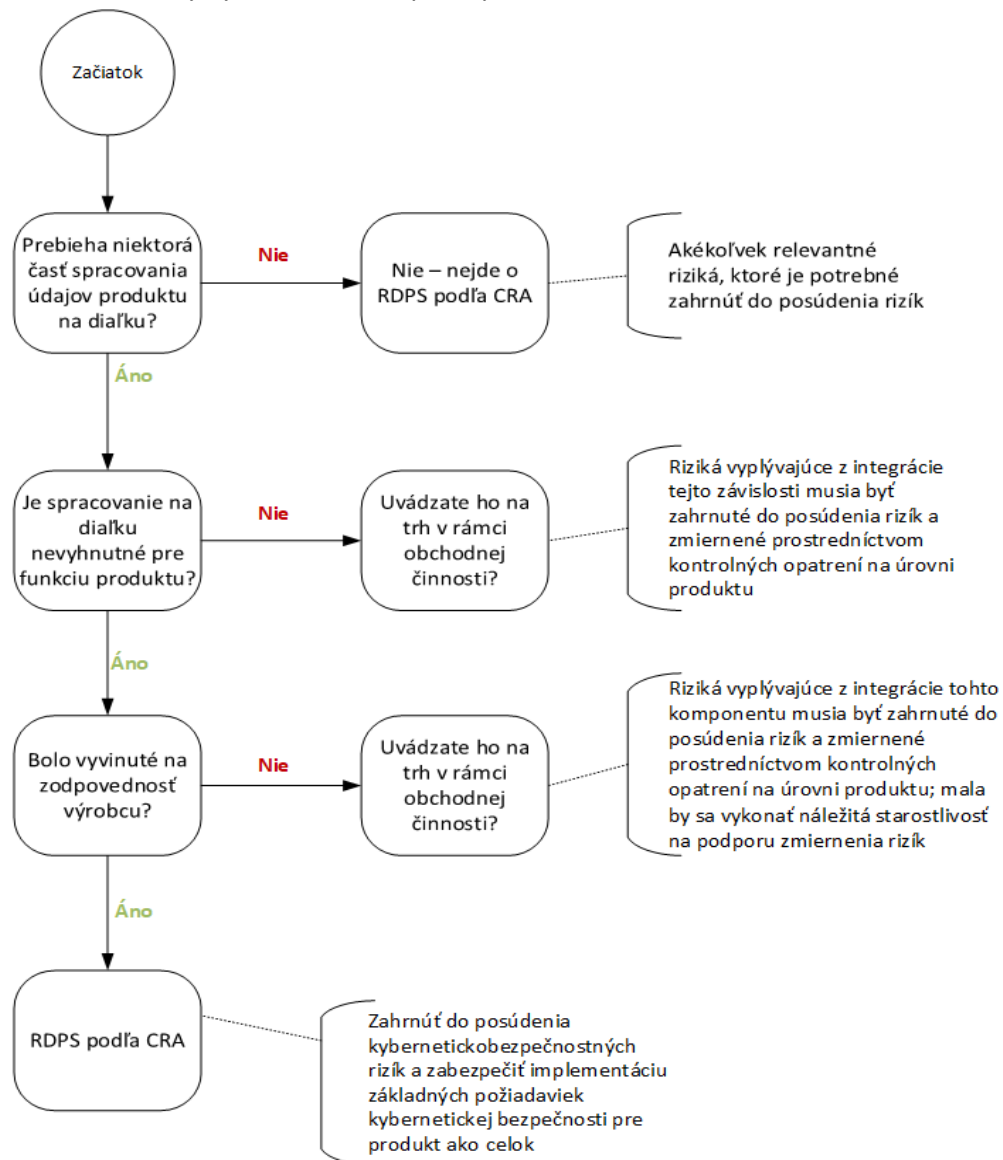
### 8.1.3. Bol softvér navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť?

195. Definícia „spracovania údajov na diaľku“ v článku 3 ods. 2 CRA ďalej špecifikuje, že softvér takéhoto spracovania údajov na diaľku musí byť navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť. Spracovanie údajov na diaľku, ktoré bolo v plnom rozsahu vyvinuté a navrhnuté výrobcom (interné), by sa prirodzene kvalifikovalo ako RDPS. To by platilo aj v prípade, ak by sa výrobcovia pri vývoji a návrhu riešenia spoliehali na externého poskytovateľa služieb (t. j. „na jeho zodpovednosť“). Výraz „pod zodpovednosťou výrobcu“ sa vzťahuje na riešenia spracovania na diaľku, ktoré sú šité na mieru pre výrobcu. Ide o prípady, keď výrobca nezískava iba licenciu na existujúci produkt s digitálnymi prvkami alebo službu, ktorú poskytovateľ služieb ponúka svojim zákazníkom, alebo na ich mierne upravené verzie. „Pod zodpovednosťou výrobcu“ znamená, že softvér je vytvorený výlučne výrobcom alebo v jeho mene na základe návrhov a špecifikácií, ktoré poskytol.
196. Pri chápaní RDPS nie je pojem „kto riešenie prevádzkuje“ rozhodujúcim faktorom, keďže definícia CRA sa vzťahuje iba na návrh a vývoj RDPS. To je v súlade s prístupom CRA, podľa ktorého sa požiadavky a povinnosti vzťahujú na výrobcov, a nie na prevádzku produktu s digitálnymi prvkami. Ak výrobcovia navrhujú a vyvíjajú riešenia, ktoré následne prevádzkuje tretia strana, naďalej nesú zodpovednosť za splnenie základných požiadaviek CRA na produkt s digitálnymi prvkami, ktorý uvádzajú na trh.
197. Je potrebné rozlišovať medzi prípadmi, keď návrh a vývoj vykonávajú výrobcovia (alebo sa vykonávajú pod ich zodpovednosťou), a prípadmi, keď sa využívajú riešenia tretích

strán, ktoré neboli navrhnuté a vyvinuté výrobcami (alebo pod ich zodpovednosťou). Ako príklad je užitočné zvážiť najbežnejšie modely cloudových služieb, ktoré poskytujú rôznu stupeň kontroly zo strany používateľa a ktoré sú uvedené aj v odôvodnení 12 CRA, a to konkrétne „Software as a Service“ (SaaS), „Platform as a Service“ (PaaS) a „Infrastructure as a Service“ (IaaS).

198. V prípade riešenia IaaS od tretej strany výrobca nespravuje ani nekontroluje základné fyzické a virtuálne zdroje (napríklad základný hardvér a hypervízor poskytovateľa cloudových služieb), ale je schopný nasadzovať a prevádzkovať ľubovoľný softvér s využitím týchto zdrojov, ako sú operačné systémy a aplikácie. Takýto softvér navrhuje a vyvíja výrobca alebo sa tak deje na jeho zodpovednosť, a preto sa môže kvalifikovať ako RDPS (ak spĺňa ostatné prvky definície).
199. V prípade riešenia PaaS od tretej strany výrobca nasadí svoju vlastnú (vytvorenú alebo nadobudnutú) aplikáciu s využitím programovacích jazykov a prostredí na spúšťanie poskytnutých poskytovateľom cloudových služieb a integruje túto aplikáciu do svojho produktu spolu s digitálnymi prvkami. Výrobca má kontrolu nad aplikáciou a prípadne aj nad konfiguračnými nastaveniami prostredia na spúšťanie. Aplikáciu teda navrhuje a vyvíja výrobca alebo sa tak deje na jeho zodpovednosť, a preto sa môže kvalifikovať ako RDPS (ak spĺňa ostatné prvky definície).
200. V prípade riešenia SaaS od tretej strany poskytovateľ SaaS ponúka výrobcovi plne vyvinutú aplikáciu, ktorá sa má integrovať do produktov výrobcu spolu s digitálnymi prvkami. Výrobca má obmedzenú schopnosť spravovať nastavenia konfigurácie aplikácie špecifické pre jednotlivých používateľov. Aplikácia preto nie je navrhnutá a vyvinutá výrobcou ani na jeho zodpovednosť.
201. Ak však určité prvky nespĺňajú kritériá na zaradenie medzi RDPS (napr. hypervízor v prípade infraštruktúry IaaS od tretej strany, operačný systém v prípade riešenia PaaS od tretej strany alebo aplikácia SaaS od tretej strany), ale sú integrované do produktu s digitálnymi prvkami spôsobom, ktorý ovplyvňuje jeho bezpečnosť, mali by sa takéto riešenia považovať za podobné komponentom od tretej strany. Výrobca je povinný identifikovať a posúdiť riziká spojené s integráciou týchto prvkov a riešiť ich implementáciou základných požiadaviek na samotný produkt s digitálnymi prvkami. V príslušných prípadoch to môžu podporovať bezpečnostné funkcie, ktoré poskytovateľ cloudových služieb sprístupňuje prostredníctvom svojho modelu zdieľanej zodpovednosti, pričom výrobca tieto funkcie využíva alebo konfiguruje na riešenie identifikovaných rizík. Okrem toho sa od výrobcu očakáva, že bude plniť povinnosť podobnú povinnosti vykonávať náležitú starostlivosť uvedenej v článku 13 ods. 5 v súvislosti s bezpečnosťou týchto komponentov spôsobom, ktorý je primeraný riziku, ktoré riešenie na diaľku predstavuje pre bezpečnosť produktu s digitálnymi prvkami.
202. Preto možno zhrnúť, že:
  - a. Aby sa spracovanie údajov mohlo považovať za RDPS, odpoveď na obe otázky uvedené v oddieloch 8.1.2 „Zabránila by absencia takéhoto spracovania údajov tomu, aby produkt s digitálnymi prvkami plnil jednu zo svojich funkcií?“ a 8.1.3 „Bol softvér navrhnutý a vyvinutý výrobcou alebo na jeho zodpovednosť?“ musí byť kladná.

- b. Ak je odpoveď na otázku v oddiele 8.1.2 „Zabránilo by chýbanie takéhoto spracovania údajov produktu s digitálnymi prvkami vykonávať jednu z jeho funkcií?“ záporná, výrobcovia by mali v rámci svojho posúdenia rizík posúdiť riziká vyplývajúce z existencie takéhoto spracovania údajov.
- c. Ak je odpoveď na otázku v bode 8.1.2 „Zabránilo by absencia takéhoto spracovania údajov tomu, aby produkt s digitálnymi prvkami plnil jednu zo svojich funkcií?“ kladná, ale odpoveď na otázku v bode 8.1.3 „Bol softvér navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť?“ je záporná, výrobcovia by mali riešenie tretej strany považovať za komponent. V rámci posúdenia rizík by výrobcovia mali posúdiť riziká vyplývajúce z integrácie takéhoto riešenia a primerane ich zmierniť. Okrem toho by výrobcovia mali postupovať s náležitou starostlivosťou.



Obrázok 9: Štylizovaný diagram na určenie, či produkt s digitálnymi prvkami obsahuje RDPS

## 8.2. Praktické a technické dôsledky riešení spracovania údajov na diaľku a spoliehania sa na riešenia tretích strán

203. CRA sa riadi prístupom založeným na riziku, ktorý je zakotvený v článku 13 ods. 2 a 3,

ako aj v prvej základnej požiadavke časti I prílohy I, podľa ktorej „produkty s digitálnymi prvkami sa navrhujú, vyvíjajú a vyrábajú tak, aby sa zaistila primeraná úroveň ich kybernetickej bezpečnosti voči rizikám“. V dôsledku toho by sa mal pri uplatňovaní požiadaviek CRA na RDPS a pri riešení rizík vyplývajúcich zo služieb tretích strán integrovaných do produktu s digitálnymi prvkami zohľadniť prístup založený na riziku.

204. Po prvé, výrobcovia by mali:

- i) v technickej dokumentácii uviesť, že ich produkt s digitálnymi prvkami obsahuje RDPS alebo využíva riešenia na diaľku tretích strán, a
- ii) opísať takéto riešenia. Ak ten istý RDPS podporuje viacero produktov s digitálnymi prvkami, je potrebné tento RDPS uviesť v technickej dokumentácii každého produktu. Dokumentáciu týkajúcu sa RDPS, ktorý slúži viacerým produktom s digitálnymi prvkami, je možné opätovne použiť pri posudzovaní zhody jedného produktu na druhý.

205. Ako sa uvádza v odôvodnení 11, systémy RDPS, ktoré sú súčasťou produktu s digitálnymi prvkami a na ktoré sa preto vzťahuje posudzovanie zhody produktu, by sa mali obmedziť len na tie softvérové moduly, ktoré sú zodpovedné za funkcionality produktu s digitálnymi prvkami, a na rozhrania, ktoré tieto moduly používajú s externými službami. Ďalšie back-endové systémy, ktoré vykonávajú následné spracovanie a s ktorými produkt s digitálnymi prvkami priamo neinteraguje, sa nepovažujú za systémy RDPS.

206. Tieto back-endové systémy však naďalej predstavujú externé závislosti, ktoré sa musia posúdiť v rámci posúdenia kybernetickobezpečnostného rizika a zmierniť prostredníctvom opatrení na úrovni produktu. Posúdenie rizík vykonávané výrobcom by malo v skutočnosti zohľadňovať:

- i) riziká súvisiace s RDPS;
- ii) riziká súvisiace so spoliehaním sa na riešenia tretích strán na diaľku (podobne ako v prípade komponentov tretích strán); a
- iii) riziká súvisiace s prostredím produktu (napr. základný hardvér).

Výrobcovia by mali zaviesť bezpečnostné kontroly na samotnom produkte s digitálnymi prvkami s cieľom zmierniť tieto riziká.

207. Okrem toho v rámci posudzovania zhody a/alebo plnenia povinností náležitej starostlivosti súvisiacich so službami tretích strán na diaľku možno na podporu posúdenia výrobcu opätovne použiť nasledujúci neúplný zoznam dokladov o zabezpečení:

- a. dôkaz o splnení povinností podľa vykonávacieho nariadenia Komisie (EÚ) 2024/2690;
- b. doklad o splnení povinností vyplývajúcich z nariadenia (EÚ) 2022/2554 (DORA);
- c. vyhlásenie o zhode alebo certifikát získané/ý v rámci európskej schémy certifikácie kybernetickej bezpečnosti (prijatej na základe nariadenia (EÚ) 2019/881 – akt o kybernetickej bezpečnosti);
- d. dôkaz o zhode s normou ISO/IEC 27017:2015 alebo ISO/IEC 27001:2022.

208. Nakoniec, pri interakciách s tretími stranami poskytujúcimi služby na diaľku musia výrobcovia zaviesť najvhodnejšie bezpečnostné opatrenia na základe svojho posúdenia

rizík (a v prípade potreby s podporou modelu zdieľanej zodpovednosti poskytovateľa). Tieto zmiernujúce opatrenia by mali zahŕňať bezpečnostné kontroly ich produktov s digitálnymi prvkami a overovanie bezpečnostných opatrení poskytovaných samotnými tretími stranami (náležitá starostlivosť). Nástrojom na zmiernenie takýchto rizík môže byť začlenenie bezpečnostných záruk do zmlúv o úrovni služieb (SLA) s tretími stranami, vrátane záruky, že poskytovatelia primerane riešia zraniteľnosti. Významná zmena v riešeníach poskytovaných tretími stranami poskytujúcimi služby na diaľku by sa nemala považovať za podstatnú úpravu produktu s digitálnymi prvkami, keďže tieto prvky nespádajú do zodpovednosti výrobcu. V rámci svojich povinností náležitej starostlivosti a s cieľom správne zmierniť riziká vyplývajúce z využívania tretích strán sa však výrobcom odporúča, aby zabezpečili, že ich tretie strany poskytujúce cloudové služby ich primerane informujú o zmenách, ktoré zavádzajú do svojich riešení. Na základe týchto informácií môže byť potrebné, aby výrobcovia revidovali svoje posúdenie rizík. Aktualizované posúdenie rizík by malo zohľadňovať, či poskytovatelia služieb tretích strán naďalej poskytujú dostatočné záruky v oblasti kybernetickej bezpečnosti a či bezpečnostné opatrenia na úrovni produktu sú stále primerané. V niektorých prípadoch môže byť potrebné, aby výrobcovia upravili takéto opatrenia alebo zmenili poskytovateľov služieb tretích strán.

### 8.3. Príklady použitia riešení spracovania údajov na diaľku

S cieľom poskytnúť výrobcom ďalšie praktické usmernenia, táto časť predstavuje sériu fiktívnych prípadov použitia, ktoré opisujú typické produkty s digitálnymi prvkami, ktoré sa spoliehajú na spracovanie údajov na diaľku, a ilustrujú, či sa takéto spracovanie kvalifikuje ako riešenia spracovania údajov na diaľku v zmysle CRA.

#### 8.3.1. Aplikácia pre mobilné bankovníctvo

Finančná inštitúcia uvádza na trh aplikáciu pre mobilné bankovníctvo. Back-endové systémy aplikácie podporujú okrem iného autentizáciu, autorizáciu, správu účtov a platby. Finančná inštitúcia využíva hybridnú stratégiu, ktorá sa opiera o internú infraštruktúru, ako aj o riešenia tretích strán na diaľku na podporu funkcionality aplikácie. Patria medzi ne:

*Vlastná infraštruktúra vyvinutá finančnou inštitúciou:*

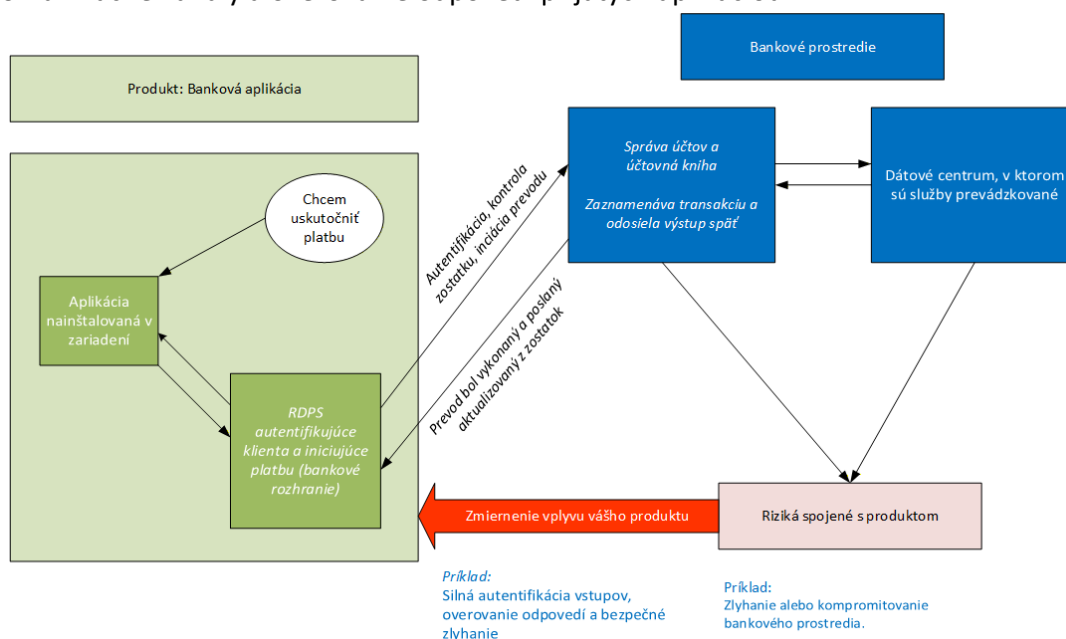
- Zákazník otvorí mobilnú bankovú aplikáciu a je overený prostredníctvom bankového rozhrania, vlastného riešenia vyvinutého finančnou inštitúciou, ktoré prijíma požiadavky aplikácie a vracia príslušné odpovede. Bankové rozhranie overí totožnosť zákazníka dotazom na systém správy účtov a udelí prístup k aplikácii.
- Zákazník iniciuje prevod prostredníctvom aplikácie. Aplikácia odošle pokyn do bankového rozhrania, ktoré odošle príslušnú požiadavku do systému účtovnej knihy.
- Systém správy účtov a systém účtovnej knihy, ktoré sú síce vlastné, ale logicky oddelené od bankového rozhrania, zaznamenajú transakciu.
- Účtovný systém vráti stav transakcie do bankového rozhrania, ktoré výsledok zobrazí zákazníkovi.

*Dôsledky pre RDPS:*

- Bankové rozhranie je nevyhnutné na to, aby aplikácia mohla vykonávať svoje funkcie, a to

overovanie totožnosti zákazníka, odosielanie pokynov zákazníka vrátane platobných a prevodných pokynov a vrátenie výsledného stavu. Bankové rozhranie je navrhnuté a vyvinuté na zodpovednosť výrobcu. Keďže odpoveď na obe otázky uvedené v predchádzajúcich častiach je kladná, bankové rozhranie sa má považovať za RDPS. Musí sa preto zahrnúť do posúdenia kybernetickobezpečnostného rizika a do implementácie základných požiadaviek na produkt s digitálnymi prvkami ako celok. Následné spracovanie pokynu po jeho odoslaní, konkrétne zaznamenávanie transakcie v systémoch správy účtov a účtovných kníh, zúčtovanie a clearing, vykonávajú systémy, s ktorými aplikácia priamo nekomunikuje, a na tomto základe nepredstavuje systém RDPS.

- Systém správy účtov a systém hlavnej knihy sa v prípade bankovej aplikácie nepovažujú za RDPS. Aplikácia s nimi priamo nekomunikuje (komunikuje namiesto toho s bankovým rozhraním, ktoré sa na ne zase spolieha). Hoci ich dostupnosť môže byť nevyhnutná na vykonanie určitej funkcie, CRA sa vzťahuje len na tie časti systému, ktoré priamo komunikujú s produktom s digitálnymi prvkami. Pre účely CRA preto nespádajú pod definíciu RDPS. Tieto systémy však naďalej predstavujú externé závislosti, ktoré môžu pre produkt s digitálnymi prvkami predstavovať významné kybernetickobezpečnostné riziká. Napríklad kompromitácia systému účtovnej knihy by mohla útočníkovi umožniť ovplyvniť výsledky transakcií, ktoré sa následne zobrazujú v aplikácii. Výrobca je preto povinný identifikovať a posúdiť tieto riziká v rámci posúdenia kybernetickobezpečnostného rizika a zmierniť ich prostredníctvom opatrení na úrovni produktu, ako je silná autentifikácia back-endových rozhraní, ochrana integrity transakčných údajov, zabezpečené komunikačné kanály a overovanie odpovedí prijatých aplikáciou.



Obrázok 10: Štylizované znázornenie bankovej aplikácie využívajúcej RDPS

*SaaS od tretej strany pre zákaznícku podporu:*

- Finančná inštitúcia integruje do svojej aplikácie riešenie chatu pre zákaznícku podporu, ktoré vyvinul a prevádzkuje tretí poskytovateľ; tento tretí poskytovateľ napísal kód chatového servera, vytvoril používateľské rozhranie a prevádzkuje infraštruktúru, v ktorej je chat nasadený (t. j. model SaaS).

- Keď zákazník iniciuje žiadosť o podporu, aplikácia ho pripojí k službe tretej strany s cieľom nadviazať chatovú reláciu a spracovať tok správ, pričom tretej strane neposkytuje prístup k základným bankovým systémom.

*Dôsledky pre RDPS:*

- Riešenie podporného chatu je nevyhnutné na to, aby produkt s digitálnymi prvkami mohol plniť jednu zo svojich funkcií, nie je však navrhnuté ani vyvinuté finančnou inštitúciou, ani nie je pod jej zodpovednosťou; preto sa nejedná o RDPS. Malo by sa však s ním zaobchádzať ako s komponentom tretej strany.
- Spoliehanie sa na túto službu tretej strany môže pre bankovú aplikáciu predstavovať kybernetickobezpečnostné riziká, napríklad ak by útočník využil chatový kanál na vydávanie sa za banku alebo na doručovanie škodlivého obsahu používateľom. Finančná inštitúcia musí tieto riziká zohľadniť vo svojom posúdení kybernetickobezpečnostných rizík a zmierniť ich prostredníctvom opatrení na úrovni produktu, ako je izolácia funkcie chatu od kľúčových bankových prvkov, kontrola tokov údajov a overovanie obsahu. Mala by sa tiež vykonať náležitá starostlivosť vo vzťahu k službe SaaS.

### 8.3.2. Inteligentný termostat

Inteligentný termostat umožňuje používateľom regulovať teplotu v ich domácnostiach prostredníctvom mobilnej aplikácie. Mobilná aplikácia a inteligentný termostat využívajú spracovanie údajov na diaľku na výmenu údajov (napr. požiadavku na zvýšenie teploty) a ukladanie údajov (napr. preferencií používateľa). Tieto funkcie boli vyvinuté a navrhnuté pod zodpovednosťou výrobcu, ale bežia na základnej fyzickej a virtuálnej infraštruktúre poskytovanej treťou stranou (IaaS tretej strany).

Keďže inteligentný termostat by bez tohto spracovania údajov na diaľku nebol schopný vykonávať svoje inteligentné funkcionality, jeho absencia by zabránila produktu s digitálnymi prvkami vykonávať jednu alebo viaceré z jeho funkcií. Okrem toho bol softvér vyvinutý a navrhnutý pod zodpovednosťou výrobcu inteligentného termostatu. Spracovanie údajov na diaľku sa preto kvalifikuje ako RDPS v zmysle definície v CRA.

Na účely splnenia požiadaviek CRA musí výrobca inteligentného termostatu zdokumentovať RDPS, ako aj využívanie IaaS tretej strany v technickej dokumentácii produktu s digitálnymi prvkami, vrátane podrobností o zmluvne dohodnutej službe. Výrobca musí zohľadniť tieto prvky pri posudzovaní rizík, ktoré zahŕňa zamýšľaný účel a odôvodnene predvídateľné použitie produktu s digitálnymi prvkami. Výrobca implementuje základné požiadavky CRA na základe rizík spojených so systémom RDPS. Pokiaľ ide o IaaS tretej strany, výrobca musí zabezpečiť, aby bezpečnostné opatrenia poskytované tretím poskytovateľom boli primerané, a/alebo prijať príslušné opatrenia vo vzťahu k infraštruktúre. V prvom prípade by výrobca mohol napríklad požiadať o dôkaz, že boli splnené povinnosti vyplývajúce z smernice NIS 2.

### 8.3.3. Čítačka e-knín

Výrobca softvéru pre čítačku e-knín využíva úložnú službu SaaS tretej strany na ukladanie elektronických kníh zakúpených zákazníkmi a na umožnenie prístupu k týmto knihám. Chýbajúca úložná služba by zabránila produktu s digitálnymi prvkami plniť jednu z jeho funkcií, avšak úložná služba SaaS tretej strany nie je vyvinutá výrobcom ani nie je v jeho zodpovednosti; poskytovateľ SaaS ju sprístupňuje zákazníkovi na akékoľvek použitie.

Služba úložiska typu SaaS nespĺňa definíciu RDPS. Výrobca čítačky e-knžíh sa však pri fungovaní svojho produktu s digitálnymi prvkami spolieha na túto externú službu, a preto musí pri posudzovaní kybernetickobezpečnostných rizík zohľadniť súvisiace riziká. Výrobca čítačky e-knžíh by mal so službou SaaS zaobchádzať ako s komponentom. Výrobca musí zaviesť primerané bezpečnostné opatrenia na úrovni produktu, ako je bezpečná autentifikácia, šifrovanie a ochrana integrity komunikácie so službou úložiska. Náležitá starostlivosť pri výbere a integrácii poskytovateľa služby SaaS tiež prispieje k plneniu povinností výrobcu, aby produkt s digitálnymi prvkami ako celok mohol spĺňať základné požiadavky.

#### 8.3.4. Priemyselný robot

Úlohou priemyselného robota je uchopovať diely. Robot odosiela informácie získané prostredníctvom kamier do služby na diaľku, ktorú navrhol a vyvinul výrobca. Táto služba beží na základnej fyzickej a virtuálnej infraštruktúre poskytovanej tretím poskytovateľom služieb (IaaS tretej strany). Cloudová služba vypočíta polohu dielu na základe záznamov z kamier a odosiela späť do robota príkazy na uchopenie dielov.

Bez tohto spracovania údajov by priemyselný robot nemohol vyberať diely, a teda by nemohol plniť jednu zo svojich funkcií. Okrem toho softvér bežiaci na tejto infraštruktúre navrhol a vyvinul výrobca. Softvér navrhnutý a vyvinutý výrobcou spĺňa definíciu RDPS.

Výrobca priemyselného robota musí v technickej dokumentácii produktu s digitálnymi prvkami zdokumentovať systém RDPS, ako aj využívanie IaaS tretej strany (vrátane podrobností o zmluvne dohodnutej službe). Výrobca musí tieto prvky zohľadniť aj pri posudzovaní rizík, ktoré zahŕňa zamýšľaný účel a odôvodnene predvídateľné použitie produktu s digitálnymi prvkami. Výrobca implementuje základné požiadavky CRA na produkt s digitálnymi prvkami, vrátane jeho RDPS, na základe rizík. Povinnosti výrobcu podporí aj náležitá starostlivosť pri výbere poskytovateľa IaaS. Výrobca by napríklad mohol požiadať o dôkaz, že boli splnené povinnosti vyplývajúce z smernice NIS 2.

#### 8.3.5. Mobilná sieť

Smartfón využíva sieť 5G na poskytovanie internetového pripojenia, telefonických hovorov a správ svojim používateľom (mobilná konektivita). Mobilnú sieť vyvíjajú a navrhujú telekomunikační operátori. Sieť pozostáva z malých buniek a vysielačích veží, ako aj ďalších sieťových zariadení.

Produkt s digitálnymi prvkami by mal byť schopný správne sa pripojiť k sieti; to je jedna z jeho funkcií. Skutočnosť, či je táto sieť v prevádzke alebo nie, však nie je relevantná pre posúdenie, či produkt s digitálnymi prvkami funguje správne. Sieť je iba komunikačným kanálom a nie je nevyhnutná na to, aby produkt s digitálnymi prvkami plnil svoju funkciu „správneho pripojenia k sieti“. Podobne sa ethernetový kábel, smerovač alebo signál Wi-Fi nepovažujú za spracovanie údajov, ktorých absencia by bránila produktu s digitálnymi prvkami vo vykonávaní jednej z jeho funkcií, ale skôr za prostriedok umožňujúci komunikáciu/pripojenie.

V dôsledku toho mobilná sieť nespĺňa definíciu RDPS. Sieť by sa nemala považovať za komponent tretej strany, keďže do produktu s digitálnymi prvkami nie je integrovaný žiadny softvér, produkt sa namiesto toho iba spolieha na túto sieť. Ako také nie je potrebné, aby výrobca plnil povinnosti náležitej starostlivosti voči poskytovateľovi siete.

## 9. Ďalšie prvky

### 9.1. Oznamovacie povinnosti

209. Podľa článku 14 ods. 1 a 3 CRA je výrobca povinný súčasne oznámiť CSIRT určenému ako koordinátorovi a agentúre ENISA:
- i) akúkoľvek aktívne zneužívanú zraniteľnosť obsiahnutú v jeho produkte s digitálnymi prvkami, o ktorej sa dozvie; a
  - ii) akýkoľvek závažný incident s dopadom na bezpečnosť produktu s digitálnymi prvkami, o ktorom sa dozvie.
210. V súlade s článkom 69 ods. 3 a článkom 71 ods. 2 druhou vetou sa povinnosť dodržiavať článok 14 uplatňuje od 11. septembra 2026 na všetky produkty s digitálnymi prvkami, ktoré spadajú do pôsobnosti CRA, vrátane produktov s digitálnymi prvkami uvedených na trh pred 11. decembrom 2027. Na rozdiel od povinností týkajúcich sa riešenia zraniteľností, ktoré trvajú len počas obdobia podpory produktu, povinnosti oznamovania sa naďalej uplatňujú aj po tom, čo produkt s digitálnymi prvkami už nie je podporovaný. Ak bol produkt s digitálnymi prvkami uvedený na trh pred 11. decembrom 2027 alebo ak jeho obdobie podpory skončilo, výrobca nie je povinný dodržiavať povinnosti týkajúce sa riešenia zraniteľností stanovené v časti II prílohy I.
211. Je potrebné pripomenúť, že povinnosť oznamovať takéto udalosti platí v okamihu, keď sa výrobca dozvie, že zraniteľnosť je aktívne zneužívaná alebo že došlo k závažnému incidentu, ktorý viedol k ohrozeniu bezpečnosti jeho produktu s digitálnymi prvkami. Usmernenia o tom, kedy sa má za to, že sa výrobca o danej skutočnosti dozvedel, by preto mali výrobcom pomôcť určiť okamih, od ktorého začínajú plynúť príslušné lehoty na oznamovanie.
212. Výrobcovia môžu podliehať porovnateľným povinnostiam oznamovania podľa rôznych právnych aktov EÚ. S cieľom zabezpečiť jednotný výklad pojmu „zistenie“ a uľahčiť výrobcom plnenie týchto povinností sú tieto usmernenia zosúladené s odôvodnením 31 vykonávacieho nariadenia Komisie (EÚ) 2024/2690 a s oddielom II(A) usmernení 9/2022 o oznamovaní porušení ochrany osobných údajov podľa GDPR.
213. V niektorých prípadoch výrobca zistí podozrivú udalosť alebo ho na potenciálny incident či zraniteľnosť upozorní tretia strana, napríklad fyzická osoba, zákazník, subjekt, orgán, mediálna organizácia alebo iný zdroj. V takýchto prípadoch by mal výrobca podozrivú udalosť bezodkladne posúdiť, aby určil, či ide o aktívne zneužívanú zraniteľnosť alebo o závažný incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami. Za moment, keď si výrobca uvedomil danú skutočnosť, sa preto považuje situácia, keď po takomto počiatočnom posúdení dospeje k primeranej miere istoty, že:
- i) zraniteľnosť obsiahnutá v jeho produkte s digitálnymi prvkami je aktívne zneužívaná; alebo
  - ii) došlo k závažnému incidentu, ktorý viedol k ohrozeniu bezpečnosti jeho produktu s digitálnymi prvkami.
214. Okamih, v ktorom možno považovať výrobcu za informovaného, bude preto závisieť od

okolností konkrétnej aktívne zneužívanej zraniteľnosti alebo závažného incidentu. V niektorých prípadoch bude od začiatku relatívne jasné, že zraniteľnosť je aktívne zneužívaná alebo že závažný incident ovplyvňuje bezpečnosť produktu s digitálnymi prvkami. V iných prípadoch môže trvať určitý čas, kým sa zistí, či je produkt s digitálnymi prvkami ovplyvnený zraniteľnosťou a či túto zraniteľnosť zneužíva škodlivý subjekt, alebo či incident ovplyvňuje bezpečnosť produktu s digitálnymi prvkami. Dôraz by sa však mal klásť na rýchle konanie s cieľom vykonať počiatočné posúdenie, aby sa zistilo, či sú takéto podmienky skutočne splnené, najmä ak zraniteľnosť môže predstavovať významné riziko, a ak áno, prijať nápravné opatrenia a oznámiť to v súlade s CRA.

215. Okrem toho štruktúra oznamovacích povinností vyžaduje, aby výrobcovia svoje oznámenia postupne aktualizovali v závislosti od pokroku svojich interných vyšetrení a v miere, v akej sa ich poznatky o aktívne zneužívanej zraniteľnosti alebo incidente stávajú podrobnejšími. Výrobcovia sú najmä povinní bez zbytočného odkladu, a v každom prípade do 24 hodín od zistenia, predložiť oznámenie o včasnom varovaní obsahujúce obmedzené informácie. Ďalšie informácie sa následne vyžadujú ako súčasť oznámenia, ktoré sa má predložiť bez zbytočného odkladu a v každom prípade do 72 hodín od zistenia („72-hodinové oznámenie“). Úplná správa sa musí predložiť do 14 dní po tom, ako bude k dispozícii nápravné alebo zmierňujúce opatrenie pre aktívne zneužívané zraniteľnosti, alebo do jedného mesiaca po 72-hodinovom oznámení v prípade závažných incidentov.
216. Ako sa pripomína aj v oddiele 3.3.1 *Trvalá podpora a zabezpečenie životaschopnosti FOSS*, správcovia softvéru s otvoreným zdrojovým kódom sú tiež povinní hlásiť aktívne zneužívané zraniteľnosti v súlade s článkom 24 ods. 3<sup>30</sup>. Táto povinnosť platí v okamihu, keď sa dozvedia o aktívne zneužívanej zraniteľnosti, a nie len v prípade, ak zraniteľnosť existuje v kódovej základni FOSS, ktorého správcom je daný subjekt. V praxi, keďže komponenty FOSS sa zvyčajne integrujú smerom nadol v dodávateľskom reťazci (downstream) do iných produktov s digitálnymi prvkami, je pravdepodobné, že správca sa o aktívnom zneužívaní dozvie prostredníctvom hlásení od tretích strán, ktoré identifikujú zneužitie v komponentoch FOSS integrovaných do iných produktov s digitálnymi prvkami. Môže to byť napríklad prípad, keď výrobca produktu s digitálnymi prvkami zistí aktívne zneužitie v komponente FOSS integrovanom do svojho vlastného produktu a nahlási to správcovi daného komponentu; alebo keď používateľ alebo výskumný pracovník nájde dôkazy o zneužití komponentu FOSS integrovaného do produktu s digitálnymi prvkami a nahlási toto aktívne zneužitie správcovi daného komponentu.
217. Malo by sa tiež objasniť, že keďže povinnosť hlásiť aktívne zneužívané zraniteľnosti platí vtedy, keď sa výrobca dozvie o aktívnom zneužívaní, výrobca nie je povinný hlásiť zraniteľnosti, o ktorých aktívnom zneužívaní sa dozvedel už pred 11. septembrom 2026 (dátum, od ktorého sa povinnosť hlásenia začína uplatňovať). CRA preto nevyžaduje spätné oznamovanie takýchto zraniteľností. Naopak, táto povinnosť sa uplatňuje v prípade, ak si výrobca bol vedomý existencie zraniteľnosti pred 11. septembrom 2026, ale v tom čase nemal vedomosť o jej aktívnom zneužívaní (buď preto, že k nemu ešte

---

<sup>30</sup> V rozsahu, v akom je správca zapojený do vývoja produktu s digitálnymi prvkami.

nedošlo, alebo preto, že si to výrobca neuvedomil). Ak po 11. septembri 2026 dôjde k aktívnemu zneužitiu alebo sa o ňom výrobca dozvie, zraniteľnosť sa považuje za aktívne zneužívanú, na ktorú sa vzťahuje povinnosť hlásenia.

218. Podobne je výrobca povinný nahlásiť len aktívne zneužívané zraniteľnosti obsiahnuté v jeho produkte s digitálnymi prvkami. Ak produkt s digitálnymi prvkami obsahuje aktívne zneužívanú zraniteľnosť pochádzajúcu z komponentu tretej strany, výrobca produktu s digitálnymi prvkami je povinný túto aktívne zneužívanú zraniteľnosť nahlásiť. Ak si však výrobca uvedomuje, že komponent tretej strany obsahuje zraniteľnosť, ale táto zraniteľnosť buď:

- i) nemôže byť zneužitá v jeho produkte s digitálnymi prvkami (napr. preto, že k zraniteľnému kódu nie je prístup) alebo
- ii) nebola zneužitá v jeho produkte s digitálnymi prvkami, táto zraniteľnosť sa nepovažuje za aktívne zneužívanú zraniteľnosť obsiahnutú v jeho produkte s digitálnymi prvkami, a preto nepodlieha povinnému hláseniu zo strany tohto výrobcu.

Tento výrobca môže túto zraniteľnosť aj naďalej oznamovať na dobrovoľnej báze v súlade s článkom 15 CRA. Je tiež povinný dodržiavať požiadavky na riešenie zraniteľností uvedené v časti II prílohy I k CRA, ako aj nahlásiť zraniteľnosť osobe alebo subjektu, ktorý komponent vyrába alebo udržiava, v súlade s článkom 13 ods. 6 a ako je ďalej vysvetlené v oddiele 9.2.1 *Oznamovanie smerom nahor v dodávateľskom reťazci a zdieľanie bezpečnostných opráv*.

219. Po zistení aktívne zneužívanej zraniteľnosti alebo závažného incidentu sú výrobcovia v súlade s článkom 14 ods. 8 povinní informovať aj dotknutých používateľov a v prípade potreby všetkých používateľov. Ak tak neurobia včas, tímy CSIRT, ktoré oznámenie prijali, môžu poskytnúť takéto informácie používateľom, ak sa to považuje za primerané a nevyhnutné na prevenciu alebo zmiernenie dopadu danej zraniteľnosti alebo incidentu.
220. V súlade s prístupom CRA založeným na riziku sa povinnosť informovať používateľov stanovená v článku 14 ods. 8 má uplatňovať spôsobom založeným na riziku a primeraným spôsobom. Poskytovanie informácií o aktívne zneužívanej zraniteľnosti alebo závažnom incidente najmä neznamena, že takéto informácie musia byť zverejnené alebo bez rozlíšenia poskytnuté. V prípade potreby a s ohľadom na povahu produktu s digitálnymi prvkami, dotknutých používateľov a potenciálny dopad zraniteľnosti alebo incidentu môžu výrobcovia obmedziť zverejňovanie podrobných informácií na príslušných používateľov alebo dotknutých zákazníkov. Platí to najmä v prípade produktov s digitálnymi prvkami používaných v citlivých alebo kľúčových prostrediach, kde by verejné zverejnenie technických podrobností mohlo samo o sebe zvýšiť kybernetickobezpečnostné riziká alebo uľahčiť ďalšie zneužitie.
221. Akonáhle bude zraniteľnosť primerane odstránená alebo zmiernená, môže byť vhodné širšie zverejnenie. Tak by to bolo napríklad v prípade, ak zverejnenie prispieva k zvýšeniu všeobecného povedomia alebo umožňuje používateľom overiť si, že ich produkty s digitálnymi prvkami už nie sú postihnuté. V takýchto prípadoch by úroveň podrobností a načasovanie akéhokoľvek širšieho zverejnenia mali zostať primerané

a mali by zohľadňovať zvyškové riziká zneužitia, povahu produktu s digitálnymi prvkami a záujmy dotknutých používateľov. Okrem toho bod 4 časti II prílohy I vyžaduje, aby výrobcovia verejne zverejňovali informácie o odstránených zraniteľnostiach, akonáhle bude k dispozícii bezpečnostná aktualizácia.

## 9.2. Riešenie zraniteľností

### 9.2.1. Oznamovanie smerom nahor v dodávateľskom reťazci a zdieľanie bezpečnostných opráv

222. Článok 13 ods. 6 CRA vyžaduje, aby výrobcovia hlásili zraniteľnosti v integrovaných komponentoch osobe alebo subjektu, ktorý daný komponent vyrába alebo udržiava („hlásenie smerom nahor“ alebo „reporting upstream“).
223. Výrobcovia sú povinní podávať hlásenia smerom nahor len v súvislosti s verziou komponentu, ktorý integrujú. Ak osoba alebo subjekt, ktorý komponent vyrába alebo udržiava, zaviedol bezpečnostné politiky, koordinované postupy zverejňovania zraniteľností alebo určil kanály na hlásenie zraniteľností, výrobcovia by mali podávať hlásenia v súlade s nimi, najmä ak by predčasné zverejnenie neopravených zraniteľností mohlo zvýšiť kybernetickobezpečnostné riziká. Okrem toho, s cieľom znížiť zaťaženie udržiavateľov v pôvodnom (upstream) stupni, najmä v projektoch s otvoreným zdrojovým kódom, výrobcovia nie sú povinní oznamovať smerom nahor v dodávateľskom reťazci, ak môžu potvrdiť, že osoba alebo subjekt, ktorý komponent vyrába alebo udržiava, si je vedomá/-ý existencie zraniteľnosti. Výrobcovia sa vyzývajú, aby prijali primerané opatrenia na zabránenie podávaniu duplicitných hlásení, napríklad kontrolou verejne dostupných databáz zraniteľností, bezpečnostných upozornení špecifických pre daný projekt alebo zavedených systémov sledovania problémov pred oznámením smerom nahor v dodávateľskom reťazci.
224. Výrobcovia sú povinní oznamovať smerom nahor v dodávateľskom reťazci len tie zraniteľnosti, ktoré existujú v samotnej integrovanej súčasti, a nie zraniteľnosti, ktoré vznikajú v dôsledku integrácie medzi súčasťou a iným kódom vyvinutým výrobcom alebo v dôsledku integrácie iných súčastí. Napriek tomu môžu nastať situácie, keď integrácia súčasti do konkrétneho produktu s digitálnymi prvkami odhalí určité správanie, interakcie alebo bezpečnostné charakteristiky tejto súčasti, ktoré neboli zrejmé alebo neboli ľahko identifikovateľné, ak bola súčasť izolovaná. V takýchto prípadoch sa výrobcom odporúča, aby tieto informácie oznámili osobe alebo subjektu, ktorý komponent vyrába alebo udržiava, s cieľom podporiť osvedčené postupy pri riešení zraniteľností zamerané na uľahčenie účinného odstránenia a zlepšenie celkovej bezpečnosti ekosystému komponentov.
225. Nakoniec, výrobcovia tiež nie sú povinní oznamovať zraniteľnosť smerom nahor v dodávateľskom reťazci, ak komponent už nemá správcu alebo ak sa výrobca pri nových verziách či bezpečnostných opravách už nespolieha na pôvodného udržiavateľa. V takýchto prípadoch sa však výrobcovi odporúča informovať používateľov daného komponentu prostredníctvom primeraných alternatívnych opatrení, napr. cez existujúce komunitné mechanizmy (ako sú e-mailové konferencie alebo hlásenia problémov) alebo prostredníctvom verejných záznamov

o zraniteľnostiach.

- 226. Okrem toho podľa článku 13 ods. 6 sú výrobcovia, ktorí vyvinuli softvérovú úpravu na odstránenie zraniteľnosti v integrovanom komponente, povinní zdieľať túto softvérovú úpravu („bezpečnostnú opravu“) s osobou alebo subjektom, ktorý komponent vyrába alebo udržiava („zdieľanie smerom nahor“).
- 227. Ak sú výrobcovia povinní zdieľať bezpečnostnú opravu podľa článku 13 ods. 6, táto oprava by mala byť, ak je to vhodné, poskytnutá v strojovo čitateľnom formáte spôsobom, ktorý možno ľahko overiť a, ak je to vhodné, integrovať osobou alebo subjektom, ktorá/-ý danú súčasť vyrába alebo udržiava. Ak ide o komponent slobodného softvéru a softvéru s otvoreným zdrojovým kódom, bezpečnostná oprava by mala byť zdieľaná spôsobom kompatibilným s licenciou daného komponentu, napríklad zdieľaním pod tou istou licenciou alebo pod licenciou, ktorá umožňuje správcovi distribuovať opravu pod vlastnou licenciou. Ak má udržiavateľ daného komponentu usmernenia o tom, ako by sa mali bezpečnostné opravy zdieľať, výrobca by sa mal týmito usmerneniami riadiť.
- 228. CRA však od výrobcov nevyžaduje, aby zabezpečili, že ich bezpečnostné opravy budú nevyhnutne prijaté osobou alebo subjektom, ktorá/-ý komponent vyrába alebo udržiava. Rovnako sa od nich nevyžaduje, aby zabezpečili, že tieto opravy budú nevyhnutne integrované do repozitára kódu komponentu, napríklad v prípade, ak udržiavateľ uprednostňuje inú možnosť na vyriešenie problému. Podobne sa od výrobcov nevyžaduje, aby prijali navrhovanú opravu vyvinutú správcom komponentu, a môžu uprednostniť zmiernenie problému inými vhodnými spôsobmi.
- 229. V niektorých prípadoch môže osoba alebo subjekt, ktorá/-ý komponent vyrába alebo udržiava, už poskytnúť bezpečnostnú opravu na odstránenie zraniteľnosti, avšak výrobca implementuje inú stratégiu zmiernenia (napríklad zmenou inej konfigurácie). V takýchto prípadoch CRA nevyžaduje, aby výrobca zdieľal úpravu inej časti systému smerom nahor v reťazci. Výrobca je však povzbudzovaný, aby tak urobil, ak to môže pomôcť osobe alebo subjektu, ktorá/-ý komponent udržiava.

### 9.2.2. Známe zneužiteľné zraniteľnosti

- 230. Jedna zo základných požiadaviek časti I prílohy I k CRA stanovuje, že na základe posúdenia kybernetickobezpečnostného rizika uvedeného v článku 13 ods. 2 a v prípade potreby musia byť produkty s digitálnymi prvkami prístupné na trhu bez známych zneužiteľných zraniteľností.
- 231. Článok 3 ods. 41 definuje „zneužiteľná zraniteľnosť“, ako „zraniteľnosť, ktorú môže nepriateľský subjekt účinne využiť za reálnych prevádzkových podmienok;“. Nie všetky zraniteľnosti je možné zneužiť za praktických prevádzkových podmienok a niektoré zraniteľnosti je možné zneužiť len za teoretických podmienok (napr. v laboratóriu alebo v simulácii) a/alebo nie za podmienok, ktoré by nastali v prevádzkovom prostredí produktu s digitálnymi prvkami.
- 232. CRA vyžaduje, aby výrobcovia mali zavedené primerané politiky a postupy na riešenie a odstraňovanie potenciálnych zraniteľností nahlásených z interných alebo externých zdrojov (článok 13 ods. 8). Nevyšpecifikuje však výslovne, kedy by sa zneužiteľná

zraniteľnosť mala považovať za známu výrobcovi, čím by vznikla povinnosť splniť túto základnú požiadavku v okamihu uvedenia na trh.

233. Zraniteľnosť by sa mala považovať za známu, ak je uvedená v príslušných verejne dostupných databázach zraniteľností, ako je Európska databáza zraniteľností zriadená podľa článku 12 ods. 2 smernice (EÚ) 2022/2555 alebo iné významné databázy zraniteľností.
234. Okrem toho môže byť zraniteľnosť známa aj vtedy, ak bola výrobcovi oznámená prostredníctvom neverejných informácií, napríklad prostredníctvom koordinovaného zverejnenia výskumným pracovníkom alebo prostredníctvom vlastného interného testovania a analýzy výrobcu, vrátane napríklad využívania služieb založených na umelej inteligencii. Podobne môže byť zraniteľnosť známa, ak bola verejne a výrazne oznámená v spoľahlivých médiách, vrátane špecializovaných publikácií o kybernetickej bezpečnosti alebo všeobecných masových médií.
235. Samotná skutočnosť, že sa o zraniteľnosti informuje alebo že bola zistená, však ešte neznamená, že je v praxi zneužiteľná alebo že sa týka konkrétneho produktu s príslušnými digitálnymi prvkami. Výrobca ju bude musieť prešetriť a potvrdiť pravdivosť týchto informácií a ich uplatniteľnosť na svoj vlastný produkt s digitálnymi prvkami. V dôsledku toho môže medzi prvým nahlásením zraniteľnosti a jej potvrdením uplynúť určitý čas. Ako sa uvádza v oddiele 9.1 *Povinnosti oznamovania*, dôraz by sa mal klásť na rýchle konanie s cieľom prešetriť situáciu a reagovať na ňu.
236. Okrem toho povinnosť výrobcov dodržiavať základné požiadavky stanovené v časti I prílohy I platí v okamihu uvedenia na trh v súlade s článkom 13 ods. 1. V praxi sa môže stať, že nové potenciálne zneužiteľné zraniteľnosti sa objavujú v záverečných fázach vývojového cyklu produktu s digitálnymi prvkami, a to aj krátko predtým, ako sa dostane do distribučného reťazca (a je teda uvedený na trh).
237. Keďže povinnosť uvádzať produkty s digitálnymi prvkami na trh bez známych zneužiteľných zraniteľností je povinnosťou založenou na riziku, je na výrobcovi, aby na základe posúdenia kybernetickobezpečnostných rizík určil, či je možné produkt s digitálnymi prvkami bezpečne uviesť na trh v súlade s CRA. Alternatívne môže výrobca rozhodnúť, že nová zraniteľnosť, o ktorej sa možno dozvedel, musí byť odstránená skôr, ako bude možné produkt s digitálnymi prvkami uviesť na trh. Pri tomto posudzovaní by výrobcovia mali zohľadniť závažnosť, zneužiteľnosť a potenciálny dopad zraniteľnosti, ako aj riziká vyplývajúce pre samotný produkt s digitálnymi prvkami po jeho uvedení do prevádzky. Môžu tiež zohľadniť riziká spojené s odložením uvedenia produktu na trh až do odstránenia zraniteľnosti, napríklad preto, že nová verzia rieši aj iné zneužiteľné zraniteľnosti alebo je nevyhnutná pre pokračovanie prevádzky kritických systémov. V každom prípade, akonáhle sa produkt s digitálnymi prvkami uvedie na trh, výrobca naďalej podlieha povinnosti riešiť zraniteľnosti účinne a v súlade s požiadavkami na riešenie zraniteľností stanovenými v časti II prílohy I.

### 9.2.3. Účinné a pravidelné testovanie a preskúmanie

238. Bod 3 časti II prílohy I vyžaduje, aby výrobcovia počas celého obdobia podpory vykonávali účinné a pravidelné testy a preskúmania produktu s digitálnymi prvkami.

Vykonávanie pravidelných testov nevyžaduje mechanické opakovanie nezmenenej testovacej kampane v pevne stanovených intervaloch. Znamená to pravidelne preskúmať, či nové informácie, ako sú novo identifikované hrozby alebo novo objavené zraniteľnosti, vyžadujú aktualizáciu existujúcich testov, a podľa toho testy vykonávať.

239. Frekvencia, hĺbka a obsah preskúmania by mali byť primerané profilu kybernetickobezpečnostného rizika produktu s digitálnymi prvkami, jeho vývoju v čase a stavu hrozbového prostredia. Ak sa pri preskúmaní zistia relevantné nové podnety ovplyvňujúce súbor testov, mali by sa navrhnúť a vykonať nové alebo upravené testy na produkte, aby sa zabezpečilo, že žiadne zraniteľnosti nezostanú nevyriešené. To môže zahŕňať opätovné vykonanie existujúcich testov, ak úprava produktu s digitálnymi prvkami robí takéto typy testovania vhodnými, napríklad regresné testovanie.
240. Ak sa pri preskúmaní nezistia žiadne takéto podnety, nie je potrebné navrhovať ďalšie testy. Paralelne naďalej platia ďalšie povinnosti týkajúce sa riešenia zraniteľností, vrátane povinnosti riešiť a odstraňovať zraniteľnosti v súvislosti s predstavovanými rizikami.

### 9.3. Vzájomné pôsobenie s inými právnymi predpismi

#### 9.3.1. Nariadenie (EÚ) 2019/2144 a nariadenie (EÚ) č. 168/2013

241. V článku 2 ods. 2 písm. c) CRA sa stanovuje, že toto nariadenie sa nevzťahuje na produkty s digitálnymi prvkami, na ktoré sa vzťahuje nariadenie (EÚ) 2019/2144. Nariadenie (EÚ) 2019/2144 sa vzťahuje na „vozidlá kategórií M, N a O, ako sú vymedzené v článku 4 nariadenia (EÚ) 2018/858, a na systémy, komponenty a samostatné technické jednotky navrhnuté a vyrobené pre takéto vozidlá“.
242. Podobne boli produkty s digitálnymi prvkami, ktoré spadajú do rozsahu pôsobnosti nariadenia (EÚ) č. 168/2013, vylúčené z rozsahu pôsobnosti CRA delegovaným nariadením Komisie (EÚ) 2025/1535. Nariadenie (EÚ) č. 168/2013 sa vzťahuje na vozidlá kategórie L a „na systémy, komponenty a samostatné technické jednotky, ako aj na diely a vybavenie, navrhnuté a vyrobené pre takéto vozidlá“ (článok 2 ods. 1).
243. Vozidlá, na ktoré sa tieto nariadenia vzťahujú, nepodliehajú CRA. Okrem toho sú potrebné ďalšie objasnenia, pokiaľ ide o rozsah výnimky pre systémy, komponenty, samostatné technické jednotky, diely a vybavenie (na účely tejto časti „súčasti“), navrhnuté a vyrobené pre takéto vozidlá, ktoré sa považujú za produkty s digitálnymi prvkami v zmysle CRA.
244. Považuje sa, že takéto komponenty nepodliehajú CRA, za predpokladu, že sú navrhnuté a vyrobené výlučne na integráciu do vozidiel, na ktoré sa vzťahujú nariadenia (EÚ) 2019/2144 a č. 168/2013. Platí to bez ohľadu na to, či výrobca danej súčasti ju predáva priamo výrobcovi vozidiel alebo inému hospodárskemu subjektu v dodávateľskom reťazci automobilového priemyslu, pokiaľ je táto súčasť jednoznačne určená a vhodná výlučne na konečnú integráciu do týchto vozidiel.
245. Naopak, výrobca, ktorý predáva generické komponenty, ktoré sú produktami s digitálnymi prvkami a ktoré môžu byť integrované do rôznych typov produktov, a nie

výlučne do vozidiel, na ktoré sa vzťahujú uvedené nariadenia, podlieha CRA.

246. Posúdenie toho, či sa súčiastka uvádza na trh v zmysle CRA, sa musí zakladať na objektívnych podmienkach, za ktorých je sprístupňovaná. Ak výrobca ponúka súčiastku, ktorá nie je výlučne vhodná na konečnú integráciu do týchto vozidiel, prostredníctvom distribučných kanálov, ktoré sú prístupné zákazníkovi mimo dodávateľského reťazca v automobilovom priemysle, ako sú bežné maloobchodné predajne alebo online predajné kanály prijímajúce objednávky od širokej verejnosti, táto súčiastka spadá do pôsobnosti CRA bez ohľadu na akékoľvek vyhlásenia týkajúce sa jej zamýšľaného použitia. Za takýchto okolností nemožno súčiastku považovať za navrhnutú a vyrobenú výlučne na účely integrácie do vozidiel, na ktoré sa vzťahujú nariadenia (EÚ) 2019/2144 a č. 168/2013, a výrobca je povinný dodržiavať CRA. Naopak, využívanie obmedzených distribučných kanálov typu „business-to-business“ (B2B), obmedzených na dodávateľský reťazec v automobilovom priemysle, môže naznačovať, že je navrhnutá a vyrobená výlučne na účely takejto integrácie.

### 9.3.2. Platnosť certifikátov EÚ skúšky typu (článok 69 ods. 1)

247. V článku 69 ods. 1 CRA sa uvádza, že „Certifikáty EÚ skúšky typu a rozhodnutia o schválení vydané v súvislosti s požiadavkami na kybernetickú bezpečnosť produktov s digitálnymi prvkami, na ktoré sa vzťahujú iné harmonizačné právne predpisy Únie ako toto nariadenie, zostávajú v platnosti do 11. júna 2028, pokiaľ ich platnosť neuplynie pred týmto dátumom, alebo pokiaľ nie je v takýchto iných harmonizačných právnych predpisoch Únie uvedené inak, pričom v takom prípade zostávajú v platnosti tak, ako sa v daných právnych predpisoch uvádza“.
248. Trvanie platnosti týchto certifikátov a rozhodnutí o schválení by sa malo chápať tak, že sa obmedzuje na kybernetickobezpečnostné riziká a príslušné požiadavky, na ktoré sa vzťahujú príslušné harmonizačné právne predpisy Únie, na základe ktorých boli vydané. Pokiaľ ide o tieto riziká, výrobcovia nie sú povinní opätovne posudzovať ani preukazovať zhodu výlučne na účely CRA počas obdobia platnosti uvedeného v článku 69 ods. 1 v prípade produktov s digitálnymi prvkami, ktoré majú v úmysle uviesť na trh 11. decembra 2027 alebo neskôr a do 11. júna 2028<sup>31</sup>. To platí pre certifikáty a rozhodnutia o schválení vydané v prípadoch, keď príslušné harmonizačné právne predpisy Únie vyžadujú, aby výrobca vykonal posúdenie zhody postup posudzovania prostredníctvom notifikovanej osoby, ako aj v prípadoch, keď sa výrobca dobrovoľne rozhodol tak urobiť.
249. Existencia platného certifikátu alebo rozhodnutia o schválení podľa iných harmonizačných právnych predpisov Únie preto neoslobodzuje výrobcov od povinnosti vykonať komplexné posúdenie kybernetickobezpečnostného rizika podľa CRA (ani od iných povinností vyplývajúcich z tohto nariadenia). Umožňuje im však spoliehať sa na existujúce certifikácie ako dôkaz o súlade v rámci ich postupu posudzovania zhody, a to

---

<sup>31</sup> Produkty s digitálnymi prvkami uvedené na trh pred 11. decembrom 2027 podliehajú právnym predpisom Únie platným v čase ich uvedenia na trh a ak boli v súlade s týmito predpismi, môžu sa predávať a uvádzať do prevádzky, pokiaľ sa 11. decembra 2027 alebo neskôr nepodrobia podstatným úpravám. Pojmy „uvádzanie na trh“ a „sprístupňovanie na trhu“ sú vysvetlené aj v časti 2.1 Uvádzanie na trh tohto dokumentu, ako aj v kapitole 2 Modrej príručky.

v rozsahu, v akom sú príslušné kybernetickobezpečnostné riziká už pokryté. Ak má certifikát alebo rozhodnutie o schválení platnosť podľa iných harmonizačných právnych predpisov Únie presahujúcu 11. jún 2028, výrobca sa môže na účely CRA na takýto certifikát alebo rozhodnutie spoliehať len do 11. júna 2028.

250. Ak posúdenie kybernetickobezpečnostného rizika vykonané v súlade s článkom 13 ods. 2 identifikuje dodatočné riziká, na ktoré sa nevzťahujú požiadavky kybernetickej bezpečnosti, na ktorých sa zakladá existujúci certifikát alebo rozhodnutie o schválení, výrobcovia naďalej nesú zodpovednosť za riešenie týchto rizík v súlade s CRA. V takýchto prípadoch súlad vyžaduje, aby boli identifikované nedostatky posúdené a zmiernené, bez ohľadu na to, či existujúci certifikát alebo rozhodnutie o schválení naďalej platí.
251. To možno ilustrovať na príklade, keď sa na produkt s digitálnymi prvkami vzťahujú požiadavky kybernetickej bezpečnosti stanovené v delegovanom nariadení Komisie (EÚ) 2022/30, ktorým sa dopĺňa smernica 2014/53/EÚ (delegovaný akt k smernici o rádiových zariadeniach (RED)), a keď bolo na základe týchto požiadaviek vydané certifikát EÚ skúšky typu alebo rozhodnutie o schválení. V takom prípade zostáva certifikát alebo rozhodnutie v súlade s článkom 69 ods. 1 platné pre kybernetickobezpečnostné riziká, na ktoré sa tento certifikát vzťahuje a ktoré súvisia so základnými požiadavkami kybernetickej bezpečnosti stanovenými v smernici 2014/53/EÚ (smernica o rádiových zariadeniach, alebo „RED“).
252. V takýchto prípadoch sa od výrobcov na účely CRA nevyžaduje, aby opätovne posudzovali alebo preukazovali zhodu s ohľadom na kybernetickobezpečnostné riziká, ktoré už boli riešené týmito certifikátmi, pokiaľ príslušný certifikát alebo rozhodnutie o schválení zostáva platné, a v žiadnom prípade nie dlhšie ako do 11. júna 2028. Patria sem napríklad kybernetickobezpečnostné riziká súvisiace s ochranou sietí, ochranou osobných údajov a súkromia alebo prevenciou podvodov (v rozsahu, v akom sa na tieto riziká vzťahuje daný certifikát) súvisiace s požiadavkami na kybernetickú bezpečnosť podľa smernice RED a zohľadnené v posúdení zhody.
253. Ak však posúdenie kybernetickobezpečnostného rizika vykonané v súlade s článkom 13 ods. 2 CRA identifikuje ďalšie kybernetickobezpečnostné riziká, na ktoré sa tieto certifikáty nevzťahujú, výrobcovia naďalej nesú zodpovednosť za riešenie týchto rizík v súlade s CRA. Môže to zahŕňať napríklad riziká súvisiace s procesmi riešenia zraniteľností, minimalizáciou údajov a zmenšením plochy útoku alebo iné aspekty kybernetickej bezpečnosti špecifické pre daný produkt, ktoré nie sú riešené týmito certifikátmi alebo v žiadnom prípade nie sú pokryté základnými požiadavkami kybernetickej bezpečnosti podľa smernice RED.
254. Existencia platného certifikátu EÚ skúšky typu alebo rozhodnutia o schválení podľa smernice RED, pokiaľ ide o jej základné požiadavky týkajúce sa kybernetickej bezpečnosti, preto sama osebe nepreukazuje úplnú zhodu s CRA. Umožňuje však výrobcovi spoliehať sa na tento certifikát alebo rozhodnutie ako na dôkaz zhody v súvislosti s príslušnými rizikami, pričom sa zabezpečuje, že akékoľvek zostávajúce alebo novo identifikované riziká sa posúdia a zmiernia v súlade s CRA.

255. Podobne, ak sa na produkt s digitálnymi prvkami vzťahujú základné požiadavky na zdravie a bezpečnosť súvisiace s kybernetickou bezpečnosťou stanovené v nariadení (EÚ) 2023/1230 (nariadenie o strojových zariadeniach), ktoré sa v plnom rozsahu uplatňuje od 20. januára 2027, a ak bolo na základe týchto požiadaviek vydaný certifikát EÚ skúšky typu alebo rozhodnutie o schválení, tento certifikát alebo rozhodnutie o schválení zostáva v súlade s článkom 69 ods. 1 CRA platné pre kybernetickobezpečnostné riziká, na ktoré sa vzťahuje nariadenie o strojových zariadeniach.
256. Konkrétne sa to týka aspektov kybernetickej bezpečnosti súvisiacich s ochranou proti poškodeniu a bezpečnosťou a spoľahlivosťou riadiacich systémov, ako je stanovené v oddieloch 1.1.9 a 1.2.1 prílohy III k nariadeniu o strojových zariadeniach. Pokiaľ ide o tieto riziká, výrobcovia nie sú na účely CRA povinní opätovne posudzovať ani preukazovať zhodu, pokiaľ príslušný certifikát alebo rozhodnutie o schválení zostáva platné, a v žiadnom prípade nie dlhšie ako do 11. júna 2028. Toto platí v rozsahu, v akom boli tieto riziká riešené v rámci posudzovania zhody podľa nariadenia o strojových zariadeniach.
257. Rovnako ako v prípade vyššie uvedených základných požiadaviek kybernetickej bezpečnosti podľa smernice RED, ak posúdenie kybernetickobezpečnostného rizika vykonané podľa článku 13 ods. 2 CRA identifikuje dodatočné kybernetickobezpečnostné riziká, na ktoré sa nevzťahuje príslušný certifikát vydaný podľa nariadenia o strojových zariadeniach a ktoré súvisia s požiadavkami kybernetickej bezpečnosti uvedeného nariadenia, výrobcovia naďalej nesú zodpovednosť za riešenie týchto rizík v súlade s CRA.