Úradný vestník
Európskej únie

SK
Séria C

C/2026/6013

17.11.2026

OZNÁMENIE KOMISIE

Usmernenie Komisie k uplatňovaniu nariadenia (EÚ) 2024/2847 (akt o kybernetickej odolnosti)

(C/2026/6013)

Obsah

Strana

1. ÚVOD ... 3
   - 1.1. Akt o kybernetickej odolnosti ... 3
   - 1.2. Účel usmernení ... 3
2. ROZSAH PÔSOBNOSTI ... 4
   - 2.1. Uvedenie na trh ... 4
   - 2.2. Softvér ako produkt s digitálnymi prvkami ... 5
   - 2.3. Počítačový kód ... 6
   - 2.4. Kombinácia hardvéru a softvéru tvoriaca produkt s digitálnymi prvkami ... 7
   - 2.5. Dátové pripojenie ... 8
   - 2.6. Zložité systémy ... 8
   - 2.7. Produkty s digitálnymi prvkami navrhnuté pred začatím uplatňovania aktu o kybernetickej odolnosti ... 9
3. SLOBODNÝ SOFTVÉR A SOFTVÉR S OTVORENÝM ZDROJOVÝM KÓDOM ... 11
   - 3.1. Určenie toho, kto je zodpovedný za slobodný softvér a softvér s otvoreným zdrojovým kódom ... 12
   - 3.2. Určenie toho, či sa slobodný softvér a softvér s otvoreným zdrojovým kódom uvádza na trh EÚ ... 13
     - 3.2.1. Účtovanie ceny ... 13
     - 3.2.2. Speňaženie iných služieb alebo požiadavka na spracovanie osobných údajov ... 13
     - 3.2.3. Podporné služby ... 14
     - 3.2.4. Dary ... 15
     - 3.2.5. Financovanie slobodného softvéru a softvéru s otvoreným zdrojovým kódom ... 15
     - 3.2.6. Neziskové subjekty zriadené na dosiahnutie neziskových cieľov ... 16
     - 3.2.7. Integrácia inými výrobcami ... 16
   - 3.3. Správcovia softvéru s otvoreným zdrojovým kódom ... 16
     - 3.3.1. Trvalá podpora a zabezpečenie životaschopnosti slobodného softvéru a softvéru s otvoreným zdrojovým kódom ... 17
   - 3.4. Prispievatelia a následné využitie ... 18
   - 3.5. Ilustratívne scenáre ... 19
4. PODSTATNÉ ÚPRAVY A NÁHRADNÉ DIELY ... 21
   - 4.1. Fyzické opravy ... 22
   - 4.2. Náhradné diely ... 23
   - 4.3. Aktualizácie softvéru ako podstatné úpravy ... 24

4.4. Dôsledky podstatnej úpravy 27
4.4.1. Podstatné úpravy vykonané inou osobou ako pôvodným výrobcom 28
4.4.2. Podstatné úpravy vykonané pôvodným výrobcom 29
5. OBDOBIE PODPORY 29
5.1. Podstatné úpravy a obdobie podpory 31
6. DÔLEŽITÉ A KRITICKÉ PRODUKTY S DIGITÁLNYMI PRVKAMI 32
6.1. Základná funkcia 33
6.2. Posudzovanie zhody dôležitých a kritických produktov s digitálnymi prvkami 36
6.3. Dôsledky pre predpoklad zhody 38
7. POSÚDENIE KYBERNETICKOBEZPEČNOSTNÝCH RIZÍK A INTEGRÁCIA PRODUKTOV S DIGITÁLNYMI PRVKAMI A KOMPONENTOV 41
7.1. O hodnotení a riešení kybernetickobezpečnostných rizík 41
7.2. O navrhovaní, vývoji a výrobe produktov s digitálnymi prvkami takým spôsobom, aby na základe rizík zabezpečovali primeranú úroveň kybernetickej bezpečnosti 42
7.3. Posúdenie rizík a náležitá starostlivosť v súvislosti s externými závislosťami a integrovanými komponentmi 42
7.4. Opätovné použitie posúdení rizík a dokumentácie o zhode pre skupiny produktov s digitálnymi prvkami 44
8. SPRACOVANIE ÚDAJOV NA DIAĽKU 44
8.1. Čo sa považuje za riešenie spracovania údajov na diaľku pre produkt s digitálnymi prvkami? 45
8.1.1. Pojem „na diaľku“ 46
8.1.2. Bránila by neexistencia takéhoto spracovania údajov produktu s digitálnymi prvkami plniť jednu z jeho funkcií? 46
8.1.3. Bol softvér navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť? 47
8.2. Praktické a technické dôsledky riešení spracovania údajov na diaľku a využívania riešení tretích strán 49
8.3. Prípady použitia riešení spracovania údajov na diaľku 50
8.3.1. Mobilná banková aplikácia 51
8.3.2. Inteligentný termostat 52
8.3.3. Elektronická čítačka 53
8.3.4. Priemyselný robot 53
8.3.5. Mobilná sieť 53
9. ĎALŠIE PRVKY 54
9.1. Oznamovacie povinnosti 54
9.2. Riešenie zraniteľností 56
9.2.1. Oznamovanie zraniteľností smerom k pôvodným zdrojom a zdieľanie bezpečnostných opráv 56
9.2.2. Známe zneužiteľné zraniteľnosti 57
9.2.3. Účinné a pravidelné testy a preskúmania 58
9.3. Vzájomné prepojenie s ostatnými právnymi predpismi 59
9.3.1. Nariadenie (EÚ) 2019/2144 a nariadenie (EÚ) č. 168/2013 59
9.3.2. Platnosť certifikátov EÚ skúšky typu (článok 69 ods. 1) 59

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) ([1]) nadobudlo účinnosť 10. decembra 2024. Cieľom uvedeného 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 na uvádzanie produktov s digitálnymi prvkami na trh Únie, ako aj počas životného cyklu takýchto produktov.

2. Akt o kybernetickej odolnosti vychádza z nového legislatívneho rámca EÚ stanoveného v nariadení Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 a rozhodnutia Európskeho parlamentu a Rady č. 768/2008/ES z 9. júla 2008 o spoločnom rámci na uvádzanie výrobkov na trh a o zrušení rozhodnutia 93/465/EHS ([2]).

3. Dohľad nad trhom a presadzovanie predpisov zabezpečujú národné orgány dohľadu nad trhom. Produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti aktu o kybernetickej odolnosti, sú upravené nariadením Európskeho parlamentu a Rady (EÚ) 2019/1020 z 20. júna 2019 o dohľade nad trhom a súlade výrobkov a o zmene smernice 2004/42/ES a nariadení (ES) č. 765/2008 a (EÚ) č. 305/2011. Hospodárske subjekty a členské štáty podporujú pri uplatňovaní aktu o kybernetickej odolnosti Komisia a Agentúra Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“).

1.2. Účel usmernení

4. V článku 26 ods. 1 aktu o kybernetickej odolnosti sa vyžaduje, aby Komisia uverejnila usmernenia na pomoc hospodárskym subjektom pri uplatňovaní tohto nariadenia s osobitným zameraním na podporu jeho dodržiavania mikropodnikmi a malými a strednými podnikmi (ďalej len „MSP“). V článku 26 ods. 2 sú stanovené minimálne aspekty, ktoré by mali byť v usmerneniach zahrnuté. Patria medzi ne: i) rozsah pôsobnosti aktu o kybernetickej odolnosti (najmä riešenia spracovania údajov na diaľku a slobodný softvér a softvér s otvoreným zdrojovým kódom); ii) pojem „obdobia podpory“; iii) vzájomné pôsobenie medzi aktom o kybernetickej odolnosti a ostatnými právnymi predpismi EÚ a iv) pojem „podstatná úprava“.

5. Komisia uverejnila 3. decembra 2025 súbor často kladených otázok, ktorých cieľom je pomôcť hospodárskym subjektom pripraviť sa na vykonávanie aktu o kybernetickej odolnosti ([3]).

6. Tieto usmernenia majú pomôcť hospodárskym subjektom pri dodržiavaní aktu o kybernetickej odolnosti a podporiť činnosť orgánov dohľadu nad trhom, notifikujúcich orgánov a notifikovaných osôb s cieľom zabezpečiť harmonizované presadzovanie aktu o kybernetickej odolnosti v celej Únii. Tieto usmernenia nie sú určené na pokrytie celého rozsahu pôsobnosti aktu o kybernetickej odolnosti, ale skôr na objasnenie odôvodnenia určitých kľúčových ustanovení a spôsobu ich vykonávania v praxi. Týkajú sa aktu o kybernetickej odolnosti a nevzťahujú sa na iné právne predpisy EÚ.

([1]) Ú. v. EÚ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) V pracovnom programe Komisie na rok 2026 sa počíta s predložením „európskeho aktu o výrobkoch“, ktorým sa aktualizuje nový legislatívny rámec a pravidlá týkajúce sa dohľadu nad trhom a normalizácie: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:52025DC0870.

([3]) Často kladené otázky je možné stiahnuť z webového sídla Komisie venovaného vykonávaniu aktu o kybernetickej odolnosti, a to na špeciálnej webovej stránke s často kladenými otázkami.

7. Pri príprave týchto usmernení prebehli rozsiahle konzultácie so zainteresovanými stranami, a to aj s expertnou skupinou pre kybernetickú bezpečnosť produktov s digitálnymi prvkami ([4]) a prostredníctvom verejnej konzultácie, ktorá sa konala v období od 3. marca do 13. apríla 2026 ([5]).

8. Tieto usmernenia nie sú pre hospodárske subjekty ani iné subjekty, na ktoré sa vzťahuje akt o kybernetickej odolnosti, záväzné. Záväzný výklad aktu o kybernetickej odolnosti môže podať len Súdny dvor Európskej únie. Predstavujú však výklad Komisie týkajúci sa aktu o kybernetickej odolnosti, ktorého cieľom je podporiť dodržiavanie predpisov a prispieť k účinnému vykonávaniu nariadenia. Okrem toho obsahujú viacero príkladov na ilustráciu uplatňovania konkrétnych ustanovení. Tieto príklady však nemajú nahradiť osobitné posúdenie jednotlivých prípadov, ktoré bude vždy potrebné s ohľadom na špecifiká každého jednotlivého prípadu.

9. V súlade s článkom 26 aktu o kybernetickej odolnosti môže Komisia zvážiť vydanie ďalších usmernení vrátane usmernení so zameraním na výrobcov, na ktorých sa vzťahuje akt o kybernetickej odolnosti, ako aj ďalšie harmonizačné právne predpisy Únie alebo iné súvisiace právne akty Únie. V týchto usmerneniach sa môžu napríklad riešiť otázky týkajúce sa vzájomného pôsobenia medzi aktom o kybernetickej odolnosti 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 (ďalej len „nariadenie DORA“).

2. **ROZSAH PÔSOBNOSTI**

2.1. **Uvedenie na trh**

10. Akt o kybernetickej odolnosti sa vzťahuje na produkty s digitálnymi prvkami, ktoré sú sprístupňované na trhu EÚ. Pojem sprístupnenie na trhu je vymedzený v článku 3 bode 22 aktu o kybernetickej odolnosti 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 bodom 21 sa produkt s digitálnymi prvkami uvádza na trh EÚ v okamihu, keď je po prvýkrát sprístupnený.

11. Usmernenia uľahčujúce pochopenie pravidiel EÚ týkajúcich sa produktov a ich jednotné uplatňovanie v rôznych odvetvových právnych rámcoch zosúladených s novým legislatívnym rámcom, ako je napríklad akt o kybernetickej odolnosti, poskytuje najnovšie vydanie „Modrej príručky na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov“, uverejnené v roku 2022 (ďalej len „Modrá príručka“) ([6]). V Modrej príručke sa uvádza, že pojmy „uvádzanie na trh“ a „sprístupňovanie“ treba chápať tak, že sa vzťahujú „na každý jednotlivý výrobok, nie na typ výrobku, a na to, či bol vyrobený ako samostatná jednotka alebo v sérii“ (oddiel 2.3).

12. V prípade „tradičnejších“ produktov s digitálnymi prvkami, na ktoré sa vzťahuje nový legislatívny rámec, ako je napríklad hardvér v podobe strojového zariadenia alebo rádiových zariadení s digitálnymi prvkami, je pojem „uvedenie na trh“ jasne vymedzený a Modrá príručka poskytuje ďalšie usmernenia, v ktorých sa objasňuje, kedy sa takéto produkty považujú za uvedené na trh. Ďalšie príklady pojmu „uvedenie na trh“ predstavujú „súhrnné príklady“ uvedené v oddiele 2.12 Modrej príručky.

13. Vzhľadom na povahu nehmotných produktov s digitálnymi prvkami, ako je samostatný softvér, sú však potrebné ďalšie usmernenia týkajúce sa toho, kedy sa takéto produkty s digitálnymi prvkami považujú za uvedené na trh. Po ukončení výrobnej fázy softvéru a ponúknutí produktu s digitálnymi prvkami potenciálnym používateľom na trhu EÚ možno vychádzať z toho, že jeho výrobca vyrobil viacero kópií toho istého softvérového produktu s digitálnymi prvkami a dodal ich na účely distribúcie alebo používania. Na rozdiel od hmotných produktov s digitálnymi prvkami totiž samostatný softvér nepodlieha fyzickým obmedzeniam spojeným s výrobou alebo skladovými

([4]) Expertná skupina pre kybernetickú bezpečnosť produktov s digitálnymi prvkami v Registri expertných skupín Komisie a iných podobných subjektov.
([5]) Verejná konzultácia k návrhu usmernení Komisie k aktu o kybernetickej odolnosti.
([6]) Oznámenie Komisie Modrá príručka na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov 2022, 2022/C 247/01 (Ú. v. EÚ C 247, 29.6.2022, s. 1).

zásobami: každé sprístupnenie softvéru na stiahnutie alebo distribúciu má za následok vytvorenie novej identickej kópie pre používateľa. Pokiaľ sa táto verzia softvéru neupraví spôsobom, ktorý by ovplyvnil súlad s aktom o kybernetickej odolnosti, uvedenie na trh EÚ sa považuje za uskutočnené v okamihu prvého ponúknutia na distribúciu alebo použitie. Možnosť následného stiahnutia alebo distribúcie tejto verzie softvérového produktu s digitálnymi prvkami je preto potrebné považovať za okamih, keď je tento softvérový produkt s digitálnymi prvkami sprístupnený ([7]).

14. Samostatný softvérový produkt s digitálnymi prvkami by sa preto mal považovať za uvedený na trh v okamihu, keď je dokončená jeho výrobná fáza a keď je tento softvér po prvýkrát dodaný na distribúciu alebo používanie na trhu EÚ v priebehu obchodnej činnosti. Malo by sa vychádzať z predpokladu, že výrobca uviedol na trh súčasne viacero kópií toho istého softvérového produktu s digitálnymi prvkami. Z toho vyplýva, že hoci viaceré kópie toho istého softvéru zostávajú samostatnými produktmi s digitálnymi prvkami, považujú sa za uvedené na trh súčasne, bez ohľadu na to, kedy dochádza k prevodu vlastníctva alebo užívania každej jednotlivej kópie na inú fyzickú alebo právnickú osobu. Zároveň v prípade, že výrobca sprístupňuje softvér v rôznych variantoch, ktoré sa líšia obsiahnutými komponentmi, konfiguráciami alebo aktivovanými funkciami (napríklad verzie pre rôzne operačné systémy alebo balíky s odlišnými súbormi funkcií), tieto varianty nemožno považovať za viacero kópií toho istého softvérového produktu s digitálnymi prvkami. Z tohto dôvodu by sa mali na účely uvedenia na trh považovať za samostatné produkty s digitálnymi prvkami.

Príklad 1: 1. januára 2028 spoločnosť A po prvýkrát dodá na distribúciu prostredníctvom svojho webového sídla verziu 1.0.0 svojho softvéru X. V ten istý deň si zákazník 1 zakúpi kópiu verzie 1.0.0 softvéru X. Dňa 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 spĺňajú kritériá „podstatnej úpravy" softvérového produktu s digitálnymi prvkami, ktorý je už na trh uvedený, ako sa uvádza v odôvodnení 41 aktu o kybernetickej odolnosti. V prípade iterácií, ktoré sa nepovažujú za podstatné úpravy, výrobca nie je povinný vykonať nový postup posudzovania zhody, a preto sa nimi nemení dátum uvedenia daného softvéru na trh. Ďalšie informácie o pojme „podstatné úpravy" sú uvedené v oddiele 4. *Podstatné úpravy a náhradné diely*.

Príklad 2: 1. januára 2028 spoločnosť A po prvýkrát dodá na distribúciu prostredníctvom svojho webového sídla 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. Obe kópie softvéru X, verzie 1.0.0 aj 1.0.1, sa považujú za uvedené na trh 1. januára 2028.

16. Usmernenia uvedené v bodoch 13, 14 a 15 sa uplatňujú výlučne v prípade, ak pri produkte s digitálnymi prvkami ide o samostatný softvér. To však neplatí napríklad vtedy, keď je softvér kombinovaný s hardvérom, ako sa uvádza v oddiele *2.4. Kombinácia hardvéru a softvéru tvoriaca produkt s digitálnymi prvkami*.

2.2. **Softvér ako produkt s digitálnymi prvkami**

17. V článku 3 bode 1 aktu o kybernetickej odolnosti sa vymedzuje 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 patria do rozsahu pôsobnosti aktu o kybernetickej odolnosti, ak ich zamýšľaný účel alebo odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové prepojenie so zariadením alebo sieťou.

([7]) V súlade s článkom 13 ods. 11 môžu výrobcovia viesť verejné softvérové archívy na zlepšenie prístupu používateľov k historickým verziám. V takých prípadoch musia byť používatelia jasne a jednoducho dostupným spôsobom informovaní o rizikách spojených s používaním softvéru, ktorý už nie je podporovaný.

18. Akt o kybernetickej odolnosti sa preto môže vzťahovať na celý rad produktov s digitálnymi prvkami, medzi ktoré patria: i) samostatný softvér, ako sú aplikácie a počítačové programy, bez ohľadu na to, či sa distribuujú v digitálnej alebo fyzickej podobe; ii) hardvér so zabudovaným softvérom (napr. zariadenia internetu vecí, notebooky, tablety); iii) samostatný hardvér (napr. integrované obvody, základné dosky) a iv) akákoľvek kombinácia hardvéru a softvéru, ktoré sa dodávajú samostatne, ale sú určené na spoločnú prevádzku.

19. Samostatný softvér teda patrí do rozsahu pôsobnosti aktu o kybernetickej odolnosti, ak sa uvádza na trh ako produkt s digitálnymi prvkami. Treba rozlišovať medzi softvérovými produktmi s digitálnymi prvkami, na ktoré sa vzťahuje akt o kybernetickej odolnosti, a poskytovaním služieb na diaľku, ktoré do rozsahu pôsobnosti aktu o kybernetickej odolnosti nepatria.

20. Aby softvér patril do rozsahu pôsobnosti aktu o kybernetickej odolnosti, používateľovi musí byť poskytnutý softvérový produkt s digitálnymi prvkami, ktorý tento používateľ získal a ktorý prevádzkuje v rámci elektronického informačného systému na strane používateľa alebo ako jeho súčasť. Softvér, ktorý je stiahnutý, nainštalovaný alebo iným spôsobom dodaný používateľovi a ktorý sa spúšťa v elektronickom informačnom systéme používateľa, spĺňa tieto kritériá, a to aj v prípade, že má napríklad formu rozšírenia prehliadača alebo aplikácie vyvinutej s využitím webových technológií, ktorá je však dodaná na lokálne spustenie.

21. Naopak, softvér, ktorý sa spúšťa na diaľku a ku ktorému má používateľ iba prístup, nie je už len na základe tejto skutočnosti produktom s digitálnymi prvkami. V odôvodneniach 11 a 12 aktu o kybernetickej odolnosti sa v skutočnosti toto rozlíšenie vysvetľuje tak, že spracovanie alebo ukladanie na diaľku podlieha aktu o kybernetickej odolnosti len v rozsahu, v akom je to nevyhnutné na to, aby produkt s digitálnymi prvkami plnil svoje funkcie (t. j. prostredníctvom pojmu „spracovanie údajov na diaľku“ v zmysle článku 3 bodu 2), a nie pre samotný produkt s digitálnymi prvkami. To platí najmä pre webové aplikácie vrátane progresívnych webových aplikácií, ku ktorým sa pristupuje výlučne prostredníctvom webového prehliadača. To isté sa vzťahuje na webové sídla: hoci sa webové sídla môžu v obmedzenom rozsahu technicky spúšťať a vykonávať na zariadení používateľa, z odôvodnenia 12 aktu o kybernetickej odolnosti vyplýva, že samotné webové sídla sa nemajú považovať za produkty s digitálnymi prvkami a do rozsahu pôsobnosti aktu o kybernetickej odolnosti patria len vtedy, keď podporujú funkciu produktu s digitálnymi prvkami, t. j. v rozsahu, v akom spĺňajú podmienky na to, aby sa považovali za spracovanie údajov na diaľku (ako je podrobnejšie vysvetlené v oddiele *8*, a najmä v bode *8.1.2*. Bránila *by neexistencia takéhoto spracovania údajov produktu s digitálnymi prvkami plniť jednu z jeho funkcií?*).

Príklad 3: Mobilná aplikácia, ktorú si používateľ stiahne z obchodu s aplikáciami a nainštaluje do svojho smartfónu, je používateľovi dodaná a spúšťa sa na jeho zariadení, a preto ide o produkt s digitálnymi prvkami. Ak sa uvádza na trh v priebehu obchodnej činnosti, môže patriť do rozsahu pôsobnosti aktu o kybernetickej odolnosti.

Príklad 4: Používateľovi je dodaná aplikácia pre stolové počítače vytvorená s využitím webových technológií, ktorá je však zabalená na účely lokálnej inštalácie a spúšťa sa na zariadení používateľa, a preto ide o produkt s digitálnymi prvkami. Ak sa uvádza na trh v priebehu obchodnej činnosti, môže patriť do rozsahu pôsobnosti aktu o kybernetickej odolnosti.

Príklad 5: Webová aplikácia, ku ktorej má používateľ prístup výlučne prostredníctvom webového prehliadača, nie je produktom s digitálnymi prvkami. Pokiaľ nepodporuje funkciu produktu s digitálnymi prvkami, nepatrí do rozsahu pôsobnosti aktu o kybernetickej odolnosti. Naopak, aplikácia dodaná používateľovi vo forme lokálne nainštalovaného klienta, ktorá beží na zariadení používateľa, je produktom s digitálnymi prvkami. Ak sa uvádza na trh v priebehu obchodnej činnosti, môže patriť do rozsahu pôsobnosti aktu o kybernetickej odolnosti.

Ak sa tento klient pri vykonávaní jednej alebo viacerých svojich funkcií spolieha na spracovanie údajov na diaľku, ktoré spĺňa vymedzenie pojmu spracovanie údajov na diaľku, toto spracovanie údajov na diaľku je takisto súčasťou produktu s digitálnymi prvkami.

Príklad 6: Webové sídlo, ktoré svojim návštevníkom iba poskytuje informácie a nepodporuje funkciu produktu s digitálnymi prvkami, samo osebe nie je produktom s digitálnymi prvkami. Nepatrí teda do rozsahu pôsobnosti aktu o kybernetickej odolnosti.

2.3. **Počítačový kód**

22. Treba takisto objasniť, či zdrojový kód môže predstavovať softvérový produkt s digitálnymi prvkami. V akte o kybernetickej odolnosti sa softvér vymedzuje ako „časť elektronického informačného systému, ktorý pozostáva z počítačového kódu“ (článok 3 bod 4). Počítačový kód môže mať formu i) strojového kódu, čo je súbor inštrukcií priamo vykonávaných procesorom počítača, napísaných v binárnom formáte, alebo ii) zdrojového kódu, t. j. súboru inštrukcií a príkazov napísaných v programovacom jazyku, ktorý je potrebné skompilovať alebo interpretovať, aby ho mohol počítač spustiť. Vymedzenie pojmu softvér stanovené v akte o kybernetickej odolnosti zahŕňa obidve kategórie.

23. Samostatnou otázkou je, či dané dodanie počítačového kódu predstavuje uvedenie produktu s digitálnymi prvkami na trh EÚ, čo si vyžaduje dodanie v priebehu obchodnej činnosti. V prípade zdrojového kódu to však často neplatí. Napríklad fyzická alebo právnická osoba, ktorá zdieľa bezplatný počítačový kód s otvoreným zdrojovým kódom vo verejne prístupných úložiskách, sa na účely aktu o kybernetickej odolnosti vo všeobecnosti nepovažuje za subjekt, ktorý tento kód uvádza na trh EÚ (ako sa podrobnejšie rozoberá v oddiele *3. Slobodný softvér a softvér s otvoreným zdrojovým kódom*). Nedokončený kód, ktorý sa zdieľa počas fázy návrhu a vývoja produktu s digitálnymi prvkami (napr. na testovanie alebo preskúmanie), sa na účely aktu o kybernetickej odolnosti takisto nepovažuje za uvedený na trh, keďže fáza jeho výroby ešte nie je ukončená. Podobne sa na účely aktu o kybernetickej odolnosti nepovažuje za uvedený na trh ani vzorový alebo ukážkový kód poskytovaný ako súčasť návodov alebo školiacich materiálov ([8]).

24. Na druhej strane, ak výrobca poskytuje svojim zákazníkom počítačový kód ako produkt s digitálnymi prvkami, tento kód sa považuje za uvedený na trh, bez ohľadu na to, či ide o strojový kód alebo zdrojový kód ([9]).

Príklad 7: Spoločnosť A poskytuje spoločnosti B licenciu na zdrojový kód pre prispôsobiteľnú internú platformu a tento zdrojový kód jej poskytuje v podobe textového súboru. Aj keby si tento zdrojový kód vyžadoval pred použitím ďalšie úpravy a kompiláciu zo strany spoločnosti B, spoločnosť A tento zdrojový kód uvádza na trh, a preto sa na ňu vzťahuje akt o kybernetickej odolnosti. Spoločnosť A nezodpovedá za súlad následných úprav a kompilácie tohto kódu zo strany spoločnosti B s aktom o kybernetickej odolnosti.

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 na základe toho, ako alebo kedy je tento softvér dodaný používateľovi, ale na základe toho, či je softvér – vzhľadom na zamýšľaný účel produktu a jeho 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 od toho istého výrobcu, tento hardvér a uvedený 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 bol získaný prostredníctvom samostatného kanála (napr. cez obchod s aplikáciami, odkaz na stiahnutie alebo iný digitálny kanál po uvedení hardvérového produktu s digitálnymi prvkami na trh). Jeho uvedenie na trh sa teda uskutočňuje 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, pričom softvérové ovládače potrebné na odosielanie tlačových úloh, konfiguráciu zariadenia a riadenie jeho prevádzky sú k dispozícii na stiahnutie z webového sídla 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 športové zariadenie určené na meranie srdcovej frekvencie a aktivity používateľa, pričom na zobrazenie nameraných hodnôt, prehľad histórie a nastavenie zariadenia je potrebná aplikácia pre smartfóny, ktorú poskytuje výrobca. 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 funkčnosť produktu s digitálnymi prvkami.

([8]) Zároveň treba pripomenúť, že článok 4 ods. 3 umožňuje výrobcom sprístupňovať na trhu nedokončený softvér, ktorý nespĺňa požiadavky nariadenia, ako sú alfa verzie, beta verzie alebo kandidáti na finálnu verziu, pokiaľ sa nedokončený softvér sprístupňuje iba na čas potrebný na jeho testovanie a získanie spätnej väzby.

([9]) Na druhej strane je potrebné poznamenať, že na účely právnych predpisov o zodpovednosti za výrobok samotný počítačový kód nepredstavuje výrobok, a preto výrobcovia, ktorí takýto kód uvádzajú na trh, nemôžu byť zodpovední podľa smernice (EÚ) 2024/2853 (smernica o zodpovednosti za výrobky). V odôvodnení 13 danej smernice sa uvádza, že „[i]nformácie sa však za výrobok nepovažujú, a preto by sa pravidlá zodpovednosti za výrobok nemali vzťahovať na obsah digitálnych súborov, ako sú mediálne súbory, e-knihy alebo iba zdrojový kód softvéru“. To nevylučuje, že výrobcovia môžu niesť zodpovednosť podľa vnútroštátneho priestupkového práva.

2.5. **Dátové pripojenie**

26. V článku 2 ods. 1 sa uvádza, že akt o kybernetickej odolnosti „sa 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 aktu o kybernetickej odolnosti sa teda nezakladá na samotnej prítomnosti elektroniky, ale na schopnosti produktu s digitálnymi prvkami vymieňať si digitálne informácie.

27. Zatiaľ čo pojmy „logické pripojenie“ a „fyzické pripojenie“ sú vymedzené v článku 3, v akte o kybernetickej odolnosti nie sú vymedzené pojmy „dátové pripojenie“ ani „digitálne údaje“. Je preto užitočné stanoviť výklad pojmu „dátové pripojenie“, aby sa objasnili hranice rozsahu pôsobnosti aktu o kybernetickej odolnosti. Táto hranica je obzvlášť dôležitá na odlíšenie produktov s digitálnymi prvkami, ktoré iba využívajú elektrické signály, od tých, ktoré sa podieľajú na digitálnej komunikácii a sú preto vystavené kybernetickobezpečnostným rizikám.

28. Dátové pripojenie v najzákladnejšej podobe spočíva v prenose informácií v binárnej forme, t. j. vo forme postupnosti núl a jednotiek. Samotné zapínanie a vypínanie výstupu (t. j. 0/1) ešte samo osebe nepredstavuje dátové pripojenie, ak tieto stavy nemajú reprezentovať dáta alebo ak ich nečíta digitálny vstup. Aby mohlo existovať dátové pripojenie, binárne stavy musia byť zámerne kódované ako informácia zdrojom a v cieli musia byť ako informácia dekódovateľné. Inými slovami, musí existovať odosielateľ, ktorý zámerne generuje digitálne symboly podľa vopred stanovenej schémy, a príjemca, ktorý je schopný tieto symboly interpretovať ako dáta. Ak sa elektrické alebo elektronické signály používajú výlučne na spustenie alebo napájanie určitej funkcie bez prenosu digitálne kódovaných informácií, na účely aktu o kybernetickej odolnosti neexistuje žiadne dátové pripojenie, a preto produkt s digitálnymi prvkami nepatrí do rozsahu pôsobnosti článku 2 ods. 1.

2.6. **Zložité systémy**

29. Produkty s digitálnymi prvkami, na ktoré sa vzťahuje akt o kybernetickej odolnosti, môžu pozostávať nielen z jednotlivých zariadení alebo softvérových komponentov, ale aj zo zložitých systémov vrátane systémov zložených z viacerých hardvérových a softvérových prvkov, ktoré fungujú spoločne, a tak vykonávajú určitú funkciu. Ak sa takýto systém uvádza na trh ako samostatný produkt s digitálnymi prvkami, predstavuje produkt s digitálnymi prvkami v zmysle aktu o kybernetickej odolnosti.

30. Takéto zložité systémy sa často vyznačujú dlhými cyklami návrhu a vývoja, zmluvami, ktoré mohli byť podpísané ešte pred začatím uplatňovania aktu o kybernetickej odolnosti, predĺženou prevádzkovou životnosťou a vysokou mierou technickej a organizačnej zložitosti. Takéto systémy, ktoré majú byť uvedené na trh po začatí uplatňovania aktu o kybernetickej odolnosti, môžu vychádzať z komponentov uvedených na trh pred začatím uplatňovania aktu o kybernetickej odolnosti, zo zavedených architektúr alebo z bežne používaných noriem interoperability vrátane noriem uvedených v iných právnych predpisoch EÚ alebo v odvetvových rámcoch. V dôsledku toho môže byť úprava niektorých technických charakteristík týchto systémov náročná alebo neprimeraná bez toho, aby to malo vplyv na ich zamýšľaný účel, bezpečnosť, spoľahlivosť alebo interoperabilitu s existujúcou infraštruktúrou.

31. Tieto charakteristiky samy osebe nevylučujú komplexné systémy z rozsahu pôsobnosti aktu o kybernetickej odolnosti. Skôr ilustrujú uplatňovanie prístupu aktu o kybernetickej odolnosti založeného na riziku, ktorý v súlade s článkom 13 ods. 3 aktu o kybernetickej odolnosti umožňuje preukázať súlad rôznymi spôsobmi v závislosti od charakteristík a obmedzení produktu s digitálnymi prvkami. Tieto charakteristiky tvoria súčasť jeho zamýšľaného účelu a prevádzkového kontextu, a preto sú relevantné pri posudzovaní súladu so základnými požiadavkami kybernetickej bezpečnosti (ďalej len „základné požiadavky“). Konkrétne sa v odôvodnení 55 výslovne uznáva, že niektoré základné požiadavky nemusia byť plne zlučiteľné s povahou produktu s digitálnymi prvkami. Môže ísť napríklad o situáciu, keď by dodržanie týchto požiadaviek narušilo 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 takisto uvádza 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 si vyžaduje, aby produkt s digitálnymi prvkami spolupracoval s existujúcimi závislosťami alebo aby spĺňal určité požiadavky na interoperabilitu. V takýchto prípadoch by výrobcovia mali tieto konkrétne obmedzenia identifikovať a zdokumentovať, posúdiť súvisiace riziká a zaviesť primerané alternatívne alebo kompenzačné opatrenia na zmiernenie rizika, aby nedošlo k ohrozeniu bezpečnosti produktu s digitálnymi prvkami. Na tieto účely majú zásadný význam jednak technická dokumentácia uvedená v článku 31, jednak informácie a návod pre používateľa uvedené v prílohe II, a to pokiaľ ide o transparentný opis zistených obmedzení, súvisiacich kybernetickobezpečnostných rizík a zavedených opatrení na zmiernenie rizika. V súlade s povinnosťou aktualizovať posúdenie rizika počas obdobia poskytovania podpory by výrobcovia mali takisto pravidelne prehodnocovať, či takéto obmedzenia naďalej existujú. Ak je možné takéto obmedzenia v priebehu času odstrániť alebo zmierniť, výrobcovia by mali produkt s digitálnymi prvkami zodpovedajúcim spôsobom aktualizovať, aby sa dosiahla primeraná úroveň kybernetickej bezpečnosti ([10]).

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 kybernetickobezpečnostných rizík stanoví, že na zabezpečenie dôvernosti a integrity údajov, ktoré si produkt s digitálnymi prvkami vymieňa, je potrebné použiť zabezpečený komunikačný protokol.

Jeho zamýšľaný účel však zahŕňa interoperabilitu s existujúcimi systémami, ktoré podporujú iba starší alebo menej bezpečný protokol. V takýchto prípadoch môže výrobca tento protokol implementovať, ak je to potrebné na dosiahnutie interoperability, a to za predpokladu, že súvisiace kybernetickobezpečnostné riziká sú identifikované a zmiernené inými prostriedkami.

Ak je z technického hľadiska možné, aby produkt s digitálnymi prvkami podporoval tak zabezpečený protokol, ako aj menej bezpečný protokol, očakáva sa, že výrobca implementuje zabezpečený protokol a nastaví jeho používanie ako predvolené. Menej bezpečný protokol by bol povolený iba v prípadoch, keď je to nevyhnutné z hľadiska interoperability.

Príklad 11: Výrobca systému priemyselnej automatizácie nakúpi určité množstvo mikroradičov ešte predtým, ako sa začne uplatňovať akt o kybernetickej odolnosti. Výrobca sa vykoná posúdenie kybernetickobezpečnostných rizík svojho systému priemyselnej automatizácie, ktorý má byť uvedený na trh po začatí uplatňovania aktu o kybernetickej odolnosti. Na základe tohto posúdenia kybernetickobezpečnostných rizík výrobca nezistí žiadne konkrétne kybernetickobezpečnostné riziká spojené s používaním niektorého z týchto mikroradičov. Výrobca integruje mikroradič 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 aktu o kybernetickej odolnosti**

33. V niektorých prípadoch výrobca po začatí uplatňovania aktu o kybernetickej odolnosti 11. decembra 2027 uvedie na trh jednotky produktu s digitálnymi prvkami, ktoré boli vyrobené v súlade s typom alebo modelom navrhnutým a vyvinutým pred dátumom začatia uplatňovania aktu o kybernetickej odolnosti. V takýchto prípadoch sa pri dodržiavaní súladu s týmto nariadením nevyhnutne nevyžaduje, aby boli uvedené jednotky produktu s digitálnymi prvkami prepracované. Výrobca je v súlade s článkom 13 ods. 2 aktu o kybernetickej odolnosti povinný vykonať posúdenie kybernetickobezpečnostných rizík s cieľom určiť na základe zamýšľaného účelu a odôvodnene predvídateľného použitia produktu s digitálnymi prvkami, ktoré zo základných požiadaviek uvedených v prílohe I časti I sa na tento produkt s digitálnymi prvkami vzťahujú, a ako sa tieto požiadavky vykonávajú.

34. Ak z výsledkov tohto posúdenia rizík vyplýva, že produkt s digitálnymi prvkami už obsahuje primerané a účinné bezpečnostné opatrenia zamerané na riešenie príslušných rizík, výrobca sa na účely preukázania súladu s aktom o kybernetickej odolnosti môže opierať o tieto existujúce opatrenia. Samotným aktom o kybernetickej odolnosti sa neukladá povinnosť zavádzať nové bezpečnostné prvky ani prepracovať produkt s digitálnymi prvkami, ak to nie je potrebné na riešenie zistených rizík.

([10]) Treba poznamenať, že úvahy uvedené v tomto odseku sa môžu v náležitých prípadoch vzťahovať na všetky produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti aktu o kybernetickej odolnosti, a nielen na „zložité systémy".

35. Napriek tomu výrobca naďalej podlieha povinnostiam stanoveným v akte o kybernetickej odolnosti. Medzi ne patrí aj zabezpečenie toho, aby pred uvedením produktu s digitálnymi prvkami na trh bol vykonaný príslušný postup posudzovania zhody, aby bolo vyhotovené EÚ vyhlásenie o zhode a umiestnené označenie CE. Dodržiavanie týchto požiadaviek nezávisí od toho, či bolo v dôsledku posúdenia rizika potrebné upraviť návrh produktu s digitálnymi prvkami. V prípade produktov s digitálnymi prvkami, ktoré boli navrhnuté pred dátumom začatia uplatňovania aktu o kybernetickej odolnosti, ale uvedené na trh po tomto dátume, ak výrobca nie je schopný preukázať, ako bolo posúdenie rizika 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 kybernetickobezpečnostných rizík a na tomto základe preukázali, že produkt s digitálnymi prvkami obsahuje primerané bezpečnostné opatrenia s cieľom minimalizovať kybernetickobezpečnostné riziká, predchádzať incidentom a minimalizovať ich vplyv, a to aj v súvislosti so zdravím a bezpečnosťou používateľov.

36. Produkty s digitálnymi prvkami navrhnuté pred začatím uplatňovania aktu o kybernetickej odolnosti preto môžu byť uvedené na trh v súlade s aktom o kybernetickej odolnosti bez nutnosti ich prepracovania, za predpokladu, že výrobca prostredníctvom posúdenia kybernetickobezpečnostných rizík a technickej dokumentácie preukáže, 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 v prípade výrobcov produktov s digitálnymi prvkami, ktoré sa uvádzajú na trh po začatí uplatňovania aktu o kybernetickej odolnosti, ale sú vyrobené v súlade s typom alebo modelom navrhnutým a vyvinutým pred týmto dátumom, vhodné objasniť uplatňovanie povinností posudzovania zhody. 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 (príloha VII bod 6).

38. Uplatňovanie týchto požiadaviek je však potrebné vykladať s ohľadom na posúdenie kybernetickobezpečnostných rizík a na rizikový profil produktu s digitálnymi prvkami, pokiaľ ide o kybernetickú bezpečnosť. Najmä v prípade produktov s digitálnymi prvkami, ktoré boli navrhnuté pred dátumom začatia uplatňovania aktu o kybernetickej odolnosti (ale uvedené na trh po tomto dátume) a na ktoré sa vzťahujú postupy posudzovania zhody podľa článku 32 ods. 1, ak sa pri posúdení rizika preukáže, že produkt s digitálnymi prvkami už obsahuje primerané a účinné bezpečnostné opatrenia zamerané na riešenie rizík daného produktu, povinnosť predložiť dôkazy v rámci postupu posudzovania zhody by sa nemala vykladať 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 samo osebe neprispievalo k zvýšeniu bezpečnosti produktu s digitálnymi prvkami. Ak sú skúšky napriek tomu potrebné, od výrobcov sa neočakáva, že predložia dôkazy o skúškach vykonaných na všetkých variantoch produktov, takéto skúšky však môžu zoskupiť v rámci skupín produktov s digitálnymi prvkami, ako sa podrobnejšie 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 procesy riešenia zraniteľností stanovené v prílohe I časti II, mal by aktualizovať svoje posúdenie rizík v súlade s článkom 13 ods. 3 a takisto splniť všetky ostatné povinnosti stanovené v akte o kybernetickej odolnosti, a to aj poskytnutím informácií a návodu pre používateľa v súlade s článkom 13 ods. 18.

Príklad 12: Výrobca uvádza na trh mikroradič, ktorý bol navrhnutý a vyvinutý pred dátumom začatia uplatňovania aktu o kybernetickej odolnosti. Mikroradič je určený na integráciu do rôznych elektronických produktov s digitálnymi prvkami vrátane produktov s digitálnymi prvkami vybavenými funkciami pripojiteľnosti.

Pred uvedením nových jednotiek mikroradičov na trh po začatí uplatňovania aktu o kybernetickej odolnosti výrobca vykoná posúdenie kybernetickobezpečnostných rizík v súlade s článkom 13 ods. 2. Na základe zamýšľaného účelu mikroradiča a jeho odôvodnene predvídateľného použitia výrobca identifikuje relevantné kybernetickobezpečnostné riziká, ako sú neoprávnený prístup, manipulácia so softvérom alebo údajmi a zneužitie dostupných rozhraní.

Z výsledku posúdenia rizík vyplýva, že mikroradič v pôvodnej podobe už obsahuje primerané a účinné bezpečnostné opatrenia zamerané na riešenie zistených rizík. Výrobca preto dospel k záveru, že produkt s digitálnymi prvkami spĺňa príslušné základné požiadavky uvedené v prílohe I časti I a že nie je potrebná žiadna úprava návrhu ani zavedenie dodatočných bezpečnostných funkcií.

Ak nie je možné preukázať, ako sa posúdenie kybernetickobezpečnostných rizík zohľadnilo počas pôvodnej fázy návrhu a vývoja, výrobca zdokumentuje aktuálne posúdenie kybernetickobezpečnostných rizík a vysvetlí, ako existujúci návrh a opatrenia zmierňujú zistené riziká. Od výrobcu sa nevyžaduje, aby nanovo vytváral historickú dokumentáciu týkajúcu sa návrhu alebo testovania, keďže by to neprispelo k zvýšeniu kybernetickej bezpečnosti produktu s digitálnymi prvkami. Ak je viacero variantov mikroradiča založených na rovnakom návrhu a vyznačuje sa rovnakým rizikovým profilom, pokiaľ ide o kybernetickú bezpečnosť, výrobca sa môže opierať aj o reprezentatívne dôkazy týkajúce sa príslušnej skupiny produktov.

Výrobca zabezpečuje aj súlad s požiadavkami na riešenie zraniteľností stanovenými v prílohe I časti II, a to aj prostredníctvom udržiavania procesov na riešenie a odstraňovanie zraniteľností a prostredníctvom priebežného prehodnocovania posúdenia kybernetickobezpečnostných rizík v súlade s článkom 13 ods. 3.

Za týchto okolností sa mikroradič navrhnutý pred dátumom začatia uplatňovania aktu o kybernetickej odolnosti môže uviesť na trh bez nutnosti jeho prepracovania, ak výrobca prostredníctvom posúdenia kybernetickobezpečnostných rizík a technickej dokumentácie preukáže, že mikroradič dosahuje primeranú úroveň kybernetickej bezpečnosti s ohľadom na jeho 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 oddiele *2.1. Uvedenie na trh*, akt o kybernetickej odolnosti sa vzťahuje na produkty s digitálnymi prvkami, ktoré sú v priebehu obchodnej činnosti po prvýkrát sprístupnené na trhu EÚ (t. j. „uvedené na trh“), ako aj na každý ďalší prípad, ktorý predstavuje sprístupnenie toho istého produktu s digitálnymi prvkami na trhu. V modrej príručke (oddiel 2.2) sa objasňuje, že pod pojmom „obchodná činnosť“ sa rozumie poskytovanie tovaru za odplatu alebo bezodplatne v súvislosti s podnikaním a túto činnosť možno posudzovať iba individuálne v každom konkrétnom prípade, pričom sa zohľadňujú pravidelnosť dodávok, charakteristiky výrobku, zámery dodávateľa atď.

41. Dodávka v priebehu obchodnej činnosti sa vyznačuje radom okolností, ktoré sú podrobne zdokumentované v Modrej príručke a pripomenuté v odôvodnení 15 aktu o kybernetickej odolnosti. Môžu medzi ne patriť priamo 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) ([11]).

42. V akte o kybernetickej odolnosti sa však zohľadňujú špecifiká rôznych spôsobov vývoja a zverejňovania „slobodného softvéru a softvéru s otvoreným zdrojovým kódom“ a ponúkajú sa určité usmernenia, ktoré pomáhajú určiť, či v prípade slobodného softvéru a softvéru s otvoreným zdrojovým kódom ide o produkt s digitálnymi prvkami uvádzaný na trh (t. j. v priebehu obchodnej činnosti) v zmysle aktu o kybernetickej odolnosti. Ako je vysvetlené v odôvodnení 18, „samotné okolnosti, za ktorých bol produkt s digitálnymi prvkami vyvinutý, alebo spôsob financovania vývoja by sa […] nemali zohľadňovať pri určovaní toho, či ide o činnosť obchodnej alebo neobchodnej povahy“. Konkrétnejšie, „poskytovanie produktov s digitálnymi prvkami považovanými za slobodný softvér a softvér s otvoreným zdrojovým kódom, ktoré ich výrobcovia nespeňažujú, [by sa] nemalo považovať za obchodnú činnosť, aby sa zabezpečilo jasné rozlíšenie medzi fázou vývoja a fázou dodávky“.

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

43. Preto je užitočné i) objasniť, čo je slobodný softvér a softvér s otvoreným zdrojovým kódom; ii) kedy sa považuje za zodpovednosť fyzickej alebo právnickej osoby, a iii) uviesť príklady, ktoré pomôžu zainteresovaným stranám pochopiť, kedy distribúcia slobodného softvéru a softvéru s otvoreným zdrojovým kódom predstavuje uvedenie na trh. Ak sa slobodný softvér a softvér s otvoreným zdrojovým kódom neuvádza na trh, nepatrí do rozsahu pôsobnosti aktu o kybernetickej odolnosti, pokiaľ subjekt, ktorý ho zverejňuje, nie je právnickou osobou, ktorá spĺňa vymedzenie pojmu „správca softvéru s otvoreným zdrojovým kódom“ (ďalej len „správca“) podľa článku 3 bodu 14. V takom prípade sa naň vzťahujú iba povinnosti stanovené v článku 24.

44. V článku 3 bode 48 sa slobodný softvér a softvér s otvoreným zdrojovým kódom vymedzuje 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 sa v týchto usmerneniach neuvádzajú konkrétne bezplatné a otvorené licencie, ktoré sú zlučiteľné s vymedzením pojmu stanoveným v článku 3 bode 48, zo znenia tohto ustanovenia vyplýva, že na účely aktu o kybernetickej odolnosti sa za slobodný softvér a softvér s otvoreným zdrojovým kódom považuje iba softvér, ktorý súčasne spĺňa dve podmienky: i) musí byť sprístupnený na základe bezplatnej a otvorenej licencie, ktorá udeľuje všetky práva uvedené v článku 3 bode 48 a ii) jeho zdrojový kód musí byť voľne dostupný.

45. V požiadavke, aby licencia zabezpečovala „voľný prístup k [softvéru], jeho použiteľnosť, modifikovateľnosť a redistribúciu“, sa zohľadňuje tradičné chápanie slobodného softvéru a softvéru s otvoreným zdrojovým kódom, a to konkrétne skutočnosť, že používatelia musia mať prístup k zdrojovému kódu, môžu tento softvér používať bez neprimeraných obmedzení, upravovať ho a redistribuovať pôvodné alebo upravené verzie. Prístup k zdrojovému kódu je preto nevyhnutnou podmienkou uplatňovania ostatných práv: bez prístupu k zdrojovému kódu nie je prakticky možné softvér upravovať ani zmysluplne opätovne využívať.

46. Článok 3 bod 48 však ide nad rámec toho, aby odkazoval len na licenčné podmienky, pretože sa v ňom výslovne vyžaduje, aby zdrojový kód bol „voľne dostupný“. Pojem „voľne dostupný“ znamená, že zdrojový kód musí byť verejne sprístupnený (buď „smerom k pôvodnému zdroju“, alebo „smerom k následným používateľom“) a nestačí, ak sa poskytuje len na obmedzenom alebo podmienenom základe. V súlade s tým sa softvér distribuovaný na základe bezplatnej a otvorenej licencie, ktorého zdrojový kód je však dostupný (alebo môže byť dostupný) len platiacim zákazníkom alebo obmedzenej skupine používateľov, nepovažuje za slobodný softvér a softvér s otvoreným zdrojovým kódom v zmysle článku 3 bodu 48. Na účely aktu o kybernetickej odolnosti by sa preto za slobodný softvér a softvér s otvoreným zdrojovým kódom mal považovať iba softvér, ktorého zdrojový kód je verejne dostupný a licencovaný na základe bezplatnej a otvorenej licencie udeľujúcej úplný súbor práv uvedených v článku 3 bode 48.

3.1. **Určenie toho, kto je zodpovedný za slobodný softvér a softvér s otvoreným zdrojovým kódom**

47. V akte o kybernetickej odolnosti sa hlavná zodpovednosť ukladá hospodárskym subjektom, ktoré dodávajú produkty s digitálnymi prvkami na trh EÚ. Podľa aktu sa za výrobcu považuje fyzická alebo právnická osoba, ktorá dodáva produkt s digitálnymi prvkami pod svojím menom alebo ochrannou známkou a ktorá tak koná v priebehu obchodnej činnosti (čím produkt uvádza na trh). Podobne sa za dovozcu považuje fyzická alebo právnická osoba usadená v EÚ, ktorá dodáva produkt s digitálnymi prvkami od osoby usadenej mimo EÚ a ktorá tak koná v priebehu obchodnej činnosti (čím produkt uvádza na trh). Povinnosti správcov sa vzťahujú na právnickú osobu, ktorá dodáva slobodný softvér a softvér s otvoreným zdrojovým kódom určený na obchodné účely ([12]), neuvádza ho však na trh v zmysle aktu o kybernetickej odolnosti.

48. Na to, aby bolo možné určiť, či fyzická alebo právnická osoba uvádza slobodný softvér a softvér s otvoreným zdrojovým kódom na trh EÚ, je preto najskôr potrebné objasniť, či táto fyzická alebo právnická osoba slobodný softvér a softvér s otvoreným zdrojovým kódom skutočne dodáva. Na správne stanovenie príslušných povinností vyplývajúcich z aktu o kybernetickej odolnosti je nutné určiť, či fyzická alebo právnická osoba skutočne vykonáva činnosť dodávania slobodného softvéru a softvéru s otvoreným zdrojovým kódom. Ako sa uvádza v odôvodnení 18, akt o kybernetickej odolnosti sa v skutočnosti nevzťahuje na fyzické ani právnické osoby, ktoré prispievajú zdrojovým kódom k produktom s digitálnymi prvkami kvalifikovaným ako slobodný softvér a softvér s otvoreným zdrojovým kódom, za ktoré nenesú zodpovednosť.

([12]) Ide o nevyhnutnú, ale nie postačujúcu podmienku na to, aby sa právnická osoba mohla považovať za správcu softvéru s otvoreným zdrojovým kódom, keďže vo vymedzení pojmu uvedenom v článku 3 bode 14 sa stanovujú ďalšie podmienky, ktoré musí právnická osoba splniť, aby sa mohla považovať za správcu.

49. Vzhľadom na špecifiká vývoja slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktorý často zahŕňa viacerých prispievateľov, decentralizované modely spolupráce a oddelenie prispievania od rozhodovania, je užitočné objasniť, že slobodný softvér a softvér s otvoreným zdrojovým kódom sa považuje za taký, ktorý je „na zodpovednosť“ fyzických alebo právnických osôb, ktoré ho zverejňujú a vykonávajú primárnu kontrolu nad jeho vývojom, vydaniami verzií a rozhodnutiami o distribúcii (často sa označujú ako „subjekty vykonávajúce údržbu“). Osoby, ktoré prispievajú zdrojovým kódom, ale nemajú vplyv na vydávanie verzií, plány ani rozhodnutia týkajúce sa riadenia, sa považujú za „prispievateľov“; V takýchto prípadoch nezodpovedajú za slobodný softvér a softvér s otvoreným zdrojovým kódom, hoci do neho prispeli kódom. Samotná existencia technických povolení, ako je napríklad prístup na zápis, nestačí na to, aby sa dalo konštatovať, že daná osoba nesie zodpovednosť za slobodný softvér a softvér s otvoreným zdrojovým kódom; zodpovednosť nesú tí, ktorí tento slobodný softvér a softvér s otvoreným zdrojovým kódom zverejňujú a riadia.

Príklad 13: Konkrétny vývojár alebo zamestnanec spoločnosti predloží do projektu slobodného softvéru a softvéru s otvoreným zdrojovým kódom žiadosť o „prijatie zmien“ alebo „zlúčenie“ obsahujúcu bezpečnostnú záplatu alebo novú funkciu. Subjekty vykonávajúce údržbu projektu kód skontrolujú, schvália a zlúčia do hlavného úložiska, pričom ho následne zahrnú do novej verzie. V tomto prípade je osoba, ktorá odoslala žiadosť o prijatie zmien, „prispievateľom“ a nevzťahuje sa na ňu akt o kybernetickej odolnosti. Hoci táto osoba prispela zdrojovým kódom, nemá primárnu kontrolu nad vývojom, vydávaním verzií ani rozhodnutiami o distribúcii.

3.2. **Určenie toho, či sa slobodný softvér a softvér s otvoreným zdrojovým kódom uvádza na trh EÚ**

50. Keď sa zistí, že slobodný softvér a softvér s otvoreným zdrojovým kódom zodpovedá fyzická alebo právnická osoba, je potrebné zistiť, či ho táto osoba dodáva v rámci obchodnej činnosti, čo predstavuje uvedenie na trh.

3.2.1. *Účtovanie ceny*

51. Ak fyzická alebo právnická osoba, ktorá dodáva slobodný softvér a softvér s otvoreným zdrojovým kódom, účtuje cenu za samotný softvér (napr. tým, že účtuje cenu za vopred skompilované binárne súbory), uvádza na trh produkt s digitálnymi prvkami. Osoba, ktorá uvádza slobodný softvér a softvér s otvoreným zdrojovým kódom na trh, je preto podľa aktu o kybernetickej odolnosti výrobcom.

52. Výrobcovia slobodného softvéru a softvéru s otvoreným zdrojovým kódom často dodávajú bezplatné verzie tohto softvéru (neraz nazývané „komunitné“ verzie), ktorých kódová základňa je (takmer) totožná s platenou verziou. Uvedené produkty s digitálnymi prvkami sú však iné produkty: platená verzia je nejakým spôsobom speňažená (napr. buď účtovaním ceny alebo inými spôsobmi, ako sa uvádza v tomto oddiele), a preto sa považuje za uvedenú na trh, z čoho vyplývajú povinnosti výrobcu. Verzia poskytovaná bezplatne (alebo komunitná verzia) sa nespeňažuje, a preto sa na účely aktu o kybernetickej odolnosti nepovažuje za uvedenú na trh. To platí aj v prípade, keď je platená verzia „vylepšenou“ komerčnou verziou, ktorá rozširuje kódovú základňu verzie poskytovanej bezplatne alebo túto verziu začleňuje do širšieho produktu s digitálnymi prvkami (napr. ako v prípade modelu „open-core“).

53. Ak je dodávateľom komunitnej verzie právnická osoba, v súvislosti s verziou, ktorú dodáva bezplatne (komunitná verzia), podlieha táto právnická osoba aj povinnostiam správcov. Ak je subjekt fyzická osoba, bezplatná verzia (komunitná verzia) nepatrí do rozsahu pôsobnosti aktu o kybernetickej odolnosti.

3.2.2. *Speňaženie iných služieb alebo požiadavka na spracovanie osobných údajov*

54. Fyzická alebo právnická osoba, ktorá zverejňuje slobodný softvér a softvér s otvoreným zdrojovým kódom, môže tento softvér zároveň uvádzať na trh (t. j. dodávať ho v priebehu obchodnej činnosti), ak poskytuje softvér, prostredníctvom ktorého speňažuje iné produkty s digitálnymi prvkami alebo služby, alebo ak ako podmienku použitia vyžaduje spracovanie osobných údajov z iných dôvodov, ako je výlučne zlepšenie bezpečnosti, kompatibility alebo interoperability softvéru.

Príklad 14: Fyzická alebo právnická osoba zverejňuje slobodnú aplikáciu a aplikáciu s otvoreným zdrojovým kódom určenú na trh. Aplikácia je k dispozícii bezplatne a umožňuje používateľom, aby jej prostredníctvom nakupovali tovar alebo služby. Aplikácia umožňuje osobe, ktorá ju zverejnila, zarábať na ďalších produktoch s digitálnymi prvkami a službách, ktoré sa prostredníctvom aplikácie ponúkajú (napr. v podobe reklám, provízií alebo poplatkov za predplatné). Aplikácia sa preto považuje za uvedenú na trh v priebehu obchodnej činnosti.

Príklad 15: Fyzická alebo právnická osoba zverejňuje slobodnú VPN a VPN s otvoreným zdrojovým kódom. Aplikácia je k dispozícii bezplatne, umožňuje však používateľom za poplatok získať prístup k ďalším serverom alebo vyhradeným IP adresám. Táto aplikácia umožňuje danej osobe speňažiť iné služby, ktoré sa prostredníctvom aplikácie ponúkajú, a preto sa považuje za uvedenú na trh v priebehu obchodnej činnosti.

Príklad 16: Fyzická alebo právnická osoba zverejňuje slobodnú aplikáciu a aplikáciu s otvoreným zdrojovým kódom na sledovanie fyzickej zdatnosti. Aplikácia je k dispozícii bezplatne, jej používanie je však podmienené spracovaním osobných údajov používateľov na účely, ako sú cielená reklama alebo analytika, ktoré nesúvisia s bezpečnosťou, kompatibilitou ani interoperabilitou softvéru. Keďže aplikácia vyžaduje spracovanie týchto údajov ako podmienku používania, považuje sa za uvedenú na trh v priebehu obchodnej činnosti.

3.2.3. *Podporné služby*

55. Samotná skutočnosť, že fyzická alebo právnická osoba, ktorá zverejňuje slobodný softvér a softvér s otvoreným zdrojovým kódom, ponúka aj súvisiace platené podporné služby, ešte sama osebe neznamená, že produkt s digitálnymi prvkami sa dodáva v priebehu obchodnej činnosti. Podporné služby môžu zahŕňať činnosti, ako sú poradenstvo, školenie alebo odborné služby súvisiace s používaním, dokumentáciou, konfiguráciou a nasadením softvéru zo strany zákazníka.

56. Rozhodujúcim faktorom je to, či je prístup k samotnému slobodnému softvéru a softvéru s otvoreným zdrojovým kódom (t. j. poskytovanie produktu s digitálnymi prvkami), vrátane jeho údržby, podmienený odmenou, a nie len ponukou odborných služieb týkajúcich sa voľne dostupného produktu s digitálnymi prvkami, ako sa uvádza v odôvodnení 18 aktu o kybernetickej odolnosti („poskytovanie produktov s digitálnymi prvkami považovanými za slobodný softvér a softvér s otvoreným zdrojovým kódom, ktoré ich výrobcovia nespeňažujú, [by sa] nemalo považovať za obchodnú činnosť“). Ak je možné slobodný softvér a softvér s otvoreným zdrojovým kódom bezplatne stiahnuť a nainštalovať a používatelia si môžu voliteľne zakúpiť odborné služby osobitne, tento slobodný softvér a softvér s otvoreným zdrojovým kódom 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 podpora alebo optimalizácia výkonu, podmienený odmenou. V takýchto prípadoch toto poskytnutie predstavuje speňažené poskytnutie produktu s digitálnymi prvkami dodaného v priebehu obchodnej činnosti, a preto sa produkt považuje za uvedený na trh. To zahŕňa aj prípady, keď sú platené vydanie alebo podniková verzia sprístupnené na základe obchodnej zmluvy, a to bez ohľadu na to, či je funkčne rovnocenný softvér k dispozícii aj bezplatne na základe bezplatnej a otvorenej licencie.

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

Príklad 18: Fyzická alebo právnická osoba zverejňuje bezplatný nástroj s otvoreným zdrojovým kódom určený na používanie z príkazového riadka. Tento nástroj je voľne dostupný a každý si ho môže stiahnuť a nainštalovať. Daná fyzická alebo právnická osoba samostatne ponúka odborné služby, ako napríklad voliteľné poradenské služby zamerané na zaškolenie používateľov a podporu pri inštalácii a používaní nástroja. Tento slobodný softvér a softvér s otvoreným zdrojovým kódom sa nepovažuje za uvedený na trh v zmysle aktu o kybernetickej odolnosti.

58. Najmä v prípade fyzických osôb, ktoré zverejňujú slobodný softvér a softvér s otvoreným zdrojovým kódom, by sa poskytovanie technickej pomoci priamo spojenej s prístupom k produktu s digitálnymi prvkami stále nepovažovalo za obchodnú činnosť, pokiaľ by, ako sa uvádza v odôvodnení 15 aktu o kybernetickej odolnosti, účtovaná cena slúžila výlučne na náhradu 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 slobodný softvér a softvér s otvoreným zdrojovým kódom a ponúka technickú pomoc s cieľom pokryť svoje náklady a získať primeranú odmenu, nesmie len na základe tejto skutočnosti považovať za subjekt, ktorý tento softvér uvádza na trh EÚ.

59. Fyzická alebo právnická osoba, ktorá poskytuje technickú pomoc súvisiacu so slobodným softvérom a softvérom s otvoreným zdrojovým kódom, za ktorý nenesie zodpovednosť, sa nepovažuje za subjekt uvádzajúci tento softvér na trh, pokiaľ daná osoba v rámci poskytovania takejto pomoci podstatne neupravuje slobodný softvér a softvér s otvoreným zdrojovým kódom v súlade s článkom 22.

Príklad 19: Poskytovateľ služieb nezverejňuje slobodný softvér a softvér s otvoreným zdrojovým kódom, ale pomáha zákazníkovi s jeho inštaláciou na jeho lokálnom serveri. Robí to bez toho, aby vykonal podstatnú úpravu tohto slobodného softvéru a softvéru s otvoreným zdrojovým kódom. Poskytovateľ služby sa preto nepovažuje za subjekt, ktorý uvádza slobodný softvér a softvér s otvoreným zdrojovým kódom na trh.

3.2.4. *Dary*

60. Fyzické alebo právnické osoby, ktoré zverejňujú projekty slobodného softvéru a softvéru s otvoreným zdrojovým kódom, zvyčajne poskytujú používateľom tohto softvéru možnosť dobrovoľne prispieť finančnou sumou, aby tak vyjadrili vďaku vydavateľom projektu a zároveň zabezpečili, že projekt bude naďalej aktívne udržiavaný.

61. Ako sa uvádza v odôvodnení 15 aktu o kybernetickej odolnosti, „prijímanie darov bez úmyslu dosiahnuť zisk by sa nemalo považovať za obchodnú činnosť“. Samotné uvedenie odkazu na darcovskú platformu alebo podobné nástroje na zbieranie darov by sa nemalo považovať za úmysel dosiahnuť zisk, a to ani v prípade, ak suma vyzbieraná prostredníctvom darov presiahne 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 zo svojej podstaty v priebehu času menia, a preto je pri posudzovaní toho, či sa slobodný softvér a softvér s otvoreným zdrojovým kódom speňažený výlučne prostredníctvom darov považuje za uvedený na trh, postupovať s určitou mierou flexibility. Je teda nepravdepodobné, že by sa slobodný softvér a softvér s otvoreným zdrojovým kódom podporovaný výlučne prostredníctvom darov považoval za produkt uvedený na trh v zmysle aktu o kybernetickej odolnosti.

Príklad 20: Fyzická alebo právnická osoba zverejní nástroj v podobe slobodného softvéru a softvéru s otvoreným zdrojovým kódom vo verejnom online úložisku, čím umožní komukoľvek, aby si ho stiahol, používal, upravoval a ďalej šíril na základe bezplatnej a otvorenej licencie. Vydavateľ vyzýva používateľov, aby prostredníctvom darcovskej platformy prispeli dobrovoľnými darmi na podporu ďalšieho rozvoja a údržby projektu. Prístup k softvéru, jeho zdrojovému kódu a aktualizáciám nie je podmienený poskytnutím daru. Tento slobodný softvér a softvér s otvoreným zdrojovým kódom sa nepovažuje za dodaný v priebehu obchodnej činnosti a nepovažuje sa za uvedený na trh v zmysle aktu o kybernetickej odolnosti.

62. Existujú však prípady, keď sa slobodný softvér a softvér s otvoreným zdrojovým kódom podporovaný výlučne prostredníctvom darov môže považovať za produkt uvedený na trh. Ide o situáciu, keď na základe celkového posúdenia okolností dary *de facto* zodpovedajú účtovaniu ceny za prístup k produktu s digitálnymi prvkami alebo k niektorým jeho funkciám. To môže platiť najmä vtedy, keď je prístup k slobodnému softvéru a softvéru s otvoreným zdrojovým kódom, k základným funkciám alebo k aktualizáciám v praxi podmienený poskytnutím daru, alebo keď sú dary spojené so zmluvným plnením či exkluzívnymi výhodami, ktoré presahujú rámec výhod poskytovaných komunitou.

Príklad 21: Fyzická alebo právnická osoba zverejňuje softvérový produkt s digitálnymi prvkami na základe bezplatnej a otvorenej licencie, ale verzie na stiahnutie a bezpečnostné aktualizácie poskytuje len používateľom, ktorí prispeli darom. Používatelia, ktorí neposkytnú dar, 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 slobodný softvér a softvér s otvoreným zdrojovým kódom sa preto považuje za uvedený na trh v zmysle aktu o kybernetickej odolnosti.

Príklad 22: Fyzická alebo právnická osoba sprístupňuje zdrojový kód slobodného softvéru a softvéru s otvoreným zdrojovým kódom verejnosti, vopred skompilované binárne súbory, pravidelné aktualizácie a zaručené bezpečnostné opravy však poskytuje iba darcom. V tomto prípade sú dary spojené s prístupom k základným aspektom produktu s digitálnymi prvkami a predstavujú odmenu za dodanie tohto produktu. Tento slobodný softvér a softvér s otvoreným zdrojovým kódom sa preto považuje za uvedený na trh v priebehu obchodnej činnosti.

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

63. Samotná skutočnosť, že tretia strana zaplatila za vývoj slobodného softvéru a softvéru s otvoreným zdrojovým kódom, sponzorovala ho alebo inak financovala, ešte sama osebe neurčuje, či je tento slobodný softvér a softvér s otvoreným zdrojovým kódom uvedený na trh. V ekosystéme slobodného softvéru a softvéru s otvoreným zdrojovým kódom je bežnou praxou, že konkrétni vývojári, nadácie alebo komunity získavajú finančné prostriedky od spoločností, verejných inštitúcií alebo iných sponzorov s cieľom pracovať na konkrétnych funkciách, odstraňovať chyby alebo udržiavať kľúčové komponenty. Toto financovanie môže mať mnoho foriem vrátane grantov, odmien za nájdenie chýb, sponzorstiev, zmlúv o poskytovaní služieb alebo platených vývojárskych prác.

64. Ako už bolo pripomenuté, v odôvodnení 18 aktu o kybernetickej odolnosti sa objasňuje, že samotné okolnosti, za ktorých bol produkt s digitálnymi prvkami vyvinutý, alebo spôsob financovania vývoja by sa nemali zohľadňovať pri určovaní toho, či ide o činnosť obchodnej povahy.

65. Preto v prípadoch, keď je slobodný softvér a softvér s otvoreným zdrojovým kódom voľne dostupný a voľne sprístupnený všetkým na účely prístupu, používania, úpravy a redistribúcie, skutočnosť, že obchodný subjekt mohol za daný projekt zaplatiť, by nemala byť faktorom pri určovaní, či je tento softvér uvedený na trh. V skutočnosti, ak sa tento slobodný softvér a softvér s otvoreným zdrojovým kódom inak nespeňažuje, nemožno ho považovať za uvedený na trh. Ak spoločnosť, ktorá financovala vývoj slobodného softvéru a softvéru s otvoreným zdrojovým kódom (rovnako ako akákoľvek iná spoločnosť), integruje tento softvér do svojho produktu s digitálnymi prvkami, je povinná postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5 aktu o kybernetickej odolnosti.

Príklad 23: Konkrétny vývojár zverejňuje projekt slobodného softvéru a softvéru s otvoreným zdrojovým kódom a aktívne ho udržiava. Výrobca A požiada konkrétneho vývojára, aby do daného slobodného softvéru a softvéru s otvoreným zdrojovým kódom pridal určitú funkciu, a tento vývoj financuje. Vývojár pridá túto funkciu do kódovej základne slobodného softvéru a softvéru s otvoreným zdrojovým kódom, otvorene ju zdieľa a sprístupňuje ju všetkým bezplatne na účely prístupu, používania, úpravy a redistribúcie. Konkrétny vývojár sa nepovažuje za subjekt, ktorý uvádza slobodný softvér a softvér s otvoreným zdrojovým kódom na trh. Ak výrobca integruje slobodný softvér a softvér s otvoreným zdrojovým kódom do svojho produktu s digitálnymi prvkami, je povinný postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

3.2.6. *Neziskové subjekty zriadené na dosiahnutie neziskových cieľov*

66. Ak je právnická osoba, ktorá zverejňuje slobodný softvér a softvér s otvoreným zdrojovým kódom, nezisková organizácia „zriadená tak, aby sa zabezpečilo, že všetky príjmy po odpočítaní nákladov sa použijú na dosiahnutie neziskových cieľov“ (odôvodnenie 18 aktu o kybernetickej odolnosti), slobodný softvér a softvér s otvoreným zdrojovým kódom, ktorý zverejňuje, sa nepovažuje za uvedený na trh. Ak táto právnická osoba spĺňa vymedzenie pojmu „správca“, podlieha príslušným povinnostiam (článok 24 aktu o kybernetickej odolnosti).

Príklad 24: Právnická osoba zverejňuje bezplatný prehliadač s otvoreným zdrojovým kódom, ktorý je priamo speňažovaný prostredníctvom partnerstiev s vyhľadávačmi, všetky jej príjmy po odpočítaní nákladov sa však využívajú na neziskové ciele. Prehliadač sa nepovažuje za uvedený na trh v zmysle aktu o kybernetickej odolnosti. Právnická osoba, ktorá ho zverejňuje, podlieha povinnostiam vzťahujúcim sa na správcov.

3.2.7. *Integrácia inými výrobcami*

67. V niektorých prípadoch je slobodný softvér a softvér s otvoreným zdrojovým kódom zverejnený jasne identifikovateľnou fyzickou alebo právnickou osobou, avšak tento slobodný softvér a softvér s otvoreným zdrojovým kódom je „určen[ý] na integráciu inými výrobcami do ich vlastných produktov s digitálnymi prvkami“. V takýchto prípadoch sa tento slobodný softvér a softvér s otvoreným zdrojovým kódom nepovažuje za uvedený na trh EÚ, pokiaľ ho osoba, ktorá ho zverejňuje (t. j. pôvodný výrobca), zároveň nespeňažuje v súlade s predchádzajúcimi oddielmi týchto usmernení.

68. Ak sa tento slobodný softvér a softvér s otvoreným zdrojovým kódom neuvádza na trh, právnická osoba, ktorá ho zverejňuje, by v súlade s vymedzením pojmu „správca“ podliehala povinnostiam správcov, keby poskytovala podporu na trvalej báze.

Príklad 25: Právnická osoba zverejňuje knižnicu slobodného softvéru a softvéru s otvoreným zdrojovým kódom určenú na tvorbu používateľských rozhraní. Dodávku knižnice nespeňažuje, ale integruje ju do jedného zo svojich produktov s digitálnymi prvkami (ktorý sa následne uvádza na trh). Knižnica sa nepovažuje za uvedenú na trh v zmysle aktu o kybernetickej odolnosti, je však určená na integráciu do produktov s digitálnymi prvkami. Právnická osoba, ktorá ju zverejňuje, je jej správcom.

Príklad 26: Právnická osoba uvádza na trh operačný systém a zároveň zverejňuje knižnice slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktoré slúžia ako referenčné implementácie pre používateľov tohto operačného systému. Právnická osoba nespeňažuje knižnice slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktoré sú určené na integráciu do iných produktov s digitálnymi prvkami. Právnická osoba, ktorá ich zverejňuje, je správcom týchto knižníc slobodného softvéru a softvéru s otvoreným zdrojovým kódom.

3.3. **Správcovia softvéru s otvoreným zdrojovým kódom**

69. V akte o kybernetickej odolnosti sa zavádza nová právna kategória „správca 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 [aktu o kybernetickej odolnosti]“ (odôvodnenie 19 aktu o kybernetickej odolnosti).

70. V niektorých prípadoch sa slobodný softvér a softvér s otvoreným zdrojovým kódom zverejňuje, ale nesprístupňuje na trhu v zmysle aktu o kybernetickej odolnosti právnickou osobou, ktorej „účelom alebo cieľom je systematicky a trvalo podporovať vývoj [slobodného softvéru a softvéru s otvoreným zdrojovým kódom] […] určených na obchodné činnosti, a ktorá zabezpečuje životaschopnosť týchto produktov“ (článok 3 bod 14 aktu o kybernetickej odolnosti). V takýchto prípadoch sa na túto právnickú osobu vzťahujú povinnosti správcov.

71. Pojem správca je vymedzený ako „právnická osoba iná ako výrobca“, pretože výrobcom je podľa vymedzenia fyzická alebo právnická osoba, ktorá uvádza produkty s digitálnymi prvkami na trh („predáva ich“) pod vlastným menom alebo ochrannou známkou. Právnická osoba môže byť správcom iba v prípade produktov s digitálnymi prvkami, ktoré spĺňajú kritériá slobodného softvéru a softvéru s otvoreným zdrojovým kódom a ktoré sú zverejnené, ale nie sú sprístupnené na trhu v zmysle aktu o kybernetickej odolnosti. Pojem „správca“ sa teda sa vzťahuje na konkrétne prípady slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktorý „je v konečnom dôsledku určený na obchodné činnosti, napríklad na integráciu do komerčných služieb alebo do speňažovaných produktov s digitálnymi prvkami“ (odôvodnenie 19 aktu o kybernetickej odolnosti ([13])), ale nie sú sprístupnené na trhu v zmysle aktu o kybernetickej odolnosti, a pre ktoré právnická osoba, ktorá tento slobodný softvér a softvér s otvoreným zdrojovým kódom zverejňuje, zabezpečuje systematickú podporu.

72. Zo skutočnosti, že určitá právnická osoba je správcom jedného konkrétneho slobodného softvéru a softvéru s otvoreným zdrojovým kódom, nevyplýva, že je nutne správcom aj iného slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktorý zverejňuje. Podobne skutočnosť, že je výrobcom jedného konkrétneho slobodného softvéru a softvéru s otvoreným zdrojovým kódom, neznamená, že táto právnická osoba nemôže byť správcom iného slobodného softvéru a softvéru s otvoreným zdrojovým kódom. To zahŕňa poskytovanie „komunitných“ verzií toho istého slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ako je opísané v oddiele *3.2.1. Účtovanie ceny*.

73. Právnická osoba môže teda byť súčasne správcom jedného konkrétneho slobodného softvéru a softvéru s otvoreným zdrojovým kódom (pričom správca systematicky poskytuje podporu na dlhodobom základe a zabezpečuje životaschopnosť softvéru) a výrobcom iného konkrétneho slobodného softvéru a softvéru s otvoreným zdrojovým kódom (pričom tento softvér uvádza na trh). Inými slovami, od tej istej právnickej osoby sa môže vyžadovať, aby v rámci rôznych projektov slobodného softvéru a softvéru s otvoreným zdrojovým kódom plnila rôzne úlohy.

74. Právnická osoba bude musieť pri každom konkrétnom slobodnom softvéri a softvéri s otvoreným zdrojovým kódom, ktorý zverejňuje, overiť, či sa tento slobodný softvér a softvér s otvoreným zdrojovým kódom považuje za uvedený na trh v zmysle aktu o kybernetickej odolnosti. Ak áno, znamená to, že právnická osoba je výrobcom tohto softvéru. Ak sa slobodný softvér a softvér s otvoreným zdrojovým kódom nepovažuje za uvedený na trh, právnická osoba môže byť správcom tohto softvéru, ak je softvér určený na obchodné činnosti a ak ho táto právnická osoba udržiava v súlade s vymedzením pojmu správca ([14]).

3.3.1. *Trvalá podpora a zabezpečenie životaschopnosti slobodného softvéru a softvéru s otvoreným zdrojovým kódom*

75. V odôvodnení 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 slobodný softvér a softvér s otvoreným zdrojovým kódom a iv) riadenie vývoja takýchto produktov s digitálnymi prvkami.

76. To môže platiť napríklad v prípade právnickej osoby, ktorá vyvíja slobodný softvér a softvér s otvoreným zdrojovým kódom na účely integrácie do svojich vlastných produktov s digitálnymi prvkami a následne ho zverejňuje bez toho, aby ho uviedla na trh. Tejto téme je venovaný aj oddiel *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 oddieloch, právnická osoba, ktorá zverejňuje bezplatnú (alebo komunitnú) verziu a speňaženú verziu toho istého slobodného softvéru a softvéru s otvoreným zdrojovým kódom, sa považuje za správcu bezplatnej (alebo komunitnej) verzie a za výrobcu speňaženej verzie.

77. Podobne aj právnická osoba, ktorá speňažuje slobodný softvér a softvér s otvoreným zdrojovým kódom, ale je neziskovým subjektom, ktorého príjmy sa po odpočítaní nákladov využívajú na dosiahnutie neziskových cieľov (a preto sa jeho slobodný softvér a softvér s otvoreným zdrojovým kódom neuvádza na trh v zmysle aktu o kybernetickej odolnosti, ako sa vysvetľuje v oddiele *3.2.6. Neziskové subjekty* zriadené na dosiahnutie neziskových cieľov), je správcom slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktorý zverejňuje.

78. Okrem toho niektoré nadácie ponúkajú platformy pre spoluprácu s rôznymi formami riadenia, ktoré výrobcom umožňujú pravidelne prispievať k vývoju slobodného softvéru a softvéru s otvoreným zdrojovým kódom a/alebo ktoré sú pravidelne financované výrobcami. Takéto nadácie je potrebné považovať za správcov v súvislosti s konkrétnym slobodným softvérom a softvérom s otvoreným zdrojovým kódom, 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 vyplývajúcim z aktu o kybernetickej odolnosti v súvislosti s iným konkrétnym slobodným softvérom a softvérom s otvoreným zdrojovým kódom, ktorý hosťuje, a to v prípadoch, keď neposkytuje systematickú podporu pre konkrétny slobodný softvér a softvér s otvoreným zdrojovým kódom, nezabezpečuje jeho životaschopnosť a/alebo ak tento konkrétny softvér nie je určený na obchodné činnosti.

([13]) Tento pojem je obsiahnutý aj vo formulácii „určených na obchodné činnosti“, ktorá je súčasťou vymedzenia pojmu „správca softvéru s otvoreným zdrojovým kódom“ uvedeného v článku 3 bode 14 aktu o kybernetickej odolnosti.

([14]) Právnická osoba takisto nemusí podliehať žiadnym povinnostiam vyplývajúcim z aktu o kybernetickej odolnosti v prípadoch, keď: i) konkrétny slobodný softvér a softvér s otvoreným zdrojovým kódom nie je uvedený na trh v zmysle aktu o kybernetickej odolnosti a ii) táto právnická osoba nespĺňa vymedzenie pojmu správca v súvislosti s daným konkrétnym slobodným softvérom a softvérom s otvoreným zdrojovým kódom.

79. Typ „trvalej podpory“, ktorú nadácie a podobné organizácie poskytujú konkrétnym projektom slobodného softvéru a softvéru s otvoreným zdrojovým kódom, sa môže výrazne líšiť. Niektoré právnické osoby napríklad poskytujú iba netechnickú podporu, ako je riadenie budovania značky projektov, stanovovanie pravidiel riadenia, organizovanie komunitných podujatí alebo zbieranie darov. Základnú IT infraštruktúru potrebnú na realizáciu projektu zabezpečujú aj iné subjekty, a to napríklad prostredníctvom hostingu úložísk zdrojového kódu, poskytovania systémov kontroly verzií alebo generovania podpisových kľúčov. Niektoré idú v poskytovaní podpory ešte ďalej a aktívne prispievajú k projektu technickými zdrojmi, napríklad zamestnávaním vývojárov, koordináciou vývojových prác, kontrolou alebo zlučovaním kódu, správou vydaní alebo riešením hlásení o zraniteľnostiach a bezpečnostných záplatách. Hoci všetky právnické osoby, ktoré sa podľa aktu o kybernetickej odolnosti považujú za správcov, 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, 3 a 8, závisí od druhu podpory, ktorú poskytujú, v súlade s článkom 24 ods. 3.

80. Napríklad správca, ktorý poskytuje iba netechnickú podporu, sa podľa vymedzenia pojmu nepodieľa na vývoji produktu s digitálnymi prvkami, a preto nie je povinný hlásiť aktívne zneužitie zraniteľností. Tento správca takisto neposkytuje žiadne sieťové a informačné systémy na vývoj takýchto produktov s digitálnymi prvkami, a preto nie je povinný hlásiť závažné incidenty agentúre ENISA a jednotkám CSIRT ani postihnutým používateľom. Ak sa však správca dozvie o aktívnom zneužití zraniteľnosti (napr. prostredníctvom hlásenia z externých zdrojov, ako sú výskumníci v oblasti bezpečnosti), mal by túto informáciu v súlade so svojou politikou kybernetickej bezpečnosti poskytnúť subjektom vykonávajúcim údržbu produktu s digitálnymi prvkami. Subjekty vykonávajúce údržbu produktov s digitálnymi prvkami a/alebo správcovia by takisto mali zvážiť dobrovoľné nahlásenie tejto zraniteľnosti 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 jednotkám CSIRT akékoľvek závažné incidenty súvisiace s touto infraštruktúrou, ktoré majú vplyv na bezpečnosť produktov s digitálnymi prvkami. V náležitých prípadoch je zároveň potrebné informovať všetkých používateľov (napr. prostredníctvom všeobecného oznámenia). Ako bolo uvedené v predchádzajúcom bode, hoci správca nie je povinný hlásiť aktívne zneužitie zraniteľností, o ktorých sa dozvie, mal by podporovať správne riešenie zraniteľností a zvážiť dobrovoľné oznamovanie v súlade s článkom 15.

82. Nakoniec, ak správca pre konkrétne produkty s digitálnymi prvkami poskytuje aj technické zdroje, je povinný: i) v súlade s článkom 14 ods. 1 oznamovať aktívne zneužité zraniteľnosti, o ktorých sa dozvie, a ii) v náležitých prípadoch informovať všetkých používateľov. Vzhľadom na to, že správca má takisto priamy vzťah s postihnutými používateľmi, je v súlade s článkom 14 ods. 8 povinný informovať ich priamo.

83. Ak subjekt prestane poskytovať systematickú a trvalú podporu konkrétnemu slobodnému softvéru a softvéru s otvoreným zdrojovým kódom, môže prestať spĺňať vymedzenie pojmu správca, a teda už nemusí podliehať príslušným povinnostiam. V takýchto prípadoch sa danému subjektu odporúča, aby jasne informoval o zmene svojho postavenia v súvislosti s daným konkrétnym slobodným softvérom a softvérom s otvoreným zdrojovým kódom.

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 následne sa naň začnú vzťahovať povinnosti výrobcu vyplývajúce z aktu o kybernetickej odolnosti. Za takýchto okolností sa daný subjekt považuje za výrobcu produktu s digitálnymi prvkami odo dňa, keď ho uvedie na trh (nie však v prípade skorších verzií, pri ktorých pôsobil ako správca).

3.4. **Prispievatelia a následné využitie**

85. Ako už bolo uvedené v oddiele *3.1. Určenie toho, kto je zodpovedný za slobodný softvér a softvér s otvoreným zdrojovým kódom*, v akte o kybernetickej odolnosti sa objasňuje, že akt sa nevzťahuje „na fyzické alebo právnické osoby, ktoré prispievajú zdrojovým kódom k produktom s digitálnymi prvkami, ktoré sa považujú za slobodný softvér a softvér s otvoreným zdrojovým kódom, za ktoré nenesú zodpovednosť“ (odôvodnenie 18).

86. Ani výrobcovia produktov s digitálnymi prvkami, ktorí integrujú komponenty slobodného softvéru a softvéru s otvoreným zdrojovým kódom do svojich vlastných produktov s digitálnymi prvkami, nenesú zodpovednosť za individuálnu zhodu týchto komponentov s aktom o kybernetickej odolnosti, a to ani v prípade, že prispievajú zdrojovým kódom k ich údržbe.

87. Podobne ani samotná skutočnosť, že výrobcovia integrujú komponenty slobodného softvéru a softvéru s otvoreným zdrojovým kódom do svojich vlastných (speňažených) produktov s digitálnymi prvkami, nemá žiadny vplyv na status daného komponentu slobodného softvéru a softvéru s otvoreným zdrojovým kódom podľa aktu o kybernetickej odolnosti. Subjekty vykonávajúce údržbu komponentov slobodného softvéru a softvéru s otvoreným zdrojovým kódom neuvedených na trh nemajú žiadne povinnosti voči iným subjektom, ktoré môžu takéto komponenty integrovať do svojich produktov s digitálnymi prvkami. To, či sa na daný komponent slobodného softvéru a softvéru s otvoreným zdrojovým kódom vzťahuje akt o kybernetickej odolnosti, závisí výlučne od toho, či fyzická alebo právnická osoba, ktorá daný komponent zverejňuje, uvádza tento komponent na trh.

88. Výrobcovia produktov s digitálnymi prvkami, ktorí integrujú komponenty slobodného softvéru a softvéru s otvoreným zdrojovým kódom, sú však povinní dodržiavať akt o kybernetickej odolnosti v súvislosti so svojimi vlastnými produktmi s digitálnymi prvkami. V súlade s článkom 13 ods. 5 majú aj povinnosť vykonávať náležitú starostlivosť vo vzťahu ku komponentom slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktoré integrujú. Okrem toho sú povinní hlásiť zraniteľnosti v integrovaných komponentoch a zdieľať bezpečnostné opravy v súlade s článkom 13 ods. 6. Ďalšie informácie k tejto téme sú uvedené v oddiele *9.2.1. Oznamovanie zraniteľností smerom k pôvodným zdrojom a zdieľanie bezpečnostných opráv*.

3.5. **Ilustratívne scenáre**

89. Príklady, ktoré uvádzame ďalej, sú čisto hypotetické a ich účelom je len ilustrovať rôzne prípady vysvetlené v predchádzajúcich oddieloch.

Príklad 27: Konkrétny vývojár A vyvinul slobodný softvér a softvér s otvoreným zdrojovým kódom. Vývojár A zverejňuje tento slobodný softvér a softvér s otvoreným zdrojovým kódom pod svojím vlastným menom alebo ochrannou známkou, ale za jeho používanie neúčtuje žiadnu cenu. Tento softvér je voľne dostupný a je bezplatne k dispozícii pre všetkých na účely prístupu, používania, úpravy a redistribúcie. Vývojár A takisto uvádza odkaz na platformu určenú na zbieranie darov.

Spoločnosti B, C a D integrujú tento slobodný softvér a softvér s otvoreným zdrojovým kódom do svojich vlastných produktov s digitálnymi prvkami. Spoločnosti B, C a D poskytujú vývojárovi A dobrovoľné dary na podporu priebežnej údržby. Tieto dary umožňujú vývojárovi A aktívne udržiavať projekt.

Daný slobodný softvér a softvér s otvoreným zdrojovým kódom nie je uvedený na trh v zmysle aktu o kybernetickej odolnosti. Vývojár A nemá žiadne povinnosti vyplývajúce z aktu o kybernetickej odolnosti. Spoločnosti B, C a D sú pri integrácii uvedeného slobodného softvéru a softvéru s otvoreným zdrojovým kódom do svojich vlastných produktov s digitálnymi prvkami povinné postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

Príklad 28: Nezisková nadácia F zverejňuje komponent slobodného softvéru a softvéru s otvoreným zdrojovým kódom určený na integráciu do iných komerčných produktov s digitálnymi prvkami. Nadácia F sa zaväzuje poskytovať tomuto slobodnému softvéru a softvéru s otvoreným zdrojovým kódom trvalú podporu s cieľom zabezpečiť jeho životaschopnosť a rozšírenie. Spoločnosti A, B a C integrujú tento slobodný softvér a softvér s otvoreným zdrojovým kódom do svojich vlastných produktov s digitálnymi prvkami. Spoločnosti A a B dobrovoľne prispievajú určitým časom svojich vývojárov na vývoj a údržbu projektov slobodného softvéru a softvéru s otvoreným zdrojovým kódom v rámci nadácie F, a to aj pre tento slobodný softvér a softvér s otvoreným zdrojovým kódom.

Keďže nadácia F je neziskový subjekt zriadený tak, že jej príjmy sa po odpočítaní nákladov využívajú na dosahovanie neziskových cieľov, slobodný softvér a softvér s otvoreným zdrojovým kódom sa nepovažuje za uvedený na trh v zmysle aktu o kybernetickej odolnosti. Nadácia F je správcom slobodného softvéru a softvéru s otvoreným zdrojovým kódom a podlieha príslušným povinnostiam stanoveným v článku 24. Spoločnosti A, B a C sú pri integrácii uvedeného slobodného softvéru a softvéru s otvoreným zdrojovým kódom do svojich vlastných produktov s digitálnymi prvkami povinné postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

Príklad 29: Spoločnosť A vyvinula komponent slobodného softvéru a softvéru s otvoreným zdrojovým kódom určený na integráciu do svojich vlastných produktov s digitálnymi prvkami. Tento slobodný softvér a softvér s otvoreným zdrojovým kódom takisto zverejňuje samostatne pod vlastným menom alebo ochrannou známkou a aktívne ho udržiava. Za jeho používanie si však neúčtuje žiadnu cenu ani ho nespeňažuje iným spôsobom. Spoločnosti B, C a D integrujú tento slobodný softvér a softvér s otvoreným zdrojovým kódom do svojich vlastných produktov s digitálnymi prvkami a dobrovoľne prispievajú určitým časom svojich vývojárov na jeho údržbu.

Tento slobodný softvér a softvér s otvoreným zdrojovým kódom sa nepovažuje za uvedený na trh v zmysle aktu o kybernetickej odolnosti. Spoločnosť A nie je jeho výrobcom, ale jeho správcom. Spoločnosti B, C a D sú pri integrácii slobodného softvéru a softvéru s otvoreným zdrojovým kódom do svojich vlastných produktov s digitálnymi prvkami povinné postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

Príklad 30: Spoločnosť A zverejňuje slobodný softvér a softvér s otvoreným zdrojovým kódom pod vlastným menom alebo ochrannou známkou a ponúka ho ako platenú verziu, ktorá zahŕňa určité výhody, ako napríklad technickú podporu alebo optimalizáciu výkonu. Vývojári zo spoločností B, C a D prispievajú k údržbe tohto slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ten však naďalej zostáva pod kontrolou spoločnosti A.

Spoločnosť A sa v súvislosti s týmto slobodným softvérom a softvérom s otvoreným zdrojovým kódom považuje za výrobcu ([15]). Spoločnosti B, C a D nemajú v súvislosti s týmto konkrétnym slobodným softvérom a softvérom s otvoreným zdrojovým kódom žiadne povinnosti vyplývajúce z aktu o kybernetickej odolnosti. Ak tento slobodný softvér a softvér s otvoreným zdrojovým kódom integrujú do svojich vlastných produktov s digitálnymi prvkami, sú povinní postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

Príklad 31: Spoločnosť A zverejňuje slobodný softvér a softvér s otvoreným zdrojovým kódom pod vlastným menom alebo ochrannou známkou a zabezpečuje jeho priebežnú údržbu s cieľom zabezpečiť jeho dlhodobú životaschopnosť a umožniť integráciu tohto softvéru do produktov s digitálnymi prvkami iných spoločností. Spoločnosť A neúčtuje žiadnu cenu za jeho používanie, nespracúva osobné údaje, ktoré zhromažďuje prostredníctvom produktu s digitálnymi prvkami, ani nepredáva podporné služby súvisiace so zverejnením tohto slobodného softvéru a softvéru s otvoreným zdrojovým kódom.

Spoločnosť B prispieva kódom a časom vývojárov k údržbe tohto slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ale nedistribuuje ho komerčne. Spoločnosť B poskytuje služby technickej podpory nezávisle od distribúcie slobodného softvéru a softvéru s otvoreným zdrojovým kódom. Spoločnosť A sa považuje za správcu daného slobodného softvéru a softvéru s otvoreným zdrojovým kódom, zatiaľ čo spoločnosť B nemá v súvislosti s týmto slobodným softvérom a softvérom s otvoreným zdrojovým kódom žiadne povinnosti vyplývajúce z aktu o kybernetickej odolnosti.

Príklad 32: Komponent slobodného softvéru a softvéru s otvoreným zdrojovým kódom zverejňuje neziskový subjekt zriadený tak, aby sa zabezpečilo, že všetky príjmy sa po odpočítaní nákladov použijú na dosiahnutie neziskových cieľov. Subjekt poskytuje trvalú podporu s cieľom zabezpečiť dlhodobú životaschopnosť projektu. Údržba je financovaná z verejných zdrojov, napríklad z výskumných grantov. Ďalší vývoj, vrátane nových funkcií, je financovaný z darov a v rámci konkrétnych projektov realizovaných v spolupráci s výrobcami, ktorí tento slobodný softvér a softvér s otvoreným zdrojovým kódom integrujú do svojich produktov s digitálnymi prvkami. Tieto funkcie sú integrované do kódovej základne slobodného softvéru a softvéru s otvoreným zdrojovým kódom.

Neziskový subjekt, ktorý tento slobodný softvér a softvér s otvoreným zdrojovým kódom zverejňuje, sa považuje za správcu daného komponentu slobodného softvéru a softvéru s otvoreným zdrojovým kódom. Výrobca, ktorý prispel k vývoju určitých funkcií, sa nestáva výrobcom daného komponentu slobodného softvéru a softvéru s otvoreným zdrojovým kódom. Ak výrobca integruje tento komponent slobodného softvéru a softvéru s otvoreným zdrojovým kódom do svojho vlastného produktu s digitálnymi prvkami, je povinný postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

Príklad 33: Neziskový subjekt zriadený tak, aby sa zabezpečilo, že všetky príjmy sa po odpočítaní nákladov použijú na dosiahnutie neziskových cieľov, zverejňuje súbor nástrojov na vývoj slobodného softvéru a softvéru s otvoreným zdrojovým kódom (SDK) a zabezpečuje jeho priebežnú údržbu. Súbor nástrojov na vývoj softvéru je pre každého voľne a bezplatne dostupný na účely prístupu, používania, úpravy a redistribúcie. Financovanie sa zabezpečuje prostredníctvom členských poplatkov vyplácaných neziskovému subjektu a vývojári zamestnaní v členských organizáciách prispievajú k vývoju SDK svojím kódom a ďalšími zdrojmi. Výrobcovia využívajú SDK ako komponent pri vývoji ďalších produktov s digitálnymi prvkami.

Neziskový subjekt, ktorý tento SDK zverejňuje, je jeho správcom. Členovia nadácie nezodpovedajú za súlad SDK s aktom o kybernetickej odolnosti. Ak výrobcovia používajú SDK na vytvorenie vlastného produktu s digitálnymi prvkami, musia postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

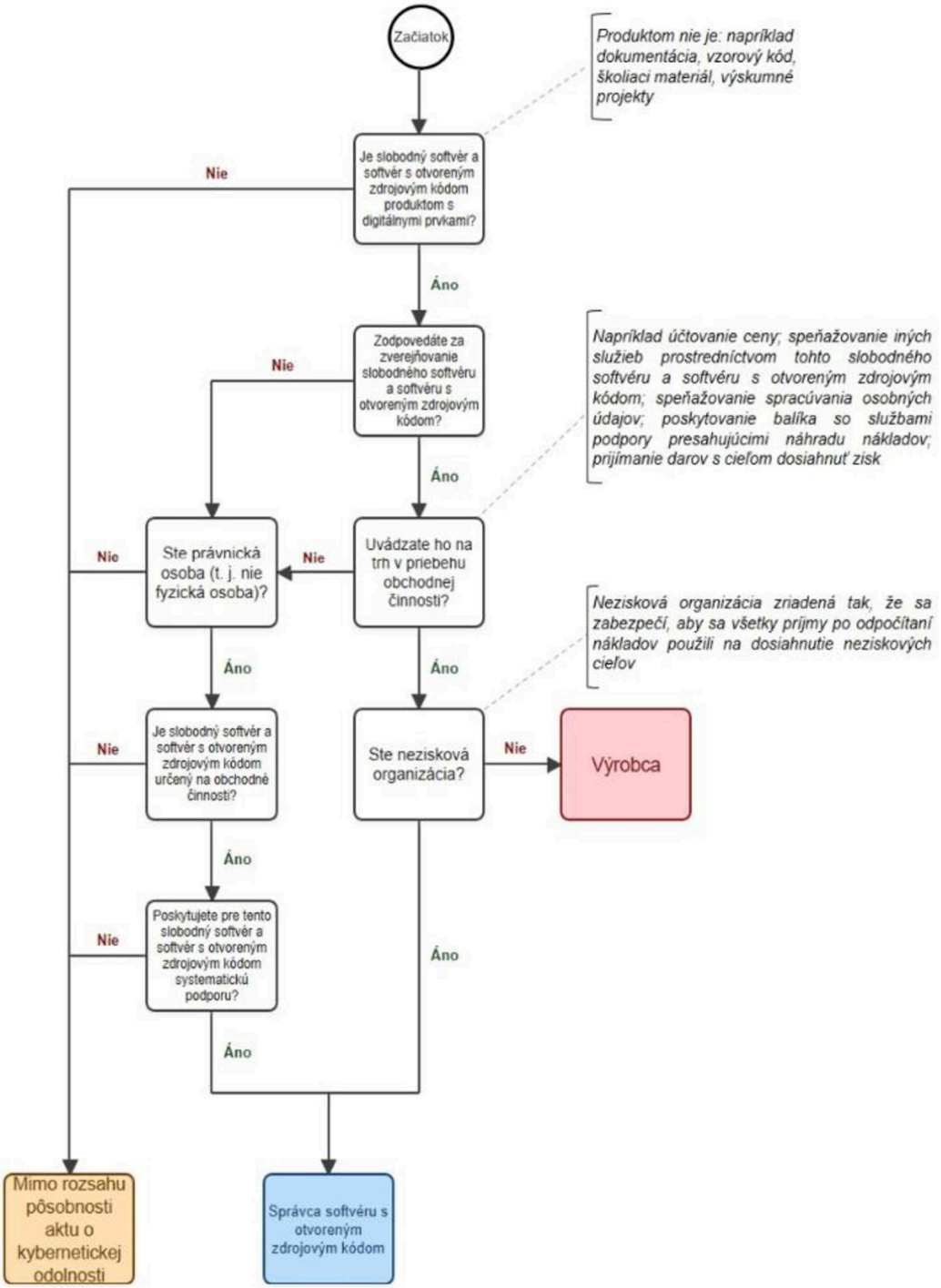
Príklad 34: Konkrétny vývojár zverejňuje knižnicu slobodného softvéru a softvéru s otvoreným zdrojovým kódom vo verejnom úložisku balíkov pre daný programovací jazyk a aktívne ju udržiava. V dokumentácii k balíku pridáva odkaz na zbierku darov. Výrobca si túto knižnicu bezplatne stiahne z úložiska a integruje ju do svojho vlastného produktu s digitálnymi prvkami.

Konkrétny vývojár ani úložisko balíkov nemajú podľa aktu o kybernetickej odolnosti žiadne povinnosti. Výrobca, ktorý integruje túto knižnicu, je povinný postupovať s náležitou starostlivosťou v súlade s článkom 13 ods. 5.

([15]) Pokiaľ spoločnosť A nie je neziskovým subjektom zriadeným tak, aby sa zabezpečilo, že všetky príjmy sa po odpočítaní nákladov použijú na dosiahnutie neziskových cieľov – v takom prípade by bola správcom daného slobodného softvéru a softvéru s otvoreným zdrojovým kódom.

Obrázok 1

Zjednodušený diagram znázorňujúci rozsah pôsobnosti aktu o kybernetickej odolnosti v súvislosti so slobodným softvérom a softvérom s otvoreným zdrojovým kódom



4. **PODSTATNÉ ÚPRAVY A NÁHRADNÉ DIELY**

90. V článku 3 bode 30 aktu o kybernetickej odolnosti sa pojem „podstatná úprava“ vymedzuje ako zmena produktu s digitálnymi prvkami po jeho uvedení na trh, ktorá i) ovplyvňuje súlad produktu s digitálnymi prvkami so základnými požiadavkami stanovenými v prílohe I časti I alebo ii) má za následok úpravu zamýšľaného účelu, pre ktorý bol produkt s digitálnymi prvkami posudzovaný.

91. Pojem „podstatná úprava“ je relevantný pre stanovenie povinností podľa aktu o kybernetickej odolnosti v mnohých prípadoch vrátane týchto:

a) 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;

b) v súlade s článkom 22 sa každá fyzická alebo právnická osoba, ktorá vykoná podstatnú úpravu produktu s digitálnymi prvkami a sprístupní ho na trhu, považuje za jeho výrobcu;

c) v súlade s článkom 69 ods. 2 sa každá fyzická alebo právnická osoba, ktorá po 11. decembri 2027 vykoná podstatnú úpravu produktu s digitálnymi prvkami, ktorý bol uvedený na trh pred 11. decembrom 2027, a tento produkt uvedie na trh, považuje za jeho výrobcu;

d) v prípade výrobcov produktov s digitálnymi prvkami, ktoré sa uvádzajú na trh po 11. decembri 2027, s cieľom určiť, či produkt s digitálnymi prvkami musí v dôsledku zmien vykonaných po tomto dátume prejsť novým postupom posudzovania zhody, 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 aktu o kybernetickej odolnosti, „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.“ To je v súlade s oddielom 2.1 Modrej príručky, v ktorom sa uvádza, že „výrobok, ktorý po uvedení do prevádzky prešiel významnými zmenami alebo generálnou opravou, sa musí považovať za nový výrobok, ak: i) sa zmení jeho pôvodný výkon, účel alebo typ, pričom táto zmena sa v počiatočnom posúdení rizika nepredpokladala; ii) sa zmenila povaha nebezpečenstva alebo sa zvýšila úroveň rizika v spojitosti s príslušnými harmonizačnými právnymi predpismi Únie a iii) výrobok je sprístupnený (alebo uvedený do prevádzky, ak do rozsahu pôsobnosti platných právnych predpisov patrí aj uvedenie do prevádzky). To sa posúdi v jednotlivých prípadoch, a najmä so zreteľom na ciele právnych predpisov a typ výrobkov, na ktoré sa vzťahuje táto právna úprava.“

94. Činnosti renovovania, údržby alebo opravy, ktoré vedú k fyzickým úpravám produktov s digitálnymi prvkami, ktoré už boli uvedené na trh, nemusia nutne predstavovať podstatné úpravy. Preto by sa malo v každom jednotlivom prípade posúdiť, či takáto fyzická úprava ovplyvňuje súlad produktu s digitálnymi prvkami so základnými požiadavkami prílohy I časti I, alebo či vedie k zmene zamýšľaného účelu produktu, na ktorý sa vzťahuje posúdenie kybernetickobezpečnostných rizík.

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 neznamená podstatnú úpravu opravovaného produktu s digitálnymi prvkami. O podstatnú úpravu ide len vtedy, keď zmena výkonu alebo spôsobu fungovania opravovaného 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 vykonáva opravu, pri ktorej vymení chybnú pamäť RAM za novú s vyšším výkonom. Súlad servera so základnými požiadavkami nie je ovplyvnený. Server dosahuje lepší výkon, jeho nový výkon sa však stále pohybuje v rámci zamýšľaného využitia 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 aktu o kybernetickej odolnosti sa stanovuje, že náhradné diely určené na výmenu identických komponentov a vyrobené podľa rovnakých špecifikácií ako tieto komponenty nepodliehajú aktu o kybernetickej odolnosti. V odôvodnení 29 sa ďalej uvádza, že výnimka sa vzťahuje jednak na náhradné diely pre produkty s digitálnymi prvkami, ktoré boli sprístupnené na trhu pred začatím uplatňovania aktu o kybernetickej odolnosti, jednak na náhradné diely, ktoré už prešli postupom posudzovania zhody stanoveným v tomto nariadení.

97. Výnimku uvedenú v článku 2 ods. 6 aktu o kybernetickej odolnosti treba chápať tak, že sa uplatňuje iba v prípade, ak sa náhradný diel dodáva výlučne na účely opravy alebo predĺženia životnosti produktu s digitálnymi prvkami, ktorý bol už uvedený na trh (pred 11. decembrom 2027 alebo po tomto dátume). 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 aktu o kybernetickej odolnosti a nemal by sa považovať za náhradný diel, na ktorý sa vzťahuje článok 2 ods. 6. Účel údržby alebo opravy by mal byť zrejmý z kontextu dodávky, napríklad na základe identifikácie produktu s digitálnymi prvkami alebo na základe uvedenia skupiny produktov v objednávke alebo obchodnej ponuke, prípadne na základe dodávky prostredníctvom popredajných alebo servisných kanálov. Príslušné podklady potvrdzujúce túto skutočnosť by mali byť k dispozícii aj orgánom dohľadu nad trhom. Skutočnosť, že produkt s digitálnymi prvkami by sa z technického hľadiska dal použiť na výmenu komponentu, sama osebe nestačí na to, aby sa naň vzťahovala výnimka v prípade, že takéto prvky chýbajú.

98. Z toho vyplýva, že ak je náhradný diel identický s komponentom, ktorý už je súčasťou produktu s digitálnymi prvkami, ktorý bol uvedený na trh buď pred dátumom začatia uplatňovania aktu o kybernetickej odolnosti, alebo ktorý bol uvedený na trh v súlade s aktom o kybernetickej odolnosti, tento náhradný diel sám osebe nepodlieha aktu o kybernetickej odolnosti.

99. Pri posudzovaní toho, či náhradný diel treba považovať za identický s komponentom, by sa pozornosť mala zamerať na funkčnú úlohu náhradného dielu v produkte s digitálnymi prvkami a na charakteristiky, ktoré môžu mať význam pre kybernetickú bezpečnosť. Hoci je vždy potrebné posúdenie každého jednotlivého prípadu, rozdiely, ktoré nemajú vplyv na bezpečnostné charakteristiky ani na rizikový profil komponentu, pokiaľ ide o kybernetickú bezpečnosť, samy osebe nebránia tomu, aby tento náhradný diel patril do rozsahu pôsobnosti článku 2 ods. 6 aktu o kybernetickej odolnosti.

100. Naopak, rozdiely v charakteristikách relevantných pre kybernetickú bezpečnosť komponentu, ako sú algoritmy, protokoly, kryptografické mechanizmy, funkcie riadenia prístupu alebo iné charakteristiky súvisiace s bezpečnosťou, môžu znamenať, že nový komponent nemožno považovať za identický s komponentom, ktorý má nahradiť.

101. Ak náhradný diel nie je identický s pôvodným komponentom, tento náhradný diel predstavuje samostatný produkt s digitálnymi prvkami, a preto sa naň vzťahuje akt o kybernetickej odolnosti. V takýchto prípadoch sa musí posúdiť súlad so základnými požiadavkami s ohľadom na zamýšľaný účel náhradného komponentu. Za obzvlášť dôležitú sa považuje funkcia náhradného komponentu, ktorou je zabezpečenie kompatibility alebo interoperability s existujúcim produktom s digitálnymi prvkami, a to aj v prípade, ak ide o produkt s digitálnymi prvkami, ktorý bol uvedený na trh pred začatím uplatňovania aktu o kybernetickej odolnosti. Ak nie je možné primerane splniť určité základné požiadavky z dôvodu uvedeného zamýšľaného účelu alebo technických obmedzení, výrobca musí túto skutočnosť zohľadniť v posúdení kybernetickobezpečnostných rizík a zaviesť primerané alternatívne alebo kompenzačné opatrenia na zmiernenie rizík, aby nedošlo k ohrozeniu bezpečnosti produktu s digitálnymi prvkami. Ako sa uvádza aj v oddiele *2.6. Zložité systémy*, kľúčovú úlohu pri transparentnom opise zistených obmedzení, súvisiacich kybernetickobezpečnostných rizík a zavedených opatrení na zmiernenie rizika zohráva nielen technická dokumentácia, ale aj informácie a návody pre používateľa. Ako je vysvetlené v oddiele *4.1. Fyzické opravy*, výmena chybných alebo opotrebovaných dielov za diely s lepšími vlastnosťami sama osebe nepredstavuje podstatnú úpravu opravovaného produktu s digitálnymi prvkami.

Príklad 36: Výrobca uviedol na trh EÚ pripojené ovládače. V jednom prípade bol ovládač uvedený na trh v roku 2026, teda pred dátumom začatia uplatňovania aktu o kybernetickej odolnosti. V inom prípade bol ovládač uvedený na trh v roku 2028 v súlade s aktom o kybernetickej odolnosti. V roku 2028 dôjde k poruche digitálneho komunikačného modulu v oboch typoch ovládačov. Výrobca dodáva ako náhradný diel náhradný modul, ktorý je identický a vyrobený podľa rovnakých špecifikácií ako originál.

V oboch prípadoch sa na náhradný modul vzťahuje výnimka uvedená v článku 2 ods. 6. Náhradný diel sám osebe nepodlieha aktu o kybernetickej odolnosti, hoci ide o produkt s digitálnymi prvkami, pretože nahrádza identický komponent v produkte s digitálnymi prvkami. Oprava nepredstavuje podstatnú úpravu produktu s digitálnymi prvkami.

Príklad 37: Výrobca uviedol na trh EÚ v roku 2026, pred dátumom začatia uplatňovania aktu o kybernetickej odolnosti, pripojený priemyselný ovládač. V roku 2028 dôjde k poruche komunikačného čipu v tomto ovládači. Keďže výrobca už tento čip nevyrába, dodá ako náhradný diel novší čip s rovnocennou funkciou, zato s odlišnou kryptografickou implementáciou a aktualizovaným mechanizmom bezpečného spustenia, aby bola zachovaná kompatibilita a nepretržitá prevádzka.

V tomto prípade nemožno náhradný čip považovať za identický, keďže rozdiely v kryptografickej implementácii a mechanizme bezpečného spustenia ovplyvňujú vlastnosti čipu z hľadiska kybernetickej bezpečnosti. Na tento produkt sa preto nevzťahuje výnimka uvedená v článku 2 ods. 6 a ide o produkt s digitálnymi prvkami, na ktorý sa vzťahuje akt o kybernetickej odolnosti. Súlad náhradného dielu sa musí posudzovať s ohľadom na jeho zamýšľaný účel vrátane jeho úlohy pri zabezpečovaní interoperability s produktom s digitálnymi prvkami, ktorý bol uvedený na trh pred začatím uplatňovania aktu o kybernetickej odolnosti.

Príklad 38: Výrobca uvedie v roku 2028 na trh inteligentný ovládač budov v súlade s aktom o kybernetickej odolnosti. V roku 2029 dôjde k poruche bezdrôtového modulu v tomto ovládači. Keďže výrobca už tento modul nevyrába, dodáva ako náhradný diel nový modul, ktorý plní rovnakú funkciu s využitím rovnakých komunikačných protokolov a bezpečnostných mechanizmov, je však založený na inom čipovom súbore a má aktualizovaný firmvér, ktorý nemení charakteristiky, ktoré by mohli mať význam pre kybernetickú bezpečnosť.

V tomto prípade možno náhradný modul považovať za identický. Modul teda spĺňa podmienky výnimky uvedenej v článku 2 ods. 6 a nepodlieha aktu o kybernetickej odolnosti.

102. Výnimka pre náhradné diely sa uplatňuje bez ohľadu na to, či náhradný diel nahrádza komponent s digitálnymi prvkami alebo celý produkt s digitálnymi prvkami, ktorý sám osebe tvorí súčasť väčšieho produktu, a to aj v prípade, ak sa tento väčší produkt s digitálnymi prvkami skladá z viacerých integrovaných komponentov, za predpokladu, že náhradný diel sa výslovne dodáva ako náhradný diel, ako je vysvetlené v predchádzajúcich odsekoch.

Príklad 39: V roku 2027 uvedie výrobca na trh systém priemyselnej automatizácie, ktorého jedným z komponentov je programovateľná logická riadiaca jednotka (PLC). V roku 2031 dôjde k poruche centrálnej procesorovej jednotky PLC. Výrobca ponúka dve možnosti opravy: i) dodanie náhradnej procesorovej jednotky, ktorú možno považovať za identickú s pôvodne nainštalovanou procesorovou jednotkou, alebo ii) dodanie kompletnej náhradnej PLC, ktorú možno považovať za identickú s pôvodne nainštalovanou PLC. V každom prípade sa náhradný diel dodáva prostredníctvom popredajného servisného kanála výrobcu ako náhradný diel a systém priemyselnej automatizácie, pre ktorý je táto výmena určená, je jasne identifikovaný. V oboch prípadoch patrí táto výmena do rozsahu pôsobnosti výnimky uvedenej v článku 2 ods. 6, a to bez ohľadu na to, či sa výmena týka komponentu 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 podrobnejšie usmernenia, aby bolo možné určiť, kedy sa softvér považuje za podstatne upravený. Tieto usmernenia majú predovšetkým pomôcť výrobcom softvérových produktov s digitálnymi prvkami, ktorí vykonávajú zmeny vo svojich vlastných produktoch, aby určili, či tieto zmeny predstavujú podstatnú úpravu.

104. V odôvodnení 39 sa uvádza, že produkt s digitálnymi prvkami je podstatne upravený v prípade, ak zmena ovplyvňuje úroveň kybernetickobezpečnostného rizika a ak výrobca takéto zmenené alebo dodatočné riziko nezohľadnil vo svojom posúdení rizík a následne ani pri plnení základných požiadaviek. Výrobca by preto mal v každom jednotlivom prípade posúdiť, či aktualizácia softvéru prináša nové alebo zvýšené kybernetickobezpečnostné riziká a či sa tieto riziká už zohľadnili v jeho posúdení rizík.

105. Ak výrobca zavedie do produktu s digitálnymi prvkami nové funkcie, ktoré majú za následok zmenu zamýšľaného účelu produktu ako celku, je pravdepodobné, že 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 informačný panel, ktorý zbiera údaje zo strojov a zobrazuje trendy a upozornenia, pričom nemá možnosť tieto stroje ovládať. Výrobca následne vyvíja novú verziu tohto informačného panela, do ktorej zavádza funkcie umožňujúce ovládanie strojov vrátane nastavovania prevádzkových parametrov a opätovného spustenia strojov po poruchových stavoch. V dôsledku týchto zmien sa zamýšľaný účel informačného panela posunul nad rámec toho, čo sa predpokladalo v posúdení rizík, a premenil sa z nástroja na získanie prehľadu o situácii na produkt s digitálnymi prvkami, ktorého účelom je vykonávať prevádzkovú kontrolu nad inými zariadeniami. Informačný 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 zavedie aktualizáciu, ktorá aplikácii umožní automaticky analyzovať obsah používateľa s cieľom vytvárať profily správania a prijímať automatizované rozhodnutia ovplyvňujúce priorizáciu, 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 zohľadnené pri posudzovaní rizík. Aplikácia bola preto podstatne upravená.

106. Zároveň je však možné, že výrobca postupne zavádza nové funkcie, ktoré už sú zahrnuté v jeho posúdení rizík, alebo ktoré samy osebe nemenia rizikový profil produktu s digitálnymi prvkami, pokiaľ ide o kybernetickú bezpečnosť. Môže ísť napríklad o prípad, keď výrobca predvídal vývoj týchto funkcií, súvisiace riziká už opísal a posúdil a zaviedol vhodné opatrenia na ich zmiernenie s cieľom zabezpečiť trvalý súlad so základnými požiadavkami. Môže ísť aj o situáciu, keď nové funkcie nezahŕňajú zmeny vedúce k vzniku nových alebo zvýšených rizík. Aktualizácie takejto povahy by sa preto nemali považovať za podstatné úpravy, keďže nezvyšujú kybernetickobezpečnostné riziko a v dôsledku toho nemenia spôsob vykonávania základných požiadaviek.

Príklad 42: Aplikácia na zasielanie správ je spočiatku uvedená na trh s funkciami obmedzenými na komunikáciu medzi dvoma používateľmi. Posúdenie rizík výrobcom zahŕňa aj neskoršie zavedenie skupinovej komunikácie vrátane napríklad zvýšenej zložitosti smerovania správ. V nasledujúcej aktualizácii výrobca pridáva funkciu skupinového chatu spolu s nástrojmi pre správu a moderovanie, ktoré boli už zohľadnené a posúdené v pôvodnom návrhu. Touto aktualizáciou sa zavádzajú funkcie, ktoré patria do rozsahu pôvodného zamýšľaného účelu a posúdenia rizík. Aplikácia na zasielanie správ preto nebola podstatne upravená.

Príklad 43: Systém monitorovania výroby sa uvádza na trh s aktivovanými informačnými panelmi určenými len na čítanie, zatiaľ čo funkcie automatizovaného riadenia sú súčasťou architektúry systému, ale zostávajú deaktivované. Posúdenie rizík výrobcom výslovne zahŕňa budúcu aktiváciu automatizovaných riadiacich slučiek vrátane kybernetickobezpečnostných rizík spojených s riadením v uzavretej slučke, ako aj ochranných opatrení, ako sú mechanizmy umožňujúce zásah operátora a bezpečnostné režimy. V neskoršej aktualizácii výrobca sprístupní funkcie automatického riadenia a aktivuje bezpečnostné opatrenia tak, ako boli pôvodne posúdené. Systém monitorovania výroby preto neprešiel žiadnymi podstatnými úpravami.

107. Naopak, aj obmedzené alebo zdanlivo menej dôležité nové funkcie môžu predstavovať významné kybernetickobezpečnostné riziká, ktoré ovplyvňujú súlad so základnými požiadavkami. Posúdenie podstatnej úpravy by sa preto nemalo zakladať na rozsahu alebo zložitosti danej zmeny, ale na jej potenciálnom nepriaznivom vplyve na rizikový profil produktu s digitálnymi prvkami, pokiaľ ide o kybernetickú bezpečnosť, a následne na plnenie základných požiadaviek.

Príklad 44: Výrobca prostredníctvom aktualizácie pridá do softvérovej aplikácie funkciu „zapamätať si ma“ alebo funkciu trvalého prihlásenia, ktorá na zlepšenie používateľského komfortu lokálne ukladá autentifikačné tokeny. Hoci je rozsah tejto funkcie obmedzený, prináša so sebou nové riziká súvisiace s krádežou tokenov, neoprávneným prístupom a prevzatím relácie, ktoré neboli zohľadnené v posúdení rizík. Táto aktualizácia má preto vplyv na súlad so základnými požiadavkami. Softvérová aplikácia bola podstatne upravená.

Príklad 45: Výrobca pridá k existujúcemu softvérovému produktu s digitálnymi prvkami novú funkciu zaznamenávania udalostí a diagnostiky, ktorá umožňuje exportovať podrobné systémové denníky na účely riešenia problémov. Hoci sa táto funkcia javí ako menej dôležitá, vedie k zberu a ukladaniu citlivých prevádzkových údajov v nezašifrovanom formáte, čím vznikajú riziká úniku údajov, ktoré neboli predtým posúdené ani zmiernené. Táto zmena môže preto mať významný vplyv na rizikový profil produktu s digitálnymi prvkami, pokiaľ ide o kybernetickú bezpečnosť. Softvérový produkt s digitálnymi prvkami bol podstatne upravený.

108. V súlade s odôvodnením 39 aktu o kybernetickej odolnosti sa bezpečnostné aktualizácie vo všeobecnosti nepovažujú za podstatné úpravy, keďže ich hlavným účelom je znížiť úroveň kybernetickobezpečnostného rizika súvisiaceho s produktom s digitálnymi prvkami. Bezpečnostná aktualizácia, ktorá nemení zamýšľaný účel daného produktu a neprináša nové kybernetickobezpečnostné riziká, by sa preto nemala považovať za podstatnú úpravu, a to ani v prípade, že môže priniesť významné technické zmeny. To platí aj v prípadoch, keď sú určité funkcie upravené alebo obmedzené výlučne s cieľom zmierniť zistené zraniteľnosti a zabezpečiť trvalý súlad so základnými požiadavkami.

Príklad 46: Výrobca nasadí bezpečnostnú aktualizáciu s cieľom odstrániť zraniteľnosť v kódovej základni produktu s digitálnymi prvkami, a to opravou chyby pri validácii vstupov, ktorá by mohla viesť k pretečeniu medzipamäte, alebo odstránením logickej chyby umožňujúcej obísť autentifikáciu v dôsledku nesprávnej validácie tokenu relácie. Táto aktualizácia mení vnútornú implementáciu softvéru bez toho, aby ovplyvnila zamýšľaný účel daného produktu alebo spôsobila nové vystavenie bezpečnostným rizikám. Výlučným cieľom aktualizácie je znížiť kybernetickobezpečnostné riziko. Táto bezpečnostná aktualizácia by sa nemala považovať za podstatnú úpravu.

Príklad 47: Výrobca zavedie bezpečnostnú aktualizáciu, ktorá posilňuje existujúce nastavenia zabezpečenia, napríklad sprísnením pravidiel brány firewall, deaktiváciou nepoužívaných sieťových portov, úpravou zásad pre predvolené heslá administrátorov alebo zavedením povinného viacfaktorového overovania, ak táto funkcia už bola dostupná alebo sa s ňou už 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 úrovne zabezpečenia. Táto bezpečnostná aktualizácia by sa nemala považovať za podstatnú úpravu.

Príklad 48: Výrobca uvádza na trh softvérový produkt s digitálnymi prvkami, ktorý zabezpečuje komunikáciu prostredníctvom konfigurovateľného rámca šifrovania podporujúceho viaceré kryptografické algoritmy a veľkosti kľúčov, ako je opísané v technickej dokumentácii a posúdení rizík produktu. Posúdenie rizík sa vzťahuje na všetky kryptografické možnosti, ktoré produkt s digitálnymi prvkami ponúka, a zohľadňuje sa v ňom budúce ukončenie používania určitých algoritmov. Posúdenie rizík zahŕňa aj opatrenia na zmiernenie rizík, ako sú kryptografická agilita, interná správa kľúčov a testovanie kompatibility. V reakcii na nové odporúčania v oblasti kryptografie výrobca nasadí bezpečnostnú aktualizáciu, ktorá deaktivuje zastaraný algoritmus a aktivuje silnejšiu alternatívu, ktorá už je podporovaná, a to bez zavedenia nových externých závislostí alebo zmeny tokov údajov. Keďže aktualizáciou sa zavádza bezpečnostné opatrenie, ktoré bolo predvídané a posúdené ako súčasť pôvodného návrhu, a nezavádzajú sa ňou nové kybernetickobezpečnostné riziká, táto bezpečnostná aktualizácia by sa nemala považovať za podstatnú úpravu.

109. Naopak, bezpečnostná aktualizácia sa môže považovať za podstatnú úpravu v prípade, ak napriek svojmu bezpečnostnému cieľu vedie k tomu, že zamýšľaný účel produktu s digitálnymi prvkami sa zmení nad rámec pôvodne predpokladaného, alebo ak so sebou prináša nové alebo zvýšené kybernetickobezpečnostné riziká. Môže ísť napríklad o prípad, keď aktualizácia podstatne mení hranice produktu alebo štruktúru jeho závislostí spôsobom, ktorý nebol predvídaný v posúdení rizík, napríklad podstatnou zmenou tokov údajov alebo pridaním nových rozhraní dostupných z externého prostredia.

Príklad 49: Výrobca uvádza na trh softvérový produkt s digitálnymi prvkami, ktorý slúži na lokálne šifrovanie súborov uložených v zariadení používateľa a umožňuje používateľom šifrovať a dešifrovať súbory podľa potreby. Po zistení zraniteľnosti v procese šifrovania výrobca nasadí bezpečnostnú aktualizáciu, ktorá odstráni funkciu lokálneho šifrovania a namiesto toho vyžaduje, aby sa všetky súbory nahrávali do služby šifrovania na diaľku prevádzkovanej výrobcom, ukladali sa v nej a táto služba ich spracúvala. V dôsledku tejto zmeny produkt s digitálnymi prvkami už nevykonáva lokálne šifrovanie, ako bolo pôvodne zamýšľané, ale funguje ako služba šifrovania a spracovania údajov na diaľku. Hoci je táto aktualizácia zavedená z bezpečnostných dôvodov, zásadným spôsobom mení zamýšľaný účel daného produktu spôsobom, ktorý nebol predvídaný v posúdení rizík, a preto sa považuje za podstatnú úpravu.

Príklad 50: Výrobca uvádza na trh softvérový produkt s digitálnymi prvkami, ktorý sa pri zabezpečovaní komunikácie medzi komponentmi produktu s digitálnymi prvkami spolieha na zavedený šifrovací protokol a interne spravovaný životný cyklus kľúčov. V reakcii na novo zistené kryptografické slabé miesta výrobca zavádza bezpečnostnú aktualizáciu, ktorá nahrádza doterajší šifrovací mechanizmus iným protokolom vyžadujúcim využitie externej služby správy kľúčov prevádzkovanej treťou stranou. V dôsledku tejto zmeny dochádza k podstatnej úprave závislostí a tokov údajov v produkte s digitálnymi prvkami, čím vznikajú nové externé rozhrania a závislosť od služieb tretích strán, ktoré neboli zohľadnené v posúdení rizík. Hoci je táto aktualizácia zameraná na bezpečnosť, prináša so sebou nové kybernetickobezpečnostné riziká, a preto sa považuje za podstatnú úpravu.

110. Ako sa uvádza vyššie v bode 104, 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 úplný), či aktualizácia softvéru:

a) prináša nové vektory hrozieb, ako sú napríklad ďalšie rozhrania, komunikačné kanály, prostredia na spúšťanie alebo externé závislosti, prostredníctvom ktorých by sa hrozby mohli prejaviť;

b) umožňuje vznik nových scenárov útokov vrátane napríklad nových spôsobov, akými by s istotou mohlo dôjsť k neoprávnenému prístupu, manipulácii, zasahovaniu alebo zneužitiu produktu s digitálnymi prvkami alebo údajov, ktoré tento produkt spracúva;

c) mení pravdepodobnosť výskytu už identifikovaných scenárov útokov, napríklad tým, že znižuje úsilie alebo odborné znalosti potrebné na ich zneužitie, zvyšuje vystavenie nedôveryhodným subjektom alebo oslabuje existujúce bezpečnostné opatrenia;

d) mení potenciálny vplyv už identifikovaných scenárov útokov vrátane napríklad rozsahu postihnutých údajov alebo funkcií, závažnosti prevádzkových, bezpečnostných alebo hospodárskych dôsledkov, alebo schopnosti zistiť incident, zabrániť jeho šíreniu alebo sa z neho zotaviť.

111. V niektorých prípadoch aktualizácia softvéru neprináša nové vektory hrozieb, neumožňuje nové scenáre útokov a podstatne nemení pravdepodobnosť ani vplyv už skôr identifikovaných scenárov útokov. To môže naznačovať, že aktualizácia so sebou neprináša nové ani zvýšené kybernetickobezpečnostné riziká, pokiaľ predpoklady a opatrenia na zmiernenie rizík, na ktorých sa zakladalo posúdenie rizík, zostávajú platné a účinné. Je preto pravdepodobné, že táto aktualizácia nespĺňa kritériá podstatnej úpravy.

112. Naopak, aktualizácia softvéru môže priniesť nové vektory hrozieb, umožniť nové scenáre útokov alebo podstatne zmeniť pravdepodobnosť či vplyv existujúcich scenárov útokov. V takýchto prípadoch by mal výrobca opätovne posúdiť kybernetickobezpečnostné riziká produktu s digitálnymi prvkami a určiť, či sú naďalej splnené základné požiadavky, a to vrátane toho, či aktualizácia prináša nové alebo zvýšené riziká, ktoré neboli predvídané v posúdení rizík.

113. To, či sa aktualizácia softvéru považuje za podstatnú úpravu, je relevantné pri určovaní toho, či sa uplatňujú určité povinnosti vyplývajúce z aktu o kybernetickej odolnosti, ako je uvedené v bode 91. Bez ohľadu na uvedenú kvalifikáciu však výrobcovia naďalej zodpovedajú za zaručenie bezpečnosti aktualizácií softvéru a svojho produktu s digitálnymi prvkami počas obdobia jeho podpory v súlade s požiadavkami na riešenie zraniteľností stanovenými v časti II prílohy I k aktu o kybernetickej odolnosti. Okrem toho, bez ohľadu na to, či sa aktualizácie softvéru považujú za podstatné úpravy alebo nie, sú výrobcovia povinní zabezpečiť, aby posúdenie rizík a technická dokumentácia boli presné, úplné a neustále aktualizované v súlade s článkom 13 ods. 7 a článkom 31 ods. 2.

4.4. **Dôsledky podstatnej úpravy**

114. Dôsledky podstatnej úpravy, ktorú vykonal iný subjekt ako pôvodný výrobca produktu s digitálnymi prvkami, ktorý je už uvedený na trh, sú upravené v článkoch 21 a 22 aktu o kybernetickej odolnosti. Článok 21 sa týka dovozcov a distribútorov, zatiaľ čo článok 22 sa týka akejkoľvek fyzickej alebo právnickej osoby, ktorá nie je výrobcom, dovozcom ani distribútorom.

115. Ak podstatnú úpravu vykonáva pôvodný výrobca produktu s digitálnymi prvkami, dôsledky vyplývajú zo všeobecne zaužívaného pojmu „podstatná úprava“, na ktorý sa odvoláva odôvodnenie 41 aktu o kybernetickej odolnosti, a sú podrobnejšie rozpracované v oddiele 2.1 Modrej príručky. V tomto oddiele sa uvádza, že produkt, ktorý bol po uvedení na trh predmetom významných zmien alebo generálnych opráv, sa považuje za nový produkt, ak došlo k úprave jeho pôvodného výkonu, účelu alebo typu, ak sa zmenil charakter nebezpečenstva alebo ak sa zvýšila úroveň rizika a produkt s digitálnymi prvkami je sprístupnený na trhu.

116. Všeobecne uznávaným dôsledkom je preto skutočnosť, že ak sa úprava produktu s digitálnymi prvkami považuje za podstatnú úpravu a upravený produkt s digitálnymi prvkami sa sprístupní na trhu, na účely aktu o kybernetickej odolnosti sa s ním má zaobchádzať ako s novým produktom s digitálnymi prvkami. V dôsledku toho sa sprístupnenie podstatne upraveného produktu na trhu považuje za nové uvedenie na trh. To platí bez ohľadu na to, či podstatnú úpravu vykoná pôvodný výrobca alebo iná osoba. S cieľom zabezpečiť jednotné a primerané uplatňovanie aktu o kybernetickej odolnosti vo vzťahu k rôznym kategóriám subjektov, ktoré môžu vykonávať podstatnú úpravu, sa v nasledujúcich pododdieloch rozoberajú povinnosti osoby vykonávajúcej podstatnú úpravu v prípade, že sa podstatne upravený produkt s digitálnymi prvkami uvádza na trh. Dôsledky pre obdobie podpory produktu s digitálnymi prvkami sú uvedené v oddiele 5. *Obdobie podpory*.

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

117. V súlade s článkami 21 a 22 platí, že 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 sprístupní upravený produkt s digitálnymi prvkami na trhu, sa považuje za výrobcu upraveného produktu s digitálnymi prvkami, a to bez ohľadu na to, či sa táto osoba podieľala na pôvodnom návrhu alebo na uvedení tohto výrobku na trh.

118. V článku 22 sa ďalej upresňuje, že osoba vykonávajúca úpravu podlieha povinnostiam stanoveným v článkoch 13 a 14 iba v súvislosti s tou časťou produktu s digitálnymi prvkami, na ktorú sa podstatná úprava vzťahuje, 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, na osobu vykonávajúcu túto úpravu sa vzťahujú články 13 (vrátane povinnosti zabezpečiť súlad so základnými požiadavkami a vykonať postup posudzovania zhody) a 14 (oznamovacie povinnosti) iba v súvislosti s tou časťou produktu s digitálnymi prvkami, ktorá bola podstatne upravená ([16]). Okrem toho sa povinnosti pôvodného výrobcu vyplývajúce z aktu o kybernetickej odolnosti naďalej vzťahujú na pôvodný produkt s digitálnymi prvkami uvedený na trh, čím sa zabezpečuje kontinuita pri riešení zraniteľností a súlad v prípade nezmenených častí.

120. Prípad podstatnej úpravy by sa nemal zamieňať s prípadmi integrácie, pri ktorých osoba spája komponenty (v prípade potreby aj ich úpravou) do nového produktu s digitálnymi prvkami, ktorý sama uvádza na trh. V takýchto prípadoch integrátor neupravuje produkt s digitálnymi prvkami, ktorý už uviedol na trh iný výrobca; skôr ide o uvedenie vlastného nového produktu s digitálnymi prvkami na trh. Na účely aktu o kybernetickej odolnosti je integrátor 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 akt o kybernetickej odolnosti, môže sa spoliehať na činnosti zabezpečenia súladu výrobcov týchto komponentov, aby si uľahčil vlastný súlad s aktom o kybernetickej odolnosti.

Príklad 51: Spoločnosť nakupuje štandardné moduly mikroradiča a komponenty na pripojenie od externých dodávateľov, vyvíja vlastný firmvér a súbor snímačov a montuje ich do prepojeného produktu s digitálnymi prvkami na monitorovanie v poľnohospodárstve, ktorý uvádza na trh pod vlastným menom. Spoločnosť síce upravila základné moduly mikroradiča a skombinovala ich s inými komponentmi, nejde však o podstatnú úpravu produktu s digitálnymi prvkami, ktorý je už uvedený na trh; spoločnosť skôr uvádza na trh nový produkt s digitálnymi prvkami. Spoločnosť je na účely aktu o kybernetickej odolnosti výrobcom poľnohospodárskeho monitorovacieho zariadenia a je povinná zabezpečiť súlad s týmto nariadením, pokiaľ ide o poľnohospodárske monitorovacie zariadenie ako celok.

([16]) V súlade s oddielom 2.1 Modrej príručky „v súvislosti s aspektmi, ktoré zmena neovplyvnila, nie je potrebné opakovať skúšky a vypracovať novú dokumentáciu. Fyzická alebo právnická osoba, ktorá na výrobku vykonáva zmeny alebo ho dáva meniť, musí preukázať, že nie všetky prvky technickej dokumentácie je potrebné aktualizovať. Fyzická alebo právnická osoba, ktorá vykonáva zmeny alebo zabezpečí vykonanie zmien na výrobku, je zodpovedná za zhodu upraveného výrobku a vyhotoví vyhlásenie o zhode, a to aj v prípade, že vychádza z existujúcich skúšok a technickej dokumentácie.“

121. Ak podstatná úprava vykonaná inou osobou ako pôvodným výrobcom negatívne ovplyvňuje kybernetickú bezpečnosť produktu s digitálnymi prvkami ako celku, napríklad preto, že úprava už nie je zameraná ani obmedzená na konkrétny komponent alebo subsystém, upravený produkt s digitálnymi prvkami sprístupnený na trhu by sa mal považovať za nový produkt s digitálnymi prvkami, na ktorý sa v plnom rozsahu vzťahuje akt o kybernetickej odolnosti. V takýchto prípadoch sa zmenil celkový profil daného produktu, pokiaľ ide o kybernetickú bezpečnosť, a túto úpravu nie je možné posúdiť bez zohľadnenia produktu s digitálnymi prvkami ako celku. Osoba, ktorá vykonáva 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 rámci iteratívneho vývoja softvérových produktov s digitálnymi prvkami, tento výrobca zostáva na účely aktu o kybernetickej odolnosti výrobcom. Podstatne upravený produkt s digitálnymi prvkami sa však má považovať za produkt, ktorý bol novo uvedený na trh.

123. V súlade s oddielom 2.1 Modrej príručky môže pôvodný výrobca, ktorý uvádza na trh podstatne upravený produkt s digitálnymi prvkami, opätovne použiť existujúcu dokumentáciu a skúšky pre tie aspekty produktu s digitálnymi prvkami, na ktoré nemá podstatná úprava vplyv. Najmä v prípadoch, keď výrobca uvádza na trh podstatne upravené verzie toho istého produktu s digitálnymi prvkami, by mal byť postup posudzovania zhody zameraný na podstatne upravené časti produktu s digitálnymi prvkami. Podobne, ak posudzovanie zhody vykonáva tretia strana, orgán posudzovania zhody by mal svoje posudzovanie zamerať na podstatne upravené časti. V prípade nezmenených častí produktu s digitálnymi prvkami je možné opätovne použiť existujúcu dokumentáciu a výsledky skúšok.

124. Úvahy týkajúce sa proporcionality uvedené v predchádzajúcom pododdiele sa rovnako uplatňujú na podstatné úpravy vykonané pôvodným výrobcom produktu s digitálnymi prvkami, ktorý bol uvedený na trh pred 11. decembrom 2027. Takáto podstatná úprava vykonaná pôvodným výrobcom sama osebe neznamená, že by výrobca musel zabezpečiť úplnú zhodu celého produktu s digitálnymi prvkami uvedeného na trh pred týmto dátumom s aktom o kybernetickej odolnosti, pokiaľ táto úprava nemá negatívny vplyv na kybernetickú bezpečnosť produktu s digitálnymi prvkami ako celku. Ak táto úprava nemá vplyv na 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. Podľa článku 13 ods. 8 aktu o kybernetickej odolnosti sú výrobcovia povinní stanoviť obdobie podpory, počas ktorého sa zraniteľnosti produktu s digitálnymi prvkami vrátane jeho komponentov riešia účinne a v súlade so základnými požiadavkami stanovenými v prílohe I časti II. V období podpory je zohľadnené obdobie, počas ktorého sa predpokladá používanie produktu s digitálnymi prvkami (očakávaný 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 určuje životnosť produktov s digitálnymi prvkami ([17]). Celkovo je potrebné zohľadňovať tieto kritériá tak, aby sa pri určovaní obdobia podpory zabezpečila proporcionalita.

([17]) Medzi ďalšie kritériá, ktoré sa v súlade s článkom 13 ods. 8 môžu zohľadniť, patria obdobia podpory produktov s digitálnymi prvkami s podobnou funkciou, ktoré na trh uvádzajú iní výrobcovia, dostupnosť prevádzkového prostredia, obdobia podpory integrovaných komponentov so základnými funkciami, ktoré pochádzajú od tretích strán, ako aj príslušné usmernenia skupiny pre administratívnu spoluprácu (ďalej len „ADCO“) podľa aktu o kybernetickej odolnosti a Komisie.

126. V článku 13 ods. 8 sa ďalej stanovuje, že obdobie podpory musí trvať najmenej päť rokov, pokiaľ sa nepredpokladá, že produkt s digitálnymi prvkami sa bude používať menej ako päť rokov; v takom prípade sa obdobie podpory zhoduje s očakávaným časom používania. Minimálne obdobie podpory preto slúži iba ako ochrana, ktorou sa zabezpečuje, že sa zraniteľnosti budú riešiť počas dostatočne dlhého obdobia, pričom výrobcom sa zároveň umožňuje zohľadniť produkty s digitálnymi prvkami, ktorých očakávaný čas používania je skutočne kratší. V odôvodnení 60 sa v tejto súvislosti poskytujú ďalšie usmernenia a objasňuje sa, že produkty s digitálnymi prvkami, pri ktorých sa dá odôvodnene predpokladať, že sa budú používať dlhšie ako päť rokov, by preto mali mať dlhšie obdobia podpory. Päťročné obdobie podpory sa preto nemá považovať za štandardné pre všetky produkty s digitálnymi prvkami. Výrobca by mal namiesto toho stanoviť primerané obdobie podpory s ohľadom na kritériá uvedené v článku 13 ods. 8.

127. Článkom 13 ods. 19 sa výrobcom ukladá povinnosť, aby pri predaji jasne a zrozumiteľne uviedli dátum ukončenia obdobia podpory (aspoň mesiac a rok). Od výrobcov sa takisto vyžaduje, aby po uplynutí obdobia podpory používateľom zobrazili oznámenie, ak je to vzhľadom na povahu produktu s digitálnymi prvkami technicky možné. Cieľom tejto povinnosti je zabezpečiť pre používateľov transparentnosť, pokiaľ ide o dĺžku obdobia, počas ktorého môžu očakávať bezpečnostnú podporu.

128. V prípade softvérových produktov s digitálnymi prvkami, ktoré sa často vyvíjajú a uvádzajú na trh cyklicky 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, ktorá sa uvádza na trh, musí mať uvedené obdobie podpory v súlade s článkom 13 ods. 8. Patrí sem minimálne obdobie podpory v trvaní aspoň piatich rokov, pokiaľ očakávaný čas používania tejto verzie nie je preukázateľne kratší, ako sa takisto objasňuje v odôvodnení 60. V oddiele *5.1. Podstatné úpravy a obdobie podpory* sa ďalej objasňuje, že ak podstatná úprava nevedie k zmenám faktorov, ktoré pôvodne určovali očakávaný čas používania produktu s digitálnymi prvkami, pôvodné obdobie podpory sa nemení (t. j. vrátane prípadov, keď zostávajúce obdobie podpory je kratšie ako päť rokov).

129. Článok 13 ods. 10 poskytuje flexibilitu v prípade softvérových produktov s digitálnymi prvkami tým, že výrobcom za určitých podmienok umožňuje zabezpečiť súlad s požiadavkou na riešenie zraniteľností stanovenou v prílohe I časti II bode 2 (riešenie a náprava zraniteľností) iba v prípade verzie softvérového produktu s digitálnymi prvkami, ktorá bola uvedená na trh ako posledná. To je povolené v prípade, ak používatelia predchádzajúcich verzií majú bezplatný prístup k verzii, ktorá bola uvedená na trh ako posledná, a nevznikajú im žiadne dodatočné náklady na prispôsobenie hardvérového a softvérového prostredia, v ktorom používajú pôvodnú verziu daného produktu.

130. Na účely článku 13 ods. 10 by sa mal pojem „dodatočné náklady“ vykladať prakticky a primeraným spôsobom, pričom by sa mali zohľadniť bežné a očakávané postupy pri údržbe a prevádzke softvéru. Do dodatočných nákladov sa nezahŕňa primerané prevádzkové úsilie, ktoré je neoddeliteľnou súčasťou uplatňovania aktualizácií softvéru alebo udržiavania bezpečného prevádzkového prostredia, ako napríklad čas personálu, bežné skúšanie, úpravy konfigurácie alebo modernizácie základných softvérových závislostí, ktoré sú potrebné na riešenie komponentov na konci životnosti alebo známych bezpečnostných zraniteľností. Naopak, pojem „dodatočné náklady“ sa vzťahuje na záťaže, ktoré presahujú rámec toho, čo sa bežne dá očakávať v súvislosti s aktualizáciami softvéru, ako sú napríklad povinný nákup nového hardvéru, výmena infraštruktúry alebo zásadné zmeny prevádzkového prostredia.

131. V prípade softvérových produktov s digitálnymi prvkami, ktoré sa neustále vyvíjajú, môžu výrobcovia uvádzať na trh v pomerne krátkych intervaloch následné podstatne upravené verzie a očakávať, že používatelia budú pravidelne vykonávať modernizáciu. 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 stanoviť nové obdobie podpory. Výrobcovia sa však môžu odvolať na článok 13 ods. 10 s cieľom ukončiť riešenie a nápravu zraniteľností v prípade skorších verzií, keď používatelia

môžu bezplatne a bez vzniku uvedených dodatočných nákladov modernizovať na novšiu verziu, a to aj v prípade, že to vedie ku kratšiemu skutočnému obdobiu podpory skorších verzií ([18]). Výrobca naďalej podlieha ostatným požiadavkám na riešenie zraniteľností uvedeným v prílohe I časti II, ako aj ohlasovacím povinnostiam podľa článku 14. Ako sa uvádza aj v odôvodnení 40, tieto požiadavky zahŕňajú okrem iného pre všetky následné podstatne upravené verzie softvérového produktu s digitálnymi prvkami uvádzané na trh: i) dodržiavanie politiky koordinovaného zverejňovania informácií o zraniteľnostiach a ii) opatrenia na uľahčenie výmeny informácií o potenciálnych zraniteľnostiach ([19]).

Príklad 52: Výrobca uvedie model smartfónu na trh EÚ a stanoví obdobie podpory X rokov od dátumu uvedenia na trh, počas ktorého bude poskytovať bezpečnostné aktualizácie, ktorými sa riešia zraniteľnosti. Počas tohto obdobia výrobca vydáva pravidelné aktualizácie softvéru a podstatne upravené verzie operačného systému, ktoré používatelia môžu nainštalovať bezplatne bez potreby nového hardvéru.

Výrobca môže v súlade s článkom 13 ods. 10 riešiť a napravať zraniteľnosti v najnovšej verzii operačného systému, ktorá je k dispozícii pre daný model smartfónu, a to za predpokladu, že staršie verzie je možné modernizovať bezplatne a bez dodatočných nákladov. Počas trvania obdobia podpory sa na výrobcu naďalej vzťahujú ostatné požiadavky na riešenie zraniteľností, ako napríklad koordinované zverejňovanie informácií o zraniteľnostiach a opatrenia na výmenu informácií.

Príklad 53: Výrobca uvádza na trh podnikový softvérový produkt s digitálnymi prvkami a každých niekoľko mesiacov vydáva podstatne upravené verzie, ktoré odrážajú zlepšenia v oblasti bezpečnosti, nové funkcie 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 v rámci bežnej prevádzky pravidelne vykonávať modernizáciu, a poskytuje bezplatný prístup k najnovšej verzii. Pri uplatňovaní modernizácie sa môže vyžadovať primerané prevádzkové úsilie, napríklad testovanie alebo úpravy konfigurácie, nevyžadujú sa však dodatočné náklady, ako je nákup nového hardvéru alebo zásadné zmeny infraštruktúry. V tejto súvislosti sa výrobca môže odvolať na článok 13 ods. 10 s cieľom ukončiť riešenie a nápravu zraniteľností v prípade skorších verzií, keď používatelia môžu modernizovať na najnovšiu verziu, pričom naďalej dodržiava ostatné požiadavky na riešenie zraniteľností v prípade všetkých následných podstatne upravených verzií.

5.1. **Podstatné úpravy a obdobie podpory**

132. Ako je uvedené v oddiele 4.4. *Dôsledky podstatnej úpravy,* ak sa úprava produktu s digitálnymi prvkami považuje za podstatnú úpravu a upravený výrobok s digitálnymi prvkami sa sprístupní na trhu, na účely aktu o kybernetickej odolnosti sa s ním má zaobchádzať ako s novým produktom a sprístupnenie podstatne upraveného produktu s digitálnymi prvkami na trhu predstavuje nové uvedenie na trh. Je preto užitočné objasniť, aký vplyv má toto nové uvedenie na trh na obdobie podpory v prípade podstatne upraveného produktu s digitálnymi prvkami.

133. Obdobie podpory pre podstatne upravený produkt s digitálnymi prvkami by sa malo stanoviť s ohľadom na očakávaný čas používania daného produktu, a to na základe kritérií stanovených v článku 13 ods. 8 aktu o kybernetickej odolnosti. Podstatná úprava by si preto mala vyžadovať opätovné posúdenie na základe týchto kritérií, ale nemusí automaticky viesť k obnoveniu či dokonca predĺženiu obdobia podpory. Hlavnou otázkou je, či podstatná úprava ovplyvňuje faktory, ktoré pôvodne určili očakávaný čas používania daného produktu, a tým aj pôvodné obdobie podpory.

([18]) Treba pripomenúť, že v článku 13 ods. 19 sa vyžaduje, aby výrobcovia, ak je to vzhľadom na povahu produktu s digitálnymi prvkami technicky možné, zobrazili pre používateľov oznámenie s informáciou, že obdobie podpory ich produktu s digitálnymi prvkami sa skončilo. Preto v sa prípadoch, keď sa už riešenie a náprava zraniteľnosti starších verzií ukončili, očakáva, že používatelia, ktorí nemodernizovali na najnovšiu verziu, o tom budú informovaní, ak je to technicky možné.

([19]) Je potrebné poznamenať, že aj keď používatelia môžu bez dodatočných nákladov modernizovať softvér na najnovšiu verziu, výrobcovia sa napriek tomu môžu rozhodnúť, že budú naďalej riešiť a napravať zraniteľnosti v starších verziách tohto softvéru, a to aj za poplatok alebo na základe iných komerčných dohôd. V akte o kybernetickej odolnosti sa nevyžaduje, aby výrobcovia poskytovali aktualizácie softvéru zamerané na bezpečnosť pre takéto skoršie verzie bezplatne.

134. Ak podstatná úprava nemá vplyv na tieto faktory, na základe kritérií uvedených v článku 13 ods. 8 sa naďalej stanovuje rovnaký očakávaný čas používania, ako bol pôvodne stanovený, a obdobie podpory pre upravený produkt s digitálnymi prvkami by sa malo zosúladiť so zostávajúcim očakávaným časom používania produktu, ktorý bol pôvodne uvedený na trh. Typicky pôjde o prípad, keď bol očakávaný čas používania určený predovšetkým faktormi, ktoré úprava nemení, ako je fyzická životnosť hardvérových komponentov, pričom podstatná úprava sa týka len funkcií softvéru alebo back-endových služieb.

Príklad 54: Výrobca uvádza na trh robotický vysávač s očakávaným časom používania X rokov, ktorý bol určený na základe povahy produktu s digitálnymi prvkami, a to aj s prihliadnutím na fyzickú životnosť a charakteristiky opotrebovania hardvérových komponentov a 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 sa považuje za podstatnú úpravu a ktorou sa pridávajú nové režimy čistenia a funkcie navigácie. Aktualizácia softvéru nemá vplyv na fyzickú životnosť hardvéru a nemení primerané očakávania používateľov, pokiaľ ide o životnosť daného produktu. Na základe kritérií podľa článku 13 ods. 8 sa teda naďalej uvádza rovnaký očakávaný čas používania. Obdobie podpory upraveného produktu s digitálnymi prvkami zodpovedá zostávajúcemu očakávanému času používania, ako bol pôvodne určený.

Príklad 55: Výrobca uvádza na trh komplexný priemyselný strojový produkt s digitálnymi prvkami s cloudovým back-endom, ktorý predstavuje riešenie na spracovanie údajov na diaľku. Očakávaný čas používania je X rokov a určil sa s prihliadnutím na primerané očakávania používateľov a povahu produktu s digitálnymi prvkami, ako sú fyzická životnosť hardvéru strojového zariadenia a predpokladané opotrebovanie. Obdobie podpory je stanovené na X rokov tak, aby zodpovedalo uvedenému očakávanému času používania. Po Y rokoch výrobca zmení architektúru cloudového back-endu (riešenia na spracovanie údajov na diaľku), pričom zavedie nové rozhrania API a toky údajov spôsobom, ktorý predstavuje podstatnú úpravu produktu s digitálnymi prvkami, ale nemení povahu tohto produktu ani neovplyvňuje očakávania používateľov. Na základe kritérií podľa článku 13 ods. 8 sa teda naďalej uvádza rovnaký očakávaný čas používania. Obdobie podpory upraveného produktu s digitálnymi prvkami zodpovedá zostávajúcemu očakávanému času používania, ako bol pôvodne určený.

135. Ak podstatná úprava ovplyvňuje faktory, ktoré pôvodne určovali očakávaný čas používania produktu s digitálnymi prvkami, výrobca by mal prepočítať obdobie podpory tak, aby zohľadňovalo nový očakávaný čas používania, a primerane pritom uplatniť kritériá uvedené v článku 13 ods. 8. Môže ísť napríklad o revitalizačné úpravy hardvéru, ktoré predlžujú prevádzkovú životnosť daného produktu, alebo o podstatné preprogramovanie či prepísanie základného softvéru daného produktu, ktoré významne mení jeho očakávaný čas používania ([20]).

Príklad 56: Výrobca uvádza na trh programovateľnú logickú riadiacu jednotku (PLC) s očakávaným časom používania X rokov, ktorá bola určená predovšetkým na základe povahy produktu s digitálnymi prvkami a životnosti základného hardvéru. Obdobie podpory je stanovené podľa týchto faktorov. Niekoľko rokov po pôvodnom uvedení na trh výrobca vykoná podstatnú úpravu spočívajúcu vo výmene zabudovanej výpočtovej platformy PLC vrátane procesora, pamäte a prostredia režimu runtime za novú generáciu komponentov navrhnutých na výrazne dlhšiu prevádzkovú životnosť. V dôsledku tejto úpravy sa menia primerané očakávania používateľov a povaha produktu s digitálnymi prvkami: používateľ PLC môže teraz dôvodne očakávať, že PLC zostane v produktívnom používaní aj po uplynutí pôvodne deklarovaného očakávaného času používania, a to vďaka novej výpočtovej platforme. Kritériá podľa článku 13 ods. 8 preto poukazujú na dlhší očakávaný čas používania a výrobca v súlade s tým prepočíta obdobie podpory pre konkrétnu PLC.

6. **DÔLEŽITÉ A KRITICKÉ PRODUKTY S DIGITÁLNYMI PRVKAMI**

136. V článku 7 ods. 1 aktu o kybernetickej odolnosti sa stanovuje, že produkty s digitálnymi prvkami, ktoré majú základnú funkciu kategórie produktov uvedenej v prílohe III k uvedenému nariadeniu, sa považujú za „dôležité produkty s digitálnymi prvkami“. V prílohe III sa ďalej rozdeľujú dôležité produkty s digitálnymi prvkami do triedy I a triedy II. Podobne sa v článku 8 ods. 1 stanovuje, že produkty s digitálnymi prvkami, ktorých hlavná funkcia patrí do kategórie produktov uvedenej v prílohe IV k aktu o kybernetickej odolnosti, sa považujú za „kritické produkty s digitálnymi prvkami“ ([21]).

([20]) Treba pripomenúť, že, ako sa uvádza v oddiele 4.1. *Fyzické opravy,* činnosti súvisiace s renováciou, údržbou alebo opravou sa vo všeobecnosti nepovažujú za podstatné úpravy.

([21]) Vo vykonávacom nariadení Komisie (EÚ) 2025/2392 sa stanovuje technický opis kategórií dôležitých a kritických produktov.

137. Klasifikácia výrobku s digitálnymi prvkami ako dôležitého alebo kritického, alebo naopak ako produktu patriaceho do kategórie „štandardných“ výrobkov ([22]) má význam pri určovaní postupu posudzovania zhody, ktorý musí výrobca v súlade s článkom 32 dodržať, než bude môcť tento produkt s digitálnymi prvkami uviesť na trh. Je potrebné poznamenať, že pri produktoch s digitálnymi prvkami zaradených do štandardnej kategórie sa možno vždy spoliehať na postup vnútornej kontroly založený na module A („vlastné posúdenie“) ([23]). Na dôležité produkty s digitálnymi prvkami triedy I alebo II a kritické produkty s digitálnymi prvkami sa vzťahujú prísnejšie postupy posudzovania zhody. Netýka sa to dôležitých produktov s digitálnymi prvkami triedy I alebo II, ktoré sa kvalifikujú ako slobodný softvér a softvér s otvoreným zdrojovým kódom a ktoré sa uvádzajú na trh, pričom výrobcom takýchto produktov sa v súlade s článkom 32 ods. 5 umožňuje postupovať podľa postupov štandardnej kategórie.

138. Pojem základná funkcia je preto pre výrobcu nevyhnutný na určenie uplatniteľného režimu posudzovania zhody. Tento pojem však nie je v akte o kybernetickej odolnosti výslovne vymedzený. Produkty s digitálnymi prvkami môžu plniť rôzne funkcie, pričom niektoré z nich môžu byť vedľajšie vo vzťahu k základnej funkcii daného produktu a nemali by mať vplyv na klasifikáciu produktu ako štandardného/dôležitého triedy I/dôležitého triedy II/kritického. Preto je užitočné poskytnúť ďalšie usmernenia s cieľom pomôcť výrobcom správne vykonávať príslušné postupy posudzovania zhody a orgánom dohľadu nad trhom zabezpečiť harmonizované presadzovanie aktu o kybernetickej odolnosti v celej Únii.

6.1. **Základná funkcia**

139. Základná funkcia produktu s digitálnymi prvkami sa vzťahuje na hlavné vlastnosti a technické schopnosti tohto produktu, bez ktorých by nebol schopný plniť svoj zamýšľaný účel. Možno ju posúdiť s prihliadnutím na osobitný kontext a podmienky používania daného produktu, pričom sa okrem iného zohľadnia informácie, ktoré výrobca poskytuje v návode na použitie, propagačných alebo predajných materiáloch a vyhláseniach, ako 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 vlastnosti patrí inicializácia hardvéru a periférnych zariadení, správa procesov a pamäte, riadenie vstupu a výstupu, plánovanie, prideľovanie zdrojov a sprístupňovanie systémových služieb a rozhraní na programovanie aplikácií (API), prostredníctvom ktorých aplikácie interagujú s hardvérovými a softvérovými zdrojmi zariadenia. Z technickej dokumentácie vyplýva, že produkt s digitálnymi prvkami koordinuje výpočtové zdroje, presadzuje konfigurácie systému a poskytuje štandardizované rozhrania pre softvérové moduly a pripojené periférne zariadenia. Výrobca zdôrazňuje, že vďaka týmto schopnostiam môže platforma slúžiť ako centrálne softvérové prostredie, v ktorom je možné spoľahlivo prevádzkovať aplikácie. Produkt s digitálnymi prvkami má základnú funkciu operačného systému, ako sa opisuje v bode 11 prílohy I k vykonávaciemu nariadeniu (EÚ) 2025/2392.

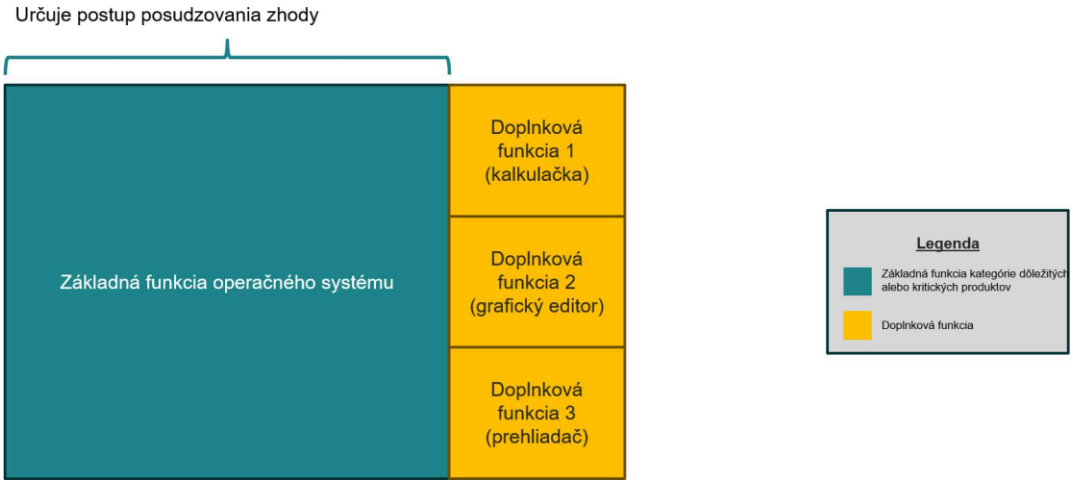
140. Funkcia produktu s digitálnymi prvkami je len zriedka obmedzená výlučne na jeho základnú funkciu, keďže produkty s digitálnymi prvkami často – ak nie vždy – vykonávajú aj ďalšie funkcie, ktoré neprispievajú k základnej funkcii daného produktu. Môže sem patriť aj začlenenie komponentov, ktoré samy osebe majú funkciu iného dôležitého alebo kritického produktu s digitálnymi prvkami. Skutočnosť, že produkt s digitálnymi prvkami vykonáva iné funkcie, než sú funkcie podrobne opísané v technických opisoch dôležitých alebo kritických produktov s digitálnymi prvkami, alebo funkcie, ktoré sú k nim doplnkové, však sama osebe nebráni tomu, aby tento produkt mal jednu z takýchto základných funkcií.

([22]) Pojem „štandardná kategória“ nie je pojmom vymedzeným v akte o kybernetickej odolnosti. Použitie tohto pojmu v tomto dokumente sa vzťahuje na produkty s digitálnymi prvkami, ktoré nemajú základnú funkciu kategórie produktov uvedenej v prílohe III alebo IV k aktu o kybernetickej odolnosti a na ktoré sa v dôsledku toho vzťahuje režim posudzovania zhody stanovený v článku 32 ods. 1.

([23]) Výrobca sa však môže kedykoľvek rozhodnúť uplatniť prísnejší postup posudzovania zhody, ako je stanovené v článku 32 ods. 1.

Obrázok 2

Znázornenie toho, ako základná funkcia, a nie doplnkové funkcie, určuje uplatniteľný postup posudzovania zhody



141. Produkt s digitálnymi prvkami môže byť schopný vykonávať funkcie kategórie dôležitých alebo kritických produktov, ale napriek tomu môže mať základnú funkciu odlišnú od základnej funkcie 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 aktu o kybernetickej odolnosti v súvislosti s dôležitými produktmi s digitálnymi prvkami (pričom rovnaká logika sa uplatňuje aj na kritické produkty s digitálnymi prvkami), samotná integrácia dôležitého alebo kritického produktu s digitálnymi prvkami sama osebe nespôsobuje, že sa produkt s digitálnymi prvkami stáva dôležitým alebo kritickým produktom s digitálnymi prvkami.

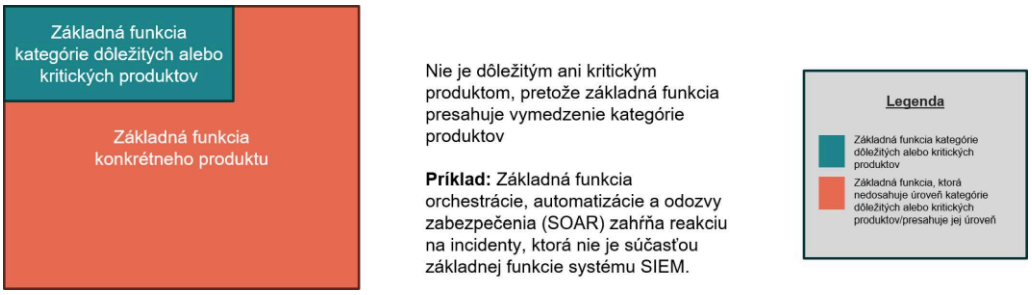
Príklad 58: Smartfón obsahuje operačný systém, ktorý poskytuje funkcie opísané v bode 11 prílohy I k vykonávaciemu nariadeniu (EÚ) 2025/2392. Zatiaľ čo operačný systém umožňuje správu hardvérových zdrojov a spúšťanie softvérových aplikácií, smartfón ako celok má inú základnú funkciu (napr. umožňuje používateľom komunikovať a získavať prístup k informáciám a službám). Samotná integrácia operačného systému ešte neznamená, že smartfón disponuje základnými funkciami operačného systému.

142. Niektoré produkty s digitálnymi prvkami môžu byť podobné kategórii dôležitých alebo kritických produktov alebo môžu patriť do rovnakej všeobecnej skupiny produktov, ich základná funkcia však môže základnú funkciu danej kategórie výrazne presahovať alebo ju nemusí spĺňať. Neplatí to však v prípade, keď produkt s digitálnymi prvkami zahŕňa ďalšie funkcie, ktoré len doplňajú alebo zlepšujú základnú funkciu, ktorá sama zodpovedá základnej funkcii kategórie dôležitých alebo kritických produktov; v takýchto prípadoch si produkt s digitálnymi prvkami zachováva základnú funkciu danej kategórie a je podľa toho klasifikovaný. Toto posúdenie by malo vychádzať z hlavných vlastností a technických schopností daného produktu, ktoré sa objektívne posudzujú s prihliadnutím na jeho zamýšľaný účel, a nie zo spôsobu, akým je produkt s digitálnymi prvkami opísaný alebo uvádzaný na trh, ak tento opis nezodpovedá skutočným technickým vlastnostiam produktu.

Príklad 59: Softvér orchestrácie, automatizácie a odozvy zabezpečenia (SOAR) často dokáže vykonávať funkcie produktov s digitálnymi prvkami kategórie „systémy riadenia bezpečnostných informácií a udalostí (SIEM)“, t. j. zhromažďovať údaje z viacerých zdrojov, analyzovať a korelovať tieto údaje a prezentovať ich ako informácie umožňujúce prijatie opatrení na účely súvisiace s bezpečnosťou. Základná funkcia tohto softvéru však výrazne presahuje základnú funkciu systému SIEM a zahŕňa aj služby, ako je reakcia na incidenty, ktoré tvoria základné prvky jeho technických schopností. Softvér SOAR sa preto vo všeobecnosti nepovažuje za softvér, ktorý má základnú funkciu systémov SIEM.

Obrázok 3

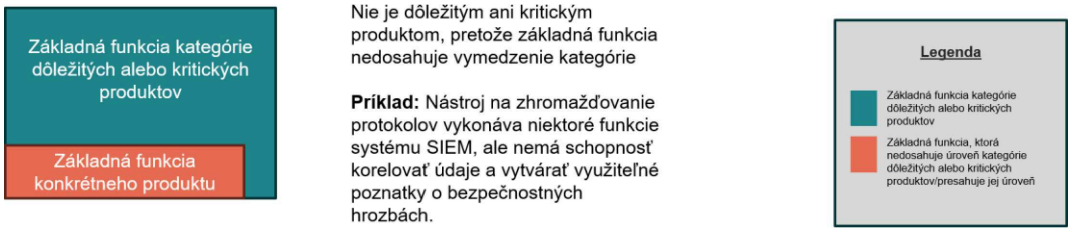
Znázornenie základnej funkcie produktu s digitálnymi prvkami, ktorá výrazne presahuje vymedzenie kategórie dôležitých alebo kritických produktov



Príklad 60: Niektoré nástroje na zhromažďovanie a vizualizáciu protokolov majú schopnosť prijímať údaje z protokolov a zobrazovať základné informačné panely znázorňujúce systémové udalosti. Hoci tieto nástroje môžu podporovať činnosti monitorovania bezpečnosti, ich základná funkcia nedosahuje úroveň základnej funkcie systémov SIEM, keďže nevykonávajú koreláciu údajov ani neposkytujú využiteľné poznatky v oblasti bezpečnosti. Takéto nástroje sa preto vo všeobecnosti nepovažujú za nástroje, ktoré majú základnú funkciu systémov SIEM.

Obrázok 4

Znázornenie základnej funkcie produktu s digitálnymi prvkami, ktorá podstatne nevyhovuje vymedzeniu kategórie dôležitých alebo kritických produktov

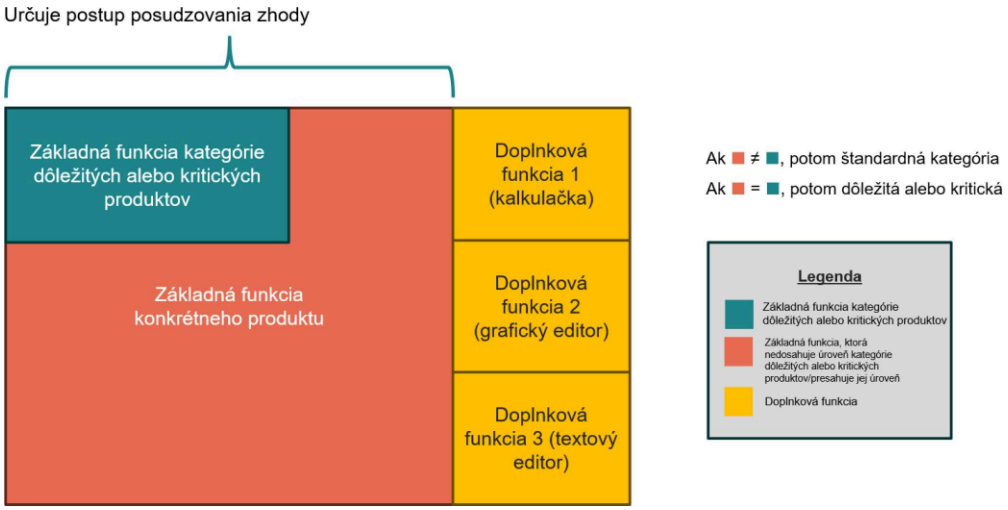


143. Výrobca nesmie skresľovať základnú funkciu svojho produktu s digitálnymi prvkami takým spôsobom, aby sa vyhol režimu posudzovania zhody uplatniteľnému na dôležité alebo kritické produkty s digitálnymi prvkami, napríklad neprimeraným zdôrazňovaním alebo zľahčovaním úlohy určitých funkcií, v dôsledku čoho produkt výrazne presahuje určitú základnú funkciu alebo ju nespĺňa. Tak by to bolo napríklad vtedy, keď by existovali zjavné nezrovnalosti medzi propagačnými materiálmi, návodmi na použitie a technickou dokumentáciou.

144. Produkt s digitálnymi prvkami nemôže mať na účely určenia uplatniteľného režimu posudzovania zhody viac ako jednu základnú funkciu. V súlade s prílohou VII k aktu o kybernetickej odolnosti sú výrobcovia povinní v rámci technickej dokumentácie produktu opísať zamýšľaný účel svojho produktu s digitálnymi prvkami a postup posudzovania zhody, ktorý uplatnili. Základná funkcia produktu by preto mala byť jasne identifikovaná. Umožňuje to správne určiť príslušný režim posudzovania zhody a orgánom dohľadu nad trhom vykonávať dohľad a overovať, či sa nariadenie správne uplatňuje.

Obrázok 5

Znázornenie toho, ako základná funkcia konkrétneho produktu s digitálnymi prvkami určuje triedu produktu, a teda aj uplatniteľný postup posudzovania zhody



145. Niektoré produkty s digitálnymi prvkami sa uvádzajú na trh ako samostatné produkty s digitálnymi prvkami, ale pozostávajú z rozličných modulov so samostatnými funkciami. Ak výrobca sprístupňuje tieto moduly na trhu aj samostatne, napríklad v prípade, že sú ponúkané na samostatný nákup, licencovanie alebo predplatné, tieto moduly samy osebe predstavujú samostatné produkty s digitálnymi prvkami. Ako také sa majú klasifikovať na základe príslušných základných funkcií (a preto sa na ne vzťahuje príslušný režim posudzovania zhody podľa základnej funkcie každého modulu). Tým nie sú dotknuté moduly, ktoré sa dodávajú výlučne ako komponenty integrovaného produktu s digitálnymi prvkami a ktoré sa neponúkajú samostatne; v takýchto prípadoch sa základná funkcia určuje na úrovni integrovaného produktu s digitálnymi prvkami.

Príklad 61: Výrobca uvádza na trh jednotný balík bezpečnostných riešení, ktorý kombinuje viacero modulov vrátane systému SIEM, systému detekcie narušenia a analytického modulu. Výrobca ponúka tieto moduly aj v rámci samostatného predplatného. V tomto scenári je každý modul samostatným produktom s digitálnymi prvkami a klasifikuje sa na základe vlastnej základnej funkcie. Na modul SIEM sa vzťahuje režim posudzovania zhody pre dôležité produkty s digitálnymi prvkami triedy I, keďže jeho základnou funkciou je funkcia „Systémy riadenia bezpečnostných informácií a udalostí (SIEM)“. Na systém detekcie narušenia sa vzťahuje režim posudzovania zhody pre dôležité produkty s digitálnymi prvkami triedy II, keďže jeho základnou funkciou je funkcia „Brány firewall, systémy na detekciu a prevenciu narušení“. Na analytický modul sa vzťahuje režim posudzovania zhody pre „štandardné“ produkty s digitálnymi prvkami, keďže jeho základnou funkciou nie je základná funkcia kategórie dôležitých ani kritických produktov.

146. Nedodržanie povinností stanovených v článku 32 aktu o kybernetickej odolnosti môže viesť k uloženiu správnych pokút v súlade s článkom 64 ods. 3.

6.2. Posudzovanie zhody dôležitých a kritických produktov s digitálnymi prvkami

147. Keď výrobca určí základnú funkciu svojho produktu s digitálnymi prvkami, musí vykonať jeden z uplatniteľných postupov posudzovania zhody. Musí zabezpečiť, aby produkt s digitálnymi prvkami ako celok spĺňal základné požiadavky, pričom podľa potreby zohľadní bezpečnosť komponentov alebo funkcií, ktoré sú doň integrované.

148. Prísnejší postup posudzovania zhody so zapojením tretej strany (založený na moduloch B + C, module H alebo schémach certifikácie kybernetickej bezpečnosti) je záväzný pre dôležité produkty s digitálnymi prvkami triedy II (s výnimkou produktov, ktoré sa kvalifikujú ako slobodný softvér a softvér s otvoreným zdrojovým kódom, v súlade s článkom 32 ods. 5) a pre kritické produkty s digitálnymi prvkami ([24]). Na rozdiel od toho sa od dôležitých produktov s digitálnymi prvkami triedy I (s výnimkou produktov, ktoré sa kvalifikujú ako slobodný softvér a softvér s otvoreným zdrojovým kódom, v súlade s článkom 32 ods. 5) vyžaduje, aby podstúpili postup posudzovania zhody treťou stranou len v prípade, že výrobca neuplatnil alebo uplatnil len čiastočne príslušné harmonizované normy, ktorých odkazy boli uverejnené v *Úradnom vestníku Európskej únie* (ďalej len „harmonizované normy"), spoločné špecifikácie alebo európske schémy certifikácie kybernetickej bezpečnosti s úrovňou zabezpečenia aspoň „podstatná" ([25]).

149. Aby sa teda na dôležitý produkt s digitálnymi prvkami triedy I mohol uplatniť postup vnútornej kontroly, i) treba uplatniť všetky uplatniteľné požiadavky príslušnej harmonizovanej normy a ii) rozsah normy musí pokrývať aspoň všetky kybernetickobezpečnostné riziká spojené so základnou funkciou daného produktu.

150. Rozsah produktu s digitálnymi prvkami môže byť širší než rozsah, ktorý sa predpokladá v príslušnej harmonizovanej norme, pričom takéto doplnkové funkcie môžu predstavovať odlišné alebo dodatočné kybernetickobezpečnostné riziká. Výrobca je vždy povinný vykonať posúdenie rizík v súlade s článkom 13 ods. 2, a preto by mal 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 funkciou daného produktu, môže sa rozhodnúť využiť postup vnútornej kontroly na preukázanie zhody svojho produktu. V rámci činností zameraných na posudzovanie zhody bude výrobca naďalej povinný preukázať, že sú zohľadnené všetky riziká, ktoré sa vzťahujú na jeho produkt s digitálnymi prvkami. Ak teda existuje rozdiel medzi rozsahom pôsobnosti harmonizovanej normy a rozsahom pôsobnosti produktu s digitálnymi prvkami ako celku, výrobca musí aj naďalej zdokumentovať, aké dodatočné opatrenia prijal na zvládnutie týchto rizík.

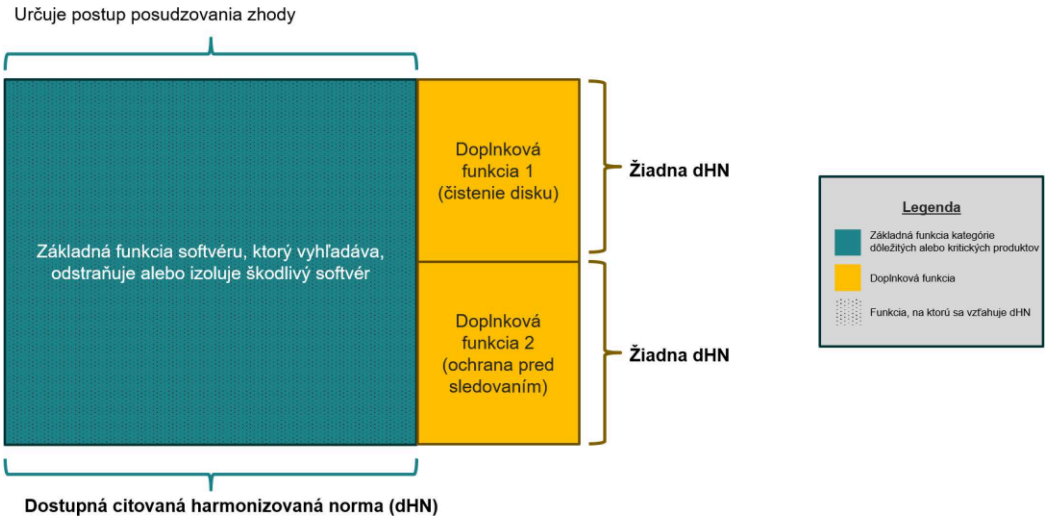
Príklad 62: Antivírusový softvér má základnú funkciu softvéru, ktorý vyhľadáva, odstraňuje alebo umiestňuje škodlivý softvér do karantény, ako sa opisuje v bode 4 prílohy I k vykonávaciemu nariadeniu (EÚ) 2025/2392. Daný produkt s digitálnymi prvkami zahŕňa aj ďalšie funkcie, konkrétne funkciu čistenia disku a funkciu ochrany pred sledovaním, ktorá chráni používateľa pri prehliadaní webu. Výrobca vykoná posúdenie rizík, ktoré sa vzťahuje na produkt s digitálnymi prvkami ako celok vrátane základnej funkcie antivírusového softvéru a funkcií čistenia disku a ochrany pred sledovaním. Uplatňuje harmonizovanú normu, ktorá pokrýva riziká spojené so základnou funkciou antivírusového softvéru, a dodatočné opatrenia na riešenie rizík vyplývajúcich z ďalších funkcií. Výrobca môže na posúdenie zhody využiť postup vnútornej kontroly, ktorý sa vzťahuje na produkt s digitálnymi prvkami ako celok vrátane funkcií čistenia disku a ochrany pred sledovaním.

([24]) To platí aj v prípade využitia európskej schémy certifikácie kybernetickej bezpečnosti aspoň na úrovni záruky „významná", keďže sa vyžaduje zapojenie certifikačného subjektu tretej strany.

([25]) Z dôvodu stručnosti sa vo zvyšnej časti tohto oddielu odkazuje len na harmonizované normy, ktorých odkazy boli uverejnené v *Úradnom vestníku Európskej únie*. Tieto usmernenia sa však rovnako vzťahujú aj na spoločné špecifikácie prijaté v súlade s článkom 27 ods. 2 a na európske schémy certifikácie kybernetickej bezpečnosti, ak tak Komisia stanoví prostredníctvom delegovaných aktov v súlade s článkom 27 ods. 9.

Obrázok 6

Znázornenie toho, ako použitie harmonizovanej normy, ktorej odkaz bol uverejnený a ktorá pokrýva len základnú funkciu, určuje uplatniteľný postup posudzovania zhody



152. To platí aj v prípade, keď produkt s digitálnymi prvkami obsahuje dodatočnú funkciu, ktorá sama osebe predstavuje funkciu iného dôležitého alebo kritického produktu s digitálnymi prvkami. V skutočnosti o tom, či produkt s digitálnymi prvkami patrí do kategórie dôležitých alebo kritických produktov (a teda aj o uplatniteľnom režime posudzovania zhody), rozhoduje základná funkcia produktu s digitálnymi prvkami ako celku, a nie funkcia integrovaných komponentov posudzovaných samostatne. Napríklad ak má produkt s digitálnymi prvkami základnú funkciu dôležitého produktu s digitálnymi prvkami triedy I, na tento produkt ako celok sa vzťahuje režim posudzovania zhody uplatniteľný na dôležité produkty s digitálnymi prvkami triedy I, aj keď je doň integrovaný komponent, ktorý je sám osebe kritickým produktom s digitálnymi prvkami. V týchto prípadoch, ak výrobca uplatňuje harmonizovanú normu, ktorá pokrýva riziká spojené so základnou funkciou daného produktu, môže využiť postup vnútornej kontroly.

Príklad 63: Hardvérový produkt s digitálnymi prvkami má základnú funkciu smerovača, ako sa opisuje v bode 12 prílohy I k vykonávaciemu nariadeniu (EÚ) 2025/2392. Daný produkt s digitálnymi prvkami zahŕňa aj ďalšie funkcie vrátane funkcií firewallu, keďže integruje komponent firewallu. Výrobca vykonáva posúdenie rizík, ktoré sa vzťahuje na celý produkt s digitálnymi prvkami vrátane základnej funkcie smerovača a funkcie firewallu. Uplatňuje harmonizovanú normu, ktorá pokrýva riziká spojené so základnou funkciou smerovača, a dodatočné opatrenia na riešenie rizík vyplývajúcich z ďalších funkcií. Výrobca môže napríklad uplatniť harmonizovanú normu pre firewally, aby sa pokryli riziká spojené s funkciou firewallu. Výrobca môže na účely posúdenia zhody využiť postup vnútornej kontroly, ktorý sa vzťahuje na produkt s digitálnymi prvkami ako celok vrátane funkcie firewallu.

6.3. Dôsledky pre predpoklad zhody

153. V článku 27 ods. 1 aktu o kybernetickej odolnosti sa stanovuje, že o produktoch s digitálnymi prvkami a postupoch zavedených výrobcom, ktoré sú v zhode s harmonizovanými normami alebo ich časťami, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*, sa predpokladá, že sú v zhode so základnými požiadavkami aktu

o kybernetickej odolnosti, na ktoré sa vzťahujú tieto normy alebo ich časti ([26]). Článkom 27 ods. 5 sa rovnaký predpoklad zhody rozširuje na produkty s digitálnymi prvkami a procesy zavedené výrobcom, ktoré sú v zhode so spoločnými špecifikáciami prijatými Komisiou prostredníctvom vykonávacích aktov, a článkom 27 ods. 8 sa stanovuje predpoklad zhody pre produkty s digitálnymi prvkami a procesy zavedené výrobcom, pre ktoré bolo vydané EÚ vyhlásenie o zhode alebo certifikát podľa európskej schémy certifikácie kybernetickej bezpečnosti prijatej podľa nariadenia (EÚ) 2019/881, ak tak bolo stanovené prostredníctvom delegovaných aktov v súlade s článkom 27 ods. 9 ([27]).

154. Ak teda výrobca uplatnil harmonizovanú normu, na ktorú sa vzťahujú odkazy uverejnené v *Úradnom vestníku Európskej únie*, platí pre neho predpoklad zhody v súvislosti s rizikami, na ktoré sa daná norma vzťahuje. Môže ísť napríklad o prípad, keď sa harmonizovanou normou, ktorej odkaz bol uverejnený, riešia všetky riziká spojené so základnou funkciou produktu s digitálnymi prvkami a neexistujú žiadne ďalšie funkcie, ktoré predstavujú kybernetickobezpečnostné riziká. Predpokladá sa napríklad, že v harmonizovanej norme pre smerovače sa budú riešiť aspoň riziká spojené so základnými funkciami týchto produktov s digitálnymi prvkami. Ak takýto produkt neobsahuje žiadne ďalšie funkcie alebo ak tieto ďalšie funkcie nepredstavujú riziká, ktoré sa v norme neriešia, na produkt s digitálnymi prvkami sa môže vzťahovať predpoklad zhody.

155. V prípadoch zmienených v bodoch 151 a 152 môže výrobca použiť postup vnútornej kontroly, pretože harmonizovaná norma pokrýva riziká spojené so základnou funkciou produktu s digitálnymi prvkami. Produkty s digitálnymi prvkami opísané v týchto príkladoch však môžu mať širší rozsah než harmonizované normy a ďalšie funkcie môžu predstavovať kybernetickobezpečnostné riziká, ktoré sa v takejto harmonizovanej norme neriešia. Na produkty s digitálnymi prvkami sa preto nemusí vzťahovať predpoklad zhody, pokiaľ ide o tieto ďalšie funkcie.

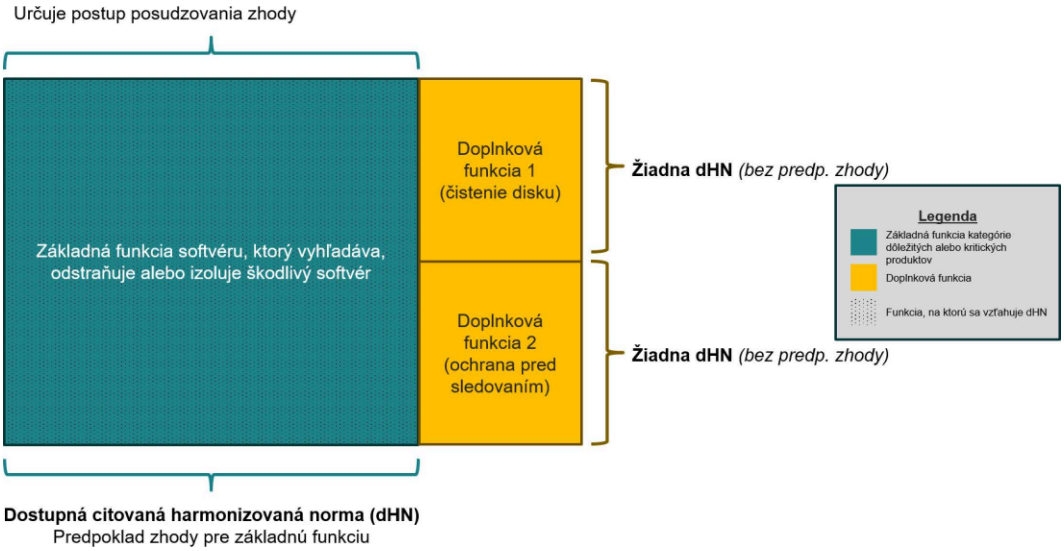
Príklad 64: Antivírusový softvér má základnú funkciu softvéru, ktorý vyhľadáva, odstraňuje alebo umiestňuje škodlivý softvér do karantény, pričom riziká spojené s touto základnou funkciou sú pokryté harmonizovanou normou. Tento produkt s digitálnymi prvkami zahŕňa aj ďalšie funkcie, konkrétne funkciu čistenia disku a funkciu ochrany pred sledovaním, ktorá chráni používateľa pri prehliadaní webu a ktorej riziká nie sú pokryté harmonizovanou normou. Ak sa uplatňuje harmonizovaná norma, výrobca môže na posúdenie zhody využiť postup vnútornej kontroly. Bude sa naň vzťahovať predpoklad zhody, pokiaľ ide o riziká spojené so základnou funkciou daného produktu, nie však pokiaľ ide o riziká spojené s ďalšími funkciami.

([26]) Ako je jasne uvedené v oddiele 4.1.2.2 Modrej príručky, „[v] harmonizačných právnych predpisoch týkajúcich sa rizík [...] výrobcovia vždy, a to aj pri použití harmonizovaných noriem, na ktoré je v *Úradnom vestníku Európskej únie* uverejnený odkaz, naďalej nesú plnú zodpovednosť za posúdenie všetkých rizík svojho výrobku s cieľom určiť, ktoré základné (alebo iné) požiadavky sú relevantné. Po tomto posúdení sa výrobca môže následne rozhodnúť, či uplatní technické špecifikácie uvedené v harmonizovaných normách, na ktoré je v *Úradnom vestníku Európskej únie* uverejnený odkaz, aby vykonal ‚opatrenia na zníženie rizika', ktoré sú uvedené v harmonizovaných normách".

([27]) Ako už bolo uvedené, vo zvyšnej časti tohto oddielu sa z dôvodu stručnosti odkazuje len na harmonizované normy, na ktoré boli uverejnené odkazy v *Úradnom vestníku Európskej únie*. Rovnaké usmernenia sa však vzťahujú aj na spoločné špecifikácie a na európske schémy certifikácie kybernetickej bezpečnosti.

Obrázok 7

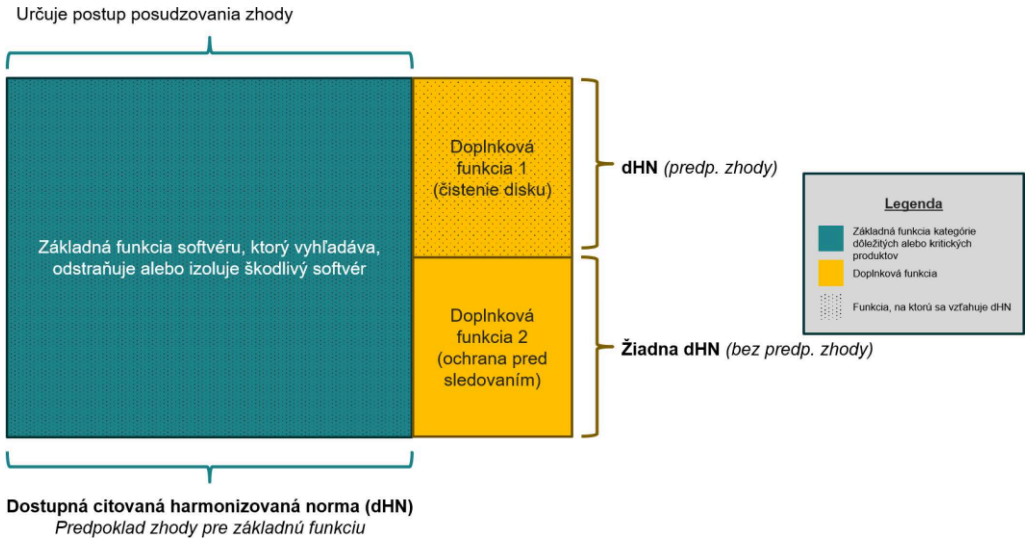
Harmonizovaná norma poskytuje predpoklad zhody pre základnú funkciu, keďže sa v nej riešia všetky riziká spojené s touto základnou funkciou, nie však pre vedľajšie funkcie



Príklad 65: V rovnakom scenári ako v predchádzajúcom príklade bola harmonizovaná norma odteraz aktualizovaná tak, aby pokrývala aj riziká spojené s jednou z ďalších funkcií, konkrétne s funkciou čistenia disku, nie však s druhou funkciou (t. j. s funkciou ochrany pred sledovaním). Ak sa uplatňuje harmonizovaná norma, výrobca môže na posúdenie zhody využiť postup vnútornej kontroly. Využije predpoklad zhody, pokiaľ ide o riziká spojené so základnou funkciou daného produktu a funkciou čistenia disku, nie však pokiaľ ide o riziká súvisiace s funkciou ochrany pred sledovaním.

Obrázok 8

Harmonizovaná norma poskytuje predpoklad zhody pre základnú funkciu a vedľajšiu funkciu 1, keďže sa v nej riešia všetky riziká spojené s týmito dvoma funkciami, nie však pre vedľajšiu funkciu 2



7. **POSÚDENIE KYBERNETICKOBEZPEČNOSTNÝCH RIZÍK A INTEGRÁCIA PRODUKTOV S DIGITÁLNYMI PRVKAMI A KOMPONENTOV**

7.1. **O hodnotení a riešení kybernetickobezpečnostných rizík**

156. Pri posúdení kybernetickobezpečnostných rizík stanovenom v článku 13 ods. 2 aktu o kybernetickej odolnosti sa vyžaduje, aby výrobcovia identifikovali príslušné riziká a posúdili ich možný vplyv na produkt s digitálnymi prvkami. Výrobcovia musia takisto zaviesť primerané opatrenia na riešenie týchto rizík v súlade so základnými požiadavkami uvedenými v prílohe I.

157. V rámci riadenia rizík v organizácii sa riziká bežne hodnotia na základe kritérií prijateľnosti vychádzajúcich z interných cieľov organizácie alebo jej ochoty podstupovať riziká. Naproti tomu by sa podľa aktu o kybernetickej odolnosti malo zvyškové kybernetickobezpečnostné riziko posudzovať s prihliadnutím na požiadavku, aby produkt s digitálnymi prvkami uvádzaný na trh zabezpečoval primeranú úroveň kybernetickej bezpečnosti na základe rizík, pričom sa zohľadňuje jeho zamýšľaný účel a odôvodnene predvídateľné používanie.

158. Preto pri určovaní toho, či boli riziká riešené, interná tolerancia výrobcu voči riziku, jeho obchodná stratégia ani samotné nákladové hľadiská nie sú relevantné. Na účely článku 13 ods. 2 a 3 musia byť výrobcovia schopní určiť, či boli identifikované kybernetickobezpečnostné riziká dostatočne riešené prostredníctvom vykonávania základných požiadaviek prílohy I časti I, a to s prihliadnutím na zamýšľaný účel, odôvodnene predvídateľné používanie a podmienky používania vrátane prípadného prevádzkového prostredia (napríklad zamýšľaných používateľov produktu s digitálnymi prvkami) a aktív, ktoré sa majú chrániť, pričom sa zohľadňuje trvanie obdobia, počas ktorého sa predpokladá používanie produktu s digitálnymi prvkami.

159. Prirodzeným výsledkom posúdenia a riešenia rizík je zvyškové kybernetickobezpečnostné riziko. Je všeobecne známe, že kybernetickobezpečnostné riziká nemožno v praxi úplne odstrániť. Existencia zvyškového rizika však neznamená, že výrobca môže podľa vlastného uváženia akceptovať akékoľvek riziko. Produkt s digitálnymi prvkami možno uviesť na trh len vtedy, keď boli zvyškové riziká po prijatí primeraných opatrení dostatočne riešené prostredníctvom vykonávania základných požiadaviek, pričom sa zohľadňuje zamýšľaný účel a odôvodnene predvídateľné používanie produktu s digitálnymi prvkami.

160. V súlade s článkom 13 ods. 3 sú výrobcovia povinní v prípade identifikácie kybernetickobezpečnostných rizík riešiť tieto riziká prostredníctvom primeraných opatrení, a to aj na úrovni produktu. V závislosti od okolností to môže zahŕňať napríklad zmenšenie plochy útoku, zavedenie technických ochranných opatrení, obmedzenie alebo prispôsobenie funkcie alebo presnejšie vymedzenie zamýšľaného účelu produktu s digitálnymi prvkami. Výrobcovia môžu takisto prijať opatrenia na formovanie odôvodnene predvídateľného používania produktu s digitálnymi prvkami, napríklad prostredníctvom komunikácie o rizikách, usmernení pre používateľov alebo navrhovania používateľského rozhrania s cieľom usmerňovať správanie používateľov smerom k bezpečným spôsobom používania.

161. Akt o kybernetickej odolnosti neumožňuje preniesť kybernetickobezpečnostné riziko ani zodpovednosť na používateľov alebo tretie strany s cieľom kompenzovať nedostatky v návrhu produktu alebo odôvodniť ponechanie kybernetickobezpečnostných rizík bez riešenia. Povinnosť uvádzať na trh bezpečný produkt s digitálnymi prvkami a preukázať jeho zhodu so základnými požiadavkami naďalej spočíva na výrobcovi.

162. Informácie a návody 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, ako aj na informovanie používateľov o zvyškových rizikách spôsobom, ktorý zodpovedá 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 funkciu, 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, v ktorých je zabránené neoprávnenému fyzickému prístupu k produktu s digitálnymi prvkami. Informácie a návod pre používateľov poskytujú jasné informácie o týchto obmedzeniach používania senzora spôsobom, ktorý zodpovedá povahe produktu s digitálnymi prvkami a jeho zamýšľaným používateľom.

Príklad 67: Výrobca vyvinie softvérovú aplikáciu určenú na profesionálne použitie na spravovaných stolových a mobilných zariadeniach. Aplikácia spracúva citlivé údaje uložené lokálne a obsah vytvorený používateľmi. Počas posúdenia rizík výrobca identifikuje riziko neoprávneného prístupu k takýmto údajom, ak sú uložené v zariadení v nezašifrovanej podobe. Namiesto navrhnutia a zavedenia vlastného šifrovacieho mechanizmu priamo v rámci samotnej aplikácie sa výrobca rozhodne spoliehať na funkcie šifrovania a správy kľúčov, ktoré natívne poskytuje operačný systém, na ktorom sa aplikácia má prevádzkovať, keďže vstavané kryptografické služby operačného systému sú vyspelé a pravidelne udržiavané.

163. Ak sa pri posúdení kybernetickobezpečnostných rizík identifikujú riziká, ktoré nemožno primerane riešiť vhodnými opatreniami, splnenie požiadaviek aktu o kybernetickej odolnosti si môže vyžadovať zmeny návrhu, funkcie alebo zamýšľaného účelu produktu s digitálnymi prvkami. Hľadiská týkajúce sa výlučne nákladov alebo obchodnej uskutočniteľnosti nepredstavujú dostatočné dôvody na ponechanie takýchto rizík bez riešenia, 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 na základe rizík zabezpečovali primeranú úroveň kybernetickej bezpečnosti

164. V základnej požiadavke kybernetickej bezpečnosti uvedenej časti I bode 1 prílohy I k aktu o kybernetickej odolnosti sa stanovuje, že produkty s digitálnymi prvkami sa navrhujú, vyvíjajú a vyrábajú takým spôsobom, aby sa zaistila primeraná úroveň ich kybernetickej bezpečnosti voči rizikám.

165. Táto základná požiadavka je zameraná na riešenie všetkých kybernetickobezpečnostných rizík, ktoré boli identifikované v rámci posúdenia kybernetickobezpečnostných rizík. Ide najmä o kybernetickobezpečnostné riziká, ktoré nie sú inak primerane riešené v rámci vykonávania základných požiadaviek uvedených v prílohe I časti I okrem bodu 1. Táto základná požiadavka sa líši od právnej povinnosti vykonať posúdenie kybernetickobezpečnostných rizík, ktoré sa vykonáva podľa článku 13 ods. 2.

166. Ak sa všetky relevantné kybernetickobezpečnostné riziká súvisiace s produktom s digitálnymi prvkami riešia zavedením primeraných opatrení na splnenie uplatniteľných základných požiadaviek okrem bodu 1, základná požiadavka uvedená v prílohe I časti I bode 1 sa považuje za splnenú. Naopak, ak sa pri posúdení kybernetickobezpečnostných rizík identifikujú dodatočné riziká, ktoré sa takýmito opatreniami v plnom rozsahu neriešia, výrobcovia sú povinní zaviesť primerané opatrenia týkajúce sa produktu s digitálnymi prvkami na riešenie týchto rizík, aby splnili základnú požiadavku uvedenú v prílohe I časti I bode 1. V praxi sa vo väčšine prípadov predpokladá, že splnenie ostatných základných požiadaviek povedie k splneniu tejto požiadavky.

7.3. Posúdenie rizík a náležitá starostlivosť v súvislosti s externými závislosťami a integrovanými komponentmi

167. V akte o kybernetickej odolnosti sa pre výrobcov stanovujú dve samostatné, ale vzájomne sa dopĺňajúce povinnosti v súvislosti s riadením kybernetickobezpečnostných rizík. Po prvé, článkom 13 ods. 2 sa výrobcom ukladá povinnosť vykonať posúdenie kybernetickobezpečnostných rizík samotného produktu s digitálnymi prvkami. Po druhé, článkom 13 ods. 5 sa ukladá povinnosť postupovať s náležitou starostlivosťou, pokiaľ ide o integrované komponenty. Tieto dve povinnosti sú spoločne koncipované 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 pochádzajúcich z prostredia mimo samotného produktu, ako sú externé siete, environmentálne faktory alebo iné vonkajšie aspekty, ktoré môžu ovplyvniť produkt s digitálnymi prvkami alebo od ktorých je tento produkt závislý. V prípade takýchto externých rizík sa v akte o kybernetickej odolnosti nevyžaduje, aby výrobcovia kontrolovali alebo riadili externé prostredie. Výrobcovia sú skôr povinní takéto riziká identifikovať a zmierňovať ich už v rámci samotného návrhu a vývoja produktu s digitálnymi prvkami. Bude to zahŕňať vykonávanie príslušných základných požiadaviek stanovených v prílohe I časti I a v prípade potreby poskytovanie informácií a návodov používateľom o rizikách spojených s integráciou alebo nasadením.

169. Výrobca môže napríklad identifikovať riziko, že neoprávnené osoby môžu počas prevádzky produktu získať prístup k back-endovým systémom, ktoré nie sú súčasťou samotného produktu s digitálnymi prvkami, a pokúsiť sa zasielať produktu s digitálnymi prvkami škodlivé príkazy. Takéto back-endové systémy, ak nie sú navrhnuté a vyvinuté výrobcom alebo na jeho zodpovednosť alebo ak nepodporujú niektorú z funkcií produktu s digitálnymi prvkami, nepredstavujú riešenia spracovania údajov na diaľku, a preto na účely aktu o kybernetickej odolnosti nepatria do vymedzenia produktu s digitálnymi prvkami. V akte o kybernetickej odolnosti sa však napriek tomu vyžaduje, aby výrobca riešil riziko, ktoré môžu takéto systémy predstavovať, prostredníctvom opatrení na úrovni produktu, napríklad vyžadovaním kryptografického overovania príkazov na diaľku, overovaním integrity zmien konfigurácie alebo generovaním bezpečnostne relevantných záznamov alebo výstrah pri zistení neobvyklého správania. Podobne, ak výrobca identifikuje riziko vyplývajúce z nedostupnosti takejto externej služby, napríklad v dôsledku výpadkov elektrickej energie alebo zlyhaní infraštruktúry, v akte o kybernetickej odolnosti sa môže vyžadovať prijatie zmierňujúcich opatrení na úrovni produktu proti takýmto kybernetickobezpečnostným rizikám, napríklad zabezpečenie toho, aby výpadok nespôsobil prechod produktu s digitálnymi prvkami do nezabezpečených stavov. V takýchto prípadoch sa v akte o kybernetickej odolnosti upravuje spôsob, akým produkt s digitálnymi prvkami reaguje na tieto externé riziká; neukladá žiadne povinnosti týkajúce sa organizácie, personálneho obsadenia ani prevádzky back-endovej infraštruktúry, ani túto infraštruktúru nepovažuje za súčasť produktu s digitálnymi prvkami.

170. Náležitá starostlivosť sa vzťahuje na prvky, ktoré tvoria súčasť samotného produktu s digitálnymi prvkami, najmä na integrované softvérové alebo hardvérové komponenty dodávané treťou stranou. Výrobcovia sú povinní prijať primerané opatrenia, aby zabezpečili, že takéto komponenty neohrozia súlad produktu s digitálnymi prvkami so základnými požiadavkami. To možno dosiahnuť len určením toho, čo produkt s digitálnymi prvkami vyžaduje od svojich komponentov, aby dosiahol svoje ciele v oblasti kybernetickej bezpečnosti, a overením na základe rizík, že tieto komponenty sú v súlade s potrebami produktu, ako sa uvádza aj v odôvodnení 34.

171. V súlade so svojím posúdením kybernetickobezpečnostných rizík musí výrobca identifikovať požiadavky, ktoré by mal integrovaný komponent spĺňať. Napríklad ak sa produkt s digitálnymi prvkami spolieha na kryptografické funkcie, mechanizmy aktualizácie alebo bezpečnú komunikáciu poskytované komponentom, výrobca musí v rámci náležitej starostlivosti tieto potreby identifikovať a overiť, že komponent ich 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 kvality. V prípade potreby môže výrobca vykonať aj skúšky s cieľom overiť, či tieto komponenty primerane plnia príslušné funkcie. Hoci náležitá starostlivosť predstavuje samostatnú právnu 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 kybernetickobezpečnostných rizík zohľadniť prvky mimo produktu, ako sú environmentálne prvky, externá infraštruktúra, iné systémy alebo siete, a ak je to relevantné, musia sa riešiť prostredníctvom opatrení na úrovni produktu s cieľom zabezpečiť, aby produkt s digitálnymi prvkami spĺňal základné požiadavky. Pri posudzovaní rizík je potrebné zohľadniť aj komponenty, ktoré sú fyzicky alebo logicky integrované do produktu s digitálnymi prvkami, ale pochádzajú od tretej strany. Z hľadiska dodržiavania predpisov by však výrobca mal tieto komponenty považovať za komponenty dodávané z vonkajších zdrojov, ktorých vlastnosti sa overujú prostredníctvom náležitej starostlivosti pri ich integrácii, keďže ich pravdepodobne neprepracoval ani nevyvinul nanovo.

173. Tá istá logika platí aj pri vývoji a integrácii komponentov. Ak výrobca vyvíja funkcie sám, musí priamo implementovať základné požiadavky. Ak výrobca do svojho produktu začleňuje komponenty vyvinuté inými subjektmi, musí prostredníctvom náležitej starostlivosti zabezpečiť, aby bolo možné tieto komponenty používať spôsobom, ktorý umožní, aby produkt s digitálnymi prvkami ako celok spĺňal príslušné požiadavky. V oboch prípadoch zostáva cieľ rovnaký: zabezpečiť, aby produkt s digitálnymi prvkami v podobe, v akej je uvádzaný na trh, dosahoval primeranú úroveň kybernetickej bezpečnosti požadovanú aktom o kybernetickej odolnosti, pričom sa zohľadňujú riziká identifikované v posúdení kybernetickobezpečnostných rizík.

7.4. **Opätovné použitie posúdení 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 rovnakú architektúru, návrh relevantný z hľadiska bezpečnosti a zamýšľaný účel a sú vystavené rovnakým kybernetickobezpečnostným rizikám, v akte o kybernetickej odolnosti sa nevyžaduje, aby výrobcovia na účely posúdenia rizík a posudzovania zhody považovali každý variant za úplne samostatný produkt s digitálnymi prvkami.

175. V takýchto prípadoch môžu výrobcovia, pokiaľ sú všetky príslušné varianty primerane pokryté z hľadiska relevantných rizík a základných požiadaviek, vychádzať z: i) jedného posúdenia kybernetickobezpečnostných rizík vykonaného v súlade s článkom 13 ods. 2 aktu o kybernetickej odolnosti; ii) jedného súboru technickej dokumentácie a iii) jedného postupu posudzovania zhody. To zároveň umožňuje vydať jedno EÚ vyhlásenie o zhode pre skupinu produktov s digitálnymi prvkami, pokiaľ sa v ňom jasne identifikujú varianty produktov, na ktoré sa vzťahuje.

176. Rozhodujúcim faktorom je to, či sú rozdiely medzi jednotlivými variantmi relevantné z hľadiska kybernetickej bezpečnosti. Varianty, ktoré nemajú vplyv na vlastnosti produktu s digitálnymi prvkami z hľadiska kybernetickej bezpečnosti, ako sú rozdiely vo farbe, vyhotovení, veľkosti pamäte alebo iných vlastnostiach, ktoré nie sú relevantné z hľadiska bezpečnosti, si nevyžadujú samostatné posúdenia rizík ani posudzovania zhody. Naopak, v niektorých prípadoch sa varianty môžu líšiť spôsobmi, ktoré ovplyvňujú splnenie základných požiadaviek, napríklad prostredníctvom rôznych komunikačných rozhraní, softvérových balíkov, mechanizmov aktualizácie alebo vzdialeného pripojenia. V takýchto prípadoch sa tieto rozdiely musia zohľadniť v posúdení rizík a v prípade potreby aj v posúdení zhody a v technickej dokumentácii.

177. Výrobcovia naďalej nesú zodpovednosť za to, aby sa v posúdení rizík a súvisiacej dokumentácii presne zohľadňovali produkty s digitálnymi prvkami uvádzané na trh. Ak nový variant prináša nové kybernetickobezpečnostné riziká alebo mení spôsob vykonávania základných požiadaviek, existujúce posúdenie rizík a dokumentácia o zhode sa musia zodpovedajúcim spôsobom aktualizovať. Možnosť vychádzať z jedného posúdenia zhody existuje len v rozsahu, v akom sa produkty s digitálnymi prvkami nelíšia, pokiaľ ide o ich vlastnosti z hľadiska kybernetickej bezpečnosti.

8. **SPRACOVANIE ÚDAJOV NA DIAĽKU**

178. V článku 3 bode 1 aktu o kybernetickej odolnosti sa vymedzuje 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 vnímať produkt s digitálnymi prvkami ako celok vrátane riešení spracovania údajov na diaľku. Napríklad pri preukazovaní toho, že produkt s digitálnymi prvkami spĺňa základné požiadavky stanovené v prílohe I, sa musia zohľadniť riešenia spracovania údajov na diaľku, počnúc posúdením rizík (článok 13 ods. 2). To isté platí aj pri zohľadňovaní povinností počas životného cyklu, ako je oznamovanie aktívne zneužívaných zraniteľností a závažných incidentov (článok 14).

179. Účelom týchto usmernení je poskytnúť výrobcom ďalšiu podporu pri určovaní toho, či ich produkt s digitálnymi prvkami obsahuje riešenie spracovania údajov na diaľku v zmysle vymedzenia v akte o kybernetickej odolnosti, a pri plnení ich povinností v oblasti zhody v tejto súvislosti. Po úvodnej analýze vymedzenia pojmov a odôvodnení stanovených v akte o kybernetickej odolnosti sa v týchto usmerneniach uvedú otázky, ktoré majú výrobcom pomôcť pri objasňovaní toho, či ich produkt s digitálnymi prvkami zahŕňa riešenia spracovania údajov na diaľku (pozri oddiel *8.1. Čo sa považuje za riešenie spracovania údajov na diaľku pre produkt s digitálnymi prvkami?*). Následne sa budú podrobnejšie rozoberať technické dôsledky riešení spracovania údajov na diaľku a spôsob posudzovania zhody s aktom o kybernetickej odolnosti (pozri oddiel *8.2. Praktické a technické dôsledky riešení spracovania údajov na diaľku a využívania riešení tretích strán*).

180. V článku 3 bode 2 sa pojem „spracovanie údajov na diaľku“ vymedzuje ako „spracovanie údajov na diaľku, pre ktoré je softvér navrhnutý a vyvinutý výrobcom alebo na zodpovednosť výrobcu a ktorého neexistencia by bránila produktu s digitálnymi prvkami plniť jednu z jeho funkcií“. Riešenia spracovania údajov na diaľku sú preto vymedzené ako softvérové prvky („časť elektronického informačného systému, ktorý pozostáva z počítačového kódu“, ako sa vymedzuje v článku 3 bode 4) spracovania údajov na diaľku. Ako súčasť rozsahu produktu s digitálnymi prvkami nemajú zahŕňať hardvér, od ktorého môže byť spracovanie údajov na diaľku závislé.

181. V odôvodneniach 11 a 12 sa uvádzajú ďalšie vysvetlenia týkajúce sa toho, ako by sa mal tento pojem vykladať. V odôvodnení 11 sa 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 výrobcom“. Zároveň sa v ňom uvádza, 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 výrobcu ako celku“.

182. Z odôvodnenia 11 teda vyplýva, že zámerom nie je, aby požiadavky aktu o kybernetickej odolnosti pokrývali celú IT infraštruktúru organizácie, ale len softvérové komponenty, ktoré umožňujú vykonávanie riešenia spracovania údajov na diaľku. Napríklad interné systémy týkajúce sa vlastných ľudských zdrojov výrobcu, mzdovej agendy, riadenia vzťahov so zákazníkmi, kanálov kontinuálnej integrácie/kontinuálneho dodávania (CI/CD) alebo distribúcie aktualizácií bezpečnosti do okrajových lokalít by sa nemali považovať za riešenia spracovania údajov na diaľku. Podobne do rozsahu produktu s digitálnymi prvkami, na ktorý sa vzťahuje akt o kybernetickej odolnosti, nepatria systémy súvisiace s audítorskými a testovacími činnosťami, ako sú penetračné testovanie, vyhľadávanie hrozieb a red teaming. Je dôležité poznamenať, že hoci je vykonávanie účinných a pravidelných skúšok a preskúmaní bezpečnosti produktu s digitálnymi prvkami základnou požiadavkou stanovenou v časti II bode 3 prílohy I k aktu o kybernetickej odolnosti, neznamená to, že sa takéto činnosti majú považovať za riešenia spracovania údajov na diaľku daného produktu s digitálnymi prvkami.

183. Odôvodnenie 12 je zamerané na cloudové služby a podrobnejšie sa v ňom rozoberajú okolnosti, za ktorých by sa cloudové služby mohli považovať za riešenia spracovania údajov na diaľku. Na záver sa v odôvodnení pripomína, že služby cloud computingu a modely cloudových služieb patria do rozsahu pôsobnosti smernice (EÚ) 2022/2555 (NIS 2) ([28]), v ktorej sa stanovujú požiadavky na riadenie kybernetickobezpečnostných rizík pre poskytovateľov služieb cloud computingu. Tieto požiadavky sú podrobnejšie upravené vo vykonávacom nariadení Komisie (EÚ) 2024/2690 ([29]).

8.1. **Čo sa považuje za riešenie spracovania údajov na diaľku pre produkt s digitálnymi prvkami?**

184. Pri vymedzení pojmu „spracovanie údajov na diaľku“ stanovenom v článku 3 bode 2 sa teda vychádza z troch prvkov: i) či sa spracovanie údajov vykonáva „na diaľku“; ii) či by neexistencia takéhoto spracovania údajov bránila produktu s digitálnymi prvkami plniť jednu z jeho funkcií a iii) či je softvér navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť. V nasledujúcich troch pododdieloch sa každý z týchto prvkov rozoberá podrobnejšie.

([28]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a 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).

([29]) Vykonávacie nariadenie Komisie (EÚ) 2024/2690 zo 17. októbra 2024, ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík a o bližšie určenie prípadov, v ktorých sa incident považuje za významný, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľom dôveryhodných služieb (Ú. v. EÚ L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Pojem „na diaľku“*

185. Pojem „na diaľku“ uvedený v článku 3 bode 2 je relevantný, ale sám osebe nestačí na určenie toho, či produkt s digitálnymi prvkami zahŕňa riešenia spracovania údajov na diaľku. Okrem toho vzhľadom na rozmanitosť riešení, ktoré by mohli patriť pod tento pojem, nie je možné poskytnúť vyčerpávajúce vymedzenie pojmu „na diaľku“. Je potrebné, aby výrobca posúdil každý prípad individuálne.

186. V odôvodnení 11 aktu o kybernetickej odolnosti sa uvádzajú údaje spracúvané alebo uchovávané „na diaľku výrobcom“ na rozdiel od údajov spracúvaných alebo uchovávaných „lokálne na zariadení používateľa“. Spracovanie údajov na diaľku sa zvyčajne uskutočňuje mimo prostredia používateľa produktu s digitálnymi prvkami alebo prevádzkového prostredia organizácie (v prípade profesionálneho používateľa). To však nebráni tomu, aby sa údaje spracúvali aj v blízkosti zariadenia („na okraji“). Prenos údajov môže prebiehať prostredníctvom kábla (napr. ethernetového kábla) alebo bezdrôtovo (napr. cez Wi-Fi alebo Bluetooth). Typickým príkladom spracovania údajov, ktoré sa uskutočňuje „na diaľku“, je cloud computing vrátane edge computingu. Napríklad v prípade funkcie založenej na cloude, ku ktorej má používateľ prístup prostredníctvom mobilnej aplikácie, sa časť spracovania údajov uskutočňuje v cloude, mimo prostredia používateľa.

187. Je dôležité poznamenať, že riešenia spracovania údajov na diaľku nemusia byť nevyhnutne prevádzkované na cloudovej infraštruktúre tretej strany. Riešenia spracovania údajov na diaľku môže takisto predstavovať spracovanie údajov na diaľku vykonávané na lokálnych serveroch v priestoroch výrobcu. Inými slovami, riešenie prevádzkované v priestoroch organizácie a v súkromnom cloude môže spĺňať podmienky spracovania údajov na diaľku rovnako ako riešenie prevádzkované vo verejnom cloude a mimo priestorov organizácie.

188. Dve rozhodujúce a kumulatívne otázky, ktoré určujú, či sa na spracovanie údajov vzťahuje akt o kybernetickej odolnosti ako na riešenie spracovania údajov na diaľku, sú uvedené ďalej v oddieloch *8.1.2* a *8.2*. Ak sú odpovede na obe otázky kladné, spracovanie údajov na diaľku spĺňa podmienky na to, aby sa považovalo za riešenie spracovania údajov na diaľku.

8.1.2. *Bránila by neexistencia takéhoto spracovania údajov produktu s digitálnymi prvkami plniť jednu z jeho funkcií?*

189. Ako sa stanovuje vo vymedzení pojmu „spracovanie údajov na diaľku“ uvedenom v článku 3 bode 2, aby spracovanie údajov na diaľku bolo možné považovať za riešenie spracovania údajov na diaľku, jeho neexistencia by musela brániť produktu s digitálnymi prvkami plniť jednu z jeho funkcií. Pojem „funkcie“ použitý v tomto vymedzení nie je obmedzený na „základnú funkciu“ ani „zamýšľaný účel“ produktu s digitálnymi prvkami, keďže v akte o kybernetickej odolnosti sa takéto obmedzenie nestanovuje. Funkciami, ktoré patria do rozsahu aktu o kybernetickej odolnosti, sú jednak funkcie, ktoré priamo plnia zamýšľaný účel produktu s digitálnymi prvkami tak, ako ho vnímajú používatelia, ako aj funkcie, ktoré podporujú celkovú výkonnosť produktu.

190. Medzi 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, patria: i) odosielanie príkazov do zariadenia; ii) synchronizácia súborov; iii) registrácia používateľa; iv) konfigurácia (personalizácia produktu s digitálnymi prvkami); v) automatizovaná distribúcia aktualizácií vrátane aktualizácií funkcií a bezpečnostných záplat; vi) riadenie identity a prístupu.

191. V niektorých prípadoch môže používateľ určitú funkciu využívať na diaľku aj manuálne (napríklad zapnúť žiarovku prostredníctvom aplikácie alebo manuálne). Táto možnosť nevylučuje, aby sa spracovanie údajov spojené s vykonávaním tejto funkcie na diaľku klasifikovalo ako riešenie spracovania údajov na diaľku. Vykonávanie tejto funkcie na diaľku sa takisto považuje za súčasť funkcií, ktoré produkt s digitálnymi prvkami ponúka.

192. Naopak, ak neexistencia určitého spracovania údajov nebráni produktu s digitálnymi prvkami plniť jednu z jeho funkcií, takéto spracovanie sa nepovažuje za riešenie spracovania údajov na diaľku v zmysle aktu o kybernetickej odolnosti. Patrí sem napríklad diaľková analýza telemetrických údajov, ktoré sa zhromažďujú výlučne na štatistické účely alebo na účely budúceho vývoja produktov.

193. Dokonca aj vtedy, keď spracovanie údajov nepodporuje žiadnu funkciu produktu s digitálnymi prvkami, výrobcovia možno budú v rámci svojho posúdenia kybernetickobezpečnostných rizík musieť zvážiť, či tieto vzdialené komponenty nepredstavujú riziká pre produkt s digitálnymi prvkami (napríklad s ohľadom na prevádzkové prostredie produktu), a takéto riziká primerane zmierniť (napríklad prostredníctvom opatrení na úrovni produktu).

194. Špecifický prípad, ktorý si zaslúži bližšie vysvetlenie, predstavujú webové sídla, ako je uvedené aj v *oddiele 2.1. Uvedenie na trh*. Podľa vysvetlenia v odôvodnení 11 aktu o kybernetickej odolnosti webové sídla nepatria do rozsahu riešení spracovania údajov na diaľku, ak nepodporujú žiadnu funkciu produktu s digitálnymi prvkami. Na to, aby sa webové sídlo považovalo za súčasť rozsahu riešení spracovania údajov na diaľku, nestačí, že obsahuje informácie o produkte s digitálnymi prvkami, a to ani v prípade, ak produkt presmeruje používateľa na takéto webové sídlo. Napríklad presmerovanie používateľov na externú webovú stránku, ktorá poskytuje používateľom informácie a návod, nepredstavuje riešenie spracovania údajov na diaľku. Naopak, webové sídlo môže patriť do rozsahu riešení spracovania údajov na diaľku vtedy, keď umožňuje alebo podporuje funkciu produktu s digitálnymi prvkami. Za riešenie spracovania údajov na diaľku by sa napríklad považoval autentifikačný portál, ktorý vydáva poverenia alebo tokeny potrebné na fungovanie produktu s digitálnymi prvkami (za predpokladu, že sú splnené aj ostatné kritériá vymedzenia).

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

195. Vo vymedzení pojmu „spracovanie údajov na diaľku“ v článku 3 bode 2 aktu o kybernetickej odolnosti sa ďalej stanovuje, že softvér takéhoto spracovania údajov na diaľku musí byť navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť. Spracovanie údajov na diaľku, ktoré výrobca navrhol a vyvinul v plnom rozsahu sám (vnútropodnikovo), by sa prirodzene považovalo za riešenie spracovania údajov na diaľku. 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 „na zodpovednosť výrobcu“ sa vzťahuje na riešenia spracovania údajov na diaľku, ktoré sú vytvorené na mieru pre výrobcu. Ide o prípady, keď výrobca neposkytuje iba licenciu na existujúci produkt s digitálnymi prvkami alebo službu, ktorú poskytovateľ služieb ponúka svojim zákazníkom, alebo na ich mierne upravené verzie. „[N]a zodpovednosť výrobcu“ znamená, že softvér je vyvinutý výlučne výrobcom alebo v jeho mene na základe návrhov a špecifikácií, ktoré poskytol.

196. Pri posudzovaní riešení spracovania údajov na diaľku nie je rozhodujúcim faktorom to, „kto riešenie prevádzkuje“, keďže vo vymedzení v akte o kybernetickej odolnosti sa odkazuje len na návrh a vývoj riešenia spracovania údajov na diaľku. Je to v súlade s prístupom aktu o kybernetickej odolnosti, 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 zodpovedajú za súlad produktu s digitálnymi prvkami, ktorý uvádzajú na trh, so základnými požiadavkami aktu o kybernetickej odolnosti.

197. Je potrebné rozlišovať medzi prípadmi, keď návrh a vývoj zabezpečujú výrobcovia (alebo sa vykonávajú na ich zodpovednosť), a prípadmi, keď sa využívajú riešenia tretích strán, ktoré neboli navrhnuté ani vyvinuté výrobcami (alebo na ich zodpovednosť). Ako príklad je užitočné zvážiť najbežnejšie modely cloudových služieb, ktoré poskytujú rôznu mieru kontroly používateľovi a ktoré sa uvádzajú aj v odôvodnení 12 aktu o kybernetickej odolnosti, konkrétne softvér ako služba (SaaS), platforma ako služba (PaaS) a infraštruktúra ako služba (IaaS).

198. V prípade riešenia IaaS poskytovaného treťou stranou výrobca nespravuje ani nekontroluje základné fyzické a virtuálne zdroje (ako sú základný hardvér a hypervízor poskytovateľa cloudových služieb), ale môže prostredníctvom týchto zdrojov nasadzovať a prevádzkovať ľubovoľný softvér, napríklad operačné systémy a aplikácie. Takýto softvér je navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť, a preto sa môže považovať za riešenie spracovania údajov na diaľku (ak spĺňa aj ostatné prvky vymedzenia).

199. V prípade riešenia PaaS poskytovaného treťou stranou výrobca nasadzuje vlastnú aplikáciu (vytvorenú alebo získanú) s využitím programovacích jazykov a prostredí na vykonávanie poskytovaných poskytovateľom cloudových služieb a integruje túto aplikáciu do svojho produktu s digitálnymi prvkami. Výrobca má kontrolu nad aplikáciou a prípadne aj nad nastaveniami konfigurácie prostredia na spúšťanie. Aplikácia je teda navrhnutá a vyvinutá výrobcom alebo na jeho zodpovednosť, a preto sa môže považovať za riešenie spracovania údajov na diaľku (ak spĺňa aj ostatné prvky vymedzenia).

200. V prípade riešenia SaaS poskytovaného treťou stranou poskytovateľ SaaS ponúka výrobcovi plne vyvinutú aplikáciu, ktorá sa má integrovať do produktu s digitálnymi prvkami výrobcu. Výrobca má obmedzené možnosti pri spravovaní nastavení konfigurácie aplikácií špecifických pre jednotlivých používateľov. Aplikácia teda nebola navrhnutá ani vyvinutá výrobcom, ani na jeho zodpovednosť.

201. Napriek tomu, ak určité prvky nespĺňajú podmienky na to, aby sa považovali za riešenia spracovania údajov na diaľku (napr. hypervízor v prípade infraštruktúry IaaS poskytovanej treťou stranou, operačný systém v prípade riešenia PaaS poskytovaného treťou stranou alebo aplikácia SaaS poskytovaná treťou stranou), ale sú integrované do produktu s digitálnymi prvkami spôsobom, ktorý ovplyvňuje jeho bezpečnosť, takéto riešenia by sa mali považovať za podobné komponentom tretích strán. Výrobca je povinný identifikovať a posúdiť riziká spojené s integráciou týchto prvkov a riešiť ich vykonávaním základných požiadaviek priamo na úrovni samotného produktu s digitálnymi prvkami. To možno v relevantných prípadoch podporiť bezpečnostnými funkciami, ktoré poskytovateľ cloudových služieb sprístupňuje v rámci svojho modelu spoločnej zodpovednosti, ak výrobca tieto funkcie využíva alebo konfiguruje na riešenie identifikovaných rizík. Okrem toho sa od výrobcu očakáva, že bude v súvislosti s bezpečnosťou týchto komponentov uplatňovať povinnosť podobnú povinnosti vykonávať náležitú starostlivosť uvedenej v článku 13 ods. 5, a to spôsobom primeraným riziku, ktoré riešenie na diaľku predstavuje pre bezpečnosť produktu s digitálnymi prvkami.

202. Na základe toho možno zhrnúť, že:

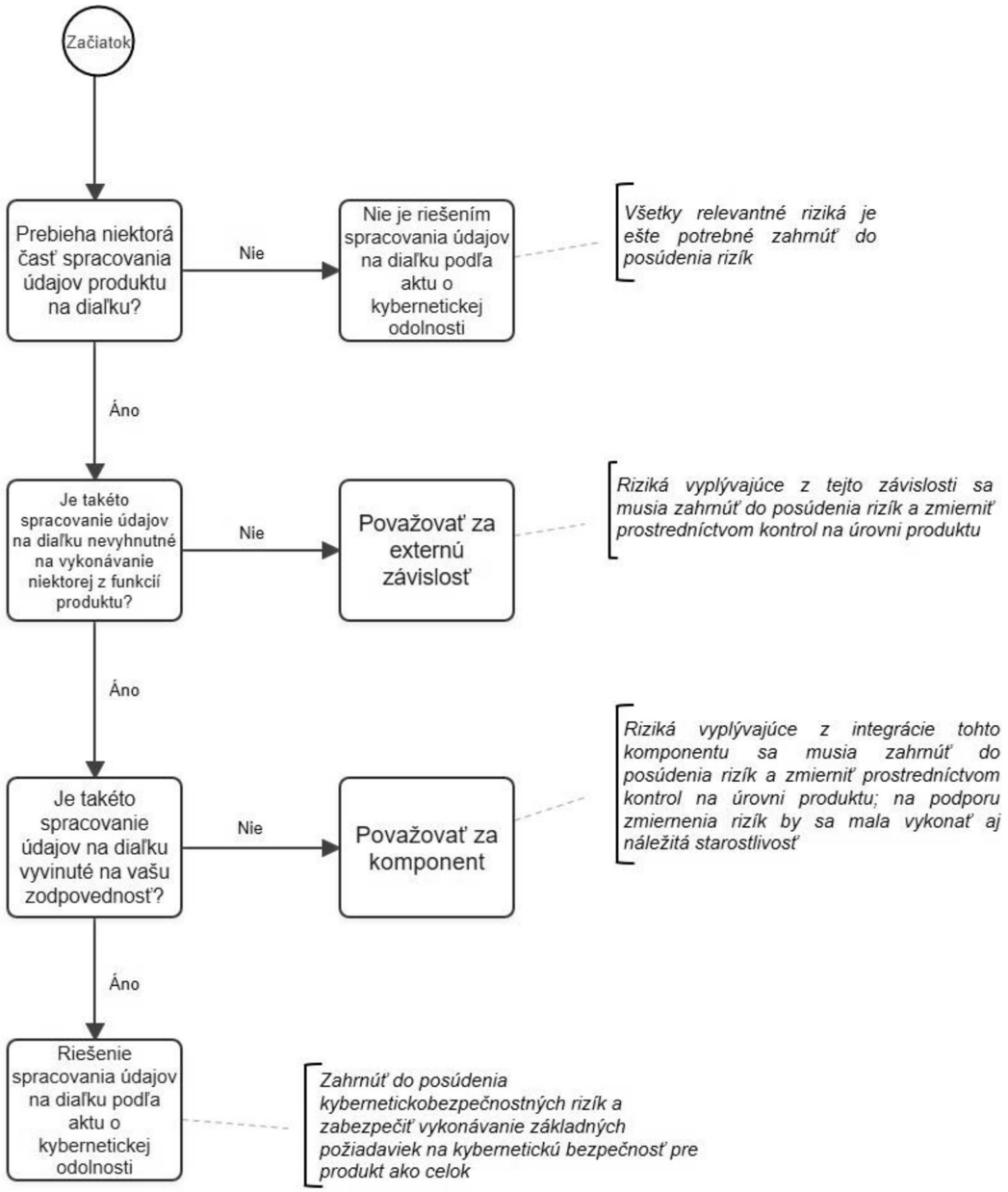
a) Aby sa spracovanie údajov mohlo považovať za riešenie spracovania údajov na diaľku, odpoveď na obe otázky uvedené v oddieloch *8.1.2. Bránila by neexistencia takéhoto spracovania údajov produktu s digitálnymi prvkami plniť jednu z jeho funkcií? a 8.1.3. Bol softvér navrhnutý a vyvinutý výrobcom alebo na jeho zodpovednosť?* musí byť kladná.

b) Ak je odpoveď na otázku uvedenú v oddiele *8.1.2. Bránila by neexistencia takéhoto spracovania údajov produktu s digitálnymi prvkami plniť 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 uvedenú v oddiele *8.1.2. Bránila by neexistencia takéhoto spracovania údajov produktu s digitálnymi prvkami plniť jednu z jeho funkcií?* kladná, ale odpoveď na otázku uvedenú v oddiele *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 vývojový diagram na určenie toho, či produkt s digitálnymi prvkami obsahuje riešenia spracovania údajov na diaľku



8.2. Praktické a technické dôsledky riešení spracovania údajov na diaľku a využívania riešení tretích strán

203. Akt o kybernetickej odolnosti vychádza z prístupu založeného na rizikách, ktorý je zakotvený v článku 13 ods. 2 a 3, ako aj v prvej základnej požiadavke prílohy I časti I, podľa ktorej „[p]rodukty 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 prístup založený na rizikách zohľadniť pri uplatňovaní požiadaviek aktu o kybernetickej odolnosti na riešenia spracovania údajov na diaľku a pri riešení rizík vyplývajúcich zo služieb tretích strán integrovaných do produktu s digitálnymi prvkami.

204. Výrobcovia by mali v prvom rade i) uviesť v technickej dokumentácii, že ich produkt s digitálnymi prvkami obsahuje riešenia spracovania údajov na diaľku alebo sa spolieha na riešenia na diaľku tretích strán a ii) opísať takéto riešenia. Ak rovnaké riešenie spracovania údajov na diaľku podporuje viacero produktov s digitálnymi prvkami, musí sa riešenie spracovania údajov na diaľku uviesť v technickej dokumentácii každého produktu. Dokumentácia týkajúca sa riešenia spracovania údajov na diaľku, ktoré slúži viacerým produktom s digitálnymi prvkami, sa môže opätovne použiť pri posudzovaní zhody jednotlivých produktov.

205. Ako sa uvádza v odôvodnení 11, riešenia spracovania údajov na diaľku, ktoré sú súčasťou produktu s digitálnymi prvkami, a preto podliehajú posudzovaniu zhody daného produktu, by sa mali obmedziť na tie softvérové moduly, ktoré sú zodpovedné za funkciu produktu s digitálnymi prvkami, a na rozhrania, ktoré tieto moduly využívajú na komunikáciu s externými službami. Ďalšie back-endové systémy, ktoré vykonávajú následné spracovanie a s ktorými produkt s digitálnymi prvkami priamo neinteraguje, sa nepovažujú za riešenia spracovania údajov na diaľku.

206. Takéto backendové systémy však naďalej predstavujú externé závislosti, ktoré sa musia posúdiť v rámci posúdenia kybernetickobezpečnostných rizík a ktorých riziká sa musia zmierniť prostredníctvom opatrení na úrovni produktu. Pri posudzovaní rizík, ktoré vykonáva výrobca, by sa v skutočnosti mali zohľadniť: i) riziká súvisiace s riešeniami spracovania údajov na diaľku; ii) riziká súvisiace so spoliehaním sa na riešenia na diaľku tretích strán (podobné komponentom tretích strán) a iii) riziká súvisiace s prostredím produktu (napr. základný hardvér). Výrobcovia by mali priamo na úrovni produktu s digitálnymi prvkami zaviesť bezpečnostné opatrenia na zmiernenie týchto rizík.

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

a) dôkaz o splnení povinností vyplývajúcich z vykonávacieho nariadenia Komisie (EÚ) 2024/2690;

b) dôkaz o splnení povinností vyplývajúcich z nariadenia (EÚ) 2022/2554 (nariadenie DORA);

c) vyhlásenie o zhode alebo certifikát získaný v rámci európskej schémy certifikácie kybernetickej bezpečnosti [prijatej podľa nariadenia (EÚ) 2019/881 – aktu o kybernetickej bezpečnosti];

d) dôkaz o súlade s normou ISO/IEC 27017:2015 alebo ISO/IEC 27001:2022.

208. Napokon, pri spolupráci s externými poskytovateľmi služieb na diaľku musia výrobcovia zaviesť najvhodnejšie bezpečnostné opatrenia na základe svojho posúdenia rizík (a v prípade potreby s podporou modelu spoločnej zodpovednosti poskytovateľa). Tieto zmierňujúce opatrenia by mali zahŕňať bezpečnostné kontroly ich produktov s digitálnymi prvkami a overovanie bezpečnostných opatrení, ktoré zabezpečujú samotní poskytovatelia, ktorí sú tretími stranami (náležitá starostlivosť). Jedným z nástrojov na zmiernenie takýchto rizík môže byť zakotvenie bezpečnostných záruk do dohôd o poskytovaní služieb uzatvorených s poskytovateľmi, ktorí sú tretími stranami, vrátane záruk, že poskytovatelia primerane riešia zraniteľnosti. Významná zmena riešení poskytovaných poskytovateľmi služieb na diaľku tretích strán by sa nemala považovať za podstatnú úpravu produktu s digitálnymi prvkami, keďže tieto prvky nie sú na zodpovednosť výrobcu. Výrobcovia sú však v rámci svojich povinností náležitej starostlivosti a s cieľom správne zmierňovať riziká vyplývajúce z využívania poskytovateľov, ktorí sú tretími stranami, nabádaní, aby zabezpečili, že ich poskytovatelia cloudových služieb, ktorí sú tretími stranami, ich budú primerane informovať o zmenách, ktoré vykonávajú vo svojich riešeniach. Na základe týchto informácií bude možno potrebné, aby výrobcovia prehodnotili svoje posúdenie rizík. V aktualizovanom posúdení rizík by sa malo zvážiť, či poskytovatelia služieb, ktorí sú tretími stranami, 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 kontrolné mechanizmy alebo zmenili poskytovateľov služieb, ktorí sú tretími stranami.

8.3. **Prípady použitia riešení spracovania údajov na diaľku**

S cieľom poskytnúť výrobcom ďalšie praktické usmernenia sa v tomto oddiele uvádza séria fiktívnych prípadov použitia, v ktorých sa opisujú typové produkty s digitálnymi prvkami využívajúce spracovanie údajov na diaľku a ilustruje sa, či sa takéto spracovanie považuje za riešenia spracovania údajov na diaľku v zmysle aktu o kybernetickej odolnosti.

8.3.1. *Mobilná banková aplikácia*

Finančný subjekt uvádza na trh mobilnú bankovú aplikáciu. Back-endové systémy aplikácie okrem iného podporujú autentifikáciu, autorizáciu, správu účtov a platby. Finančný subjekt využíva hybridnú stratégiu založenú na vnútropodnikovej infraštruktúre, ako aj na riešeniach na diaľku tretích strán na podporu funkcií aplikácie. Patria medzi ne:

Vlastná infraštruktúra vyvinutá finančným subjektom:

— Zákazník otvorí mobilnú bankovú aplikáciu a je autentifikovaný prostredníctvom bankového rozhrania, čo je vlastné riešenie vyvinuté finančným subjektom, ktoré prijíma požiadavky aplikácie a vracia príslušné odpovede. Bankové rozhranie overí totožnosť zákazníka prostredníctvom dotazu do systému správy účtov a udelí mu prístup k aplikácii.

— Zákazník iniciuje prevod prostredníctvom aplikácie. Aplikácia odošle pokyn do bankového rozhrania, ktoré následne odošle príslušnú žiadosť do systému databázy transakcií.

— Systém správy účtov a systém databázy transakcií, ktoré sa oba prevádzkujú vo vlastnej infraštruktúre, ale sú logicky oddelené od bankového rozhrania, zaznamenajú transakciu.

— Systém databázy transakcií vráti stav transakcie do bankového rozhrania, ktoré tento výsledok zobrazí zákazníkovi.

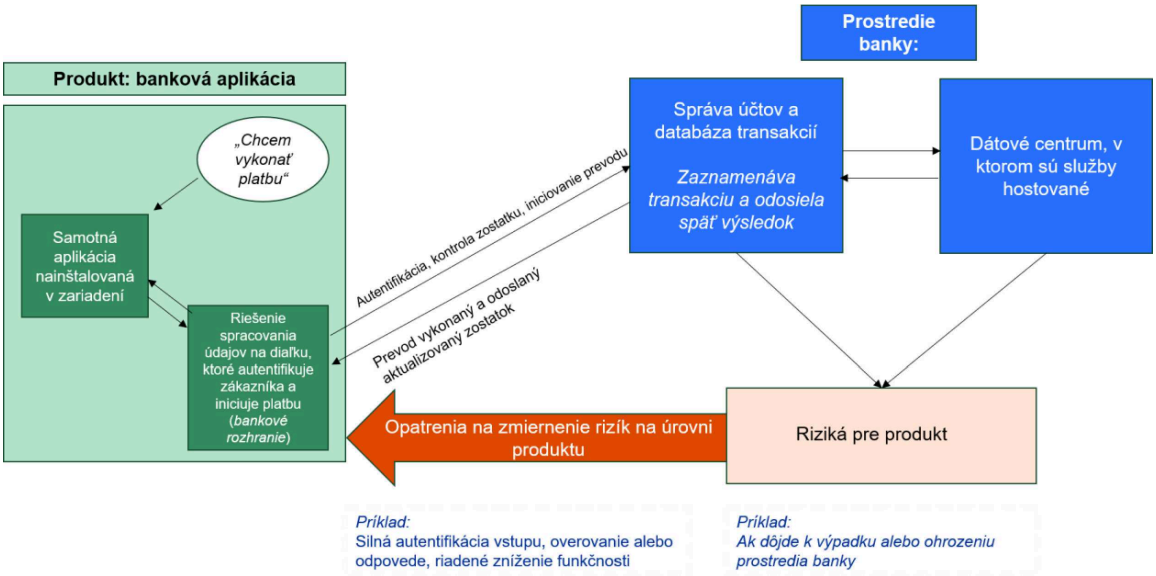
Dôsledky pre riešenia spracovania údajov na diaľku:

— Bankové rozhranie je nevyhnutné na to, aby aplikácia mohla vykonávať svoje funkcie, konkrétne autentifikovať zákazníka, odosielať pokyny zákazníka vrátane pokynov na platby a prevody a vracať výsledný stav. Bankové rozhranie je navrhnuté a vyvinuté na zodpovednosť výrobcu. Keďže odpoveď na obe otázky uvedené v predchádzajúcich oddieloch je kladná, bankové rozhranie sa má považovať za riešenie spracovania údajov na diaľku. Musí sa preto zahrnúť do posúdenia kybernetickobezpečnostných rizík a do vykonávania základných požiadaviek týkajúcich sa produktu s digitálnymi prvkami ako celku. Následné spracovanie pokynu po jeho odoslaní, najmä zaznamenanie transakcie v systéme správy účtov a v systéme databázy transakcií, ako aj zúčtovanie a vyrovnanie, vykonávajú systémy, s ktorými aplikácia priamo neinteraguje, a preto na tomto základe nepredstavujú riešenia spracovania údajov na diaľku.

— Systém správy účtov a systém databázy transakcií sa pre bankovú aplikáciu nepovažujú za riešenia spracovania údajov na diaľku. Aplikácia s nimi priamo neinteraguje (namiesto toho interaguje s bankovým rozhraním, ktoré sa na tieto systémy následne spolieha). Hoci ich dostupnosť môže byť potrebná na dokončenie určitej funkcie, akt o kybernetickej odolnosti sa vzťahuje len na tie časti systému, ktoré priamo interagujú s produktom s digitálnymi prvkami. Na účely aktu o kybernetickej odolnosti teda nepatria do vymedzenia riešení spracovania údajov na diaľku. Tieto systémy však naďalej predstavujú externé závislosti, ktoré môžu pre produkt s digitálnymi prvkami viesť k významným kybernetickobezpečnostným rizikám. Napríklad ohrozenie systému databázy transakcií by mohlo útočníkovi umožniť ovplyvniť výsledky transakcií, ktoré sa následne zobrazia v aplikácii. Výrobca je preto povinný tieto riziká identifikovať a posúdiť v rámci posúdenia kybernetickobezpečnostných rizík a zmierniť ich prostredníctvom opatrení na úrovni produktu, ako sú silná autentifikácia back-endových rozhraní, ochrana integrity transakčných údajov, zabezpečené komunikačné kanály a overovanie odpovedí prijatých aplikáciou.

Obrázok 10

Štylizované znázornenie bankovej aplikácie využívajúcej riešenia spracovania údajov na diaľku



SaaS poskytovaný treťou stranou na podporu zákazníkov:

— Finančný subjekt integruje do svojej aplikácie chatové riešenie zákazníckej podpory, ktoré vyvinul a prevádzkuje poskytovateľ, ktorý je treťou stranou. Poskytovateľ, ktorý je treťou stranou, napísal kód chatového servera, vytvoril používateľské rozhranie a prevádzkuje infraštruktúru, na 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 zabezpečiť tok správ, pričom tretej strane neposkytuje prístup k základným bankovým systémom.

Dôsledky pre riešenia spracovania údajov na diaľku:

— Riešenie chatovej podpory je nevyhnutné na to, aby produkt s digitálnymi prvkami mohol vykonávať jednu zo svojich funkcií, nie je však navrhnuté a vyvinuté finančným subjektom ani na jeho zodpovednosť; preto nejde o riešenie spracovania údajov na diaľku. Malo by sa však považovať za komponent tretej strany. Spoliehanie sa na túto službu poskytovanú treťou stranou môže pre bankovú aplikáciu vytvárať kybernetickobezpečnostné riziká, napríklad ak by útočník využil chatový kanál na vydávanie sa za banku alebo na doručovanie škodlivého obsahu používateľom. Finančný subjekt musí tieto riziká zohľadniť vo svojom posúdení kybernetickobezpečnostných rizík a zmierniť ich prostredníctvom opatrení na úrovni produktu, ako sú oddelenie funkcie chatu od základných bankových funkcií, kontrola tokov údajov a overovanie obsahu. Zároveň by sa mala vykonať aj náležitá starostlivosť v súvislosti s riešením SaaS.

8.3.2. *Inteligentný termostat*

Inteligentný termostat umožňuje používateľom regulovať teplotu v domácnostiach prostredníctvom mobilnej aplikácie. Mobilná aplikácia a inteligentný termostat sa spoliehajú na spracovanie údajov na diaľku pri výmene údajov (napr. žiadosť o zvýšenie teploty) a uchovávaní údajov (napr. preferencie používateľa). Tieto funkcie boli navrhnuté a vyvinuté na zodpovednosť výrobcu, ale fungujú na základnej fyzickej a virtuálnej infraštruktúre poskytovanej treťou stranou (IaaS poskytované treťou stranou).

Keďže inteligentný termostat by bez tohto spracovania údajov na diaľku nemohol vykonávať svoje inteligentné funkcie, jeho neexistencia by bránila produktu s digitálnymi prvkami plniť jednu alebo viacero jeho funkcií. Okrem toho bol softvér navrhnutý a vyvinutý na zodpovednosť výrobcu inteligentného termostatu. Spracovanie údajov na diaľku preto spĺňa podmienky na to, aby sa považovalo za riešenie spracovania údajov na diaľku v zmysle aktu o kybernetickej odolnosti.

Na účely plnenia požiadaviek aktu o kybernetickej odolnosti musí výrobca inteligentného termostatu v technickej dokumentácii produktu s digitálnymi prvkami zdokumentovať riešenie spracovania údajov na diaľku, ako aj využívanie IaaS poskytovaného treťou stranou vrátane podrobností o zmluvne dohodnutej službe. Výrobca musí tieto prvky zohľadniť pri posúdení rizík, ktoré zahŕňa zamýšľaný účel a odôvodnene predvídateľné používanie produktu s digitálnymi prvkami. Výrobca vykonáva základné požiadavky aktu o kybernetickej odolnosti týkajúce sa riešenia spracovania údajov na diaľku na základe rizík. Pokiaľ ide o IaaS poskytované treťou stranou, výrobca musí zabezpečiť, aby bezpečnostné opatrenia poskytované poskytovateľom, ktorý je treťou stranou, boli primerané, a/alebo prijať príslušné opatrenia vo vzťahu k infraštruktúre. V prvom prípade môže výrobca napríklad požadovať dôkazy o tom, že boli splnené povinnosti podľa smernice NIS 2.

8.3.3. *Elektronická čítačka*

Výrobca softvéru pre elektronickú čítačku využíva úložnú službu SaaS poskytovanú treťou stranou na uchovávanie elektronických kníh zakúpených zákazníkmi a na umožnenie prístupu k týmto knihám. Neexistencia tejto úložnej služby by bránila produktu s digitálnymi prvkami plniť jednu z jeho funkcií, úložná služba SaaS poskytovaná treťou stranou však nie je vyvinutá výrobcom ani na jeho zodpovednosť; poskytovateľ SaaS ju sprístupňuje zákazníkom na akýkoľvek prípad použitia.

Úložná služba SaaS nespĺňa vymedzenie riešenia spracovania údajov na diaľku. Výrobca elektronickej čítačky sa však pri fungovaní svojho produktu s digitálnymi prvkami spolieha na túto externú službu, a preto musí zohľadniť súvisiace riziká vo svojom posúdení kybernetickobezpečnostných rizík. Výrobca elektronickej čítačky by mal so službou SaaS zaobchádzať ako s komponentom. Výrobca musí zaviesť primerané bezpečnostné opatrenia na úrovni produktu, ako sú bezpečná autentifikácia, šifrovanie a ochrana integrity komunikácie s úložnou službou. Povinnosti výrobcu podporí aj vykonávanie náležitej starostlivosti pri výbere a integrácii poskytovateľa SaaS, aby produkt s digitálnymi prvkami ako celok mohol spĺňať základné požiadavky.

8.3.4. *Priemyselný robot*

Priemyselný robot má za úlohu zdvíhať súčiastky. Robot odosiela informácie zhromaždené prostredníctvom kamier vzdialenej službe navrhnutej a vyvinutej výrobcom. Táto služba funguje na základnej fyzickej a virtuálnej infraštruktúre poskytovanej poskytovateľom služieb, ktorý je treťou stranou (IaaS poskytované treťou stranou). Cloudová služba vypočítava polohu súčiastky na základe údajov z kamier a odosiela robotovi späť príkazy na zdvíhanie súčiastok.

Neexistencia tohto spracovania údajov by priemyselnému robotovi bránila zdvíhať súčiastky, a teda plniť jednu z jeho funkcií. Okrem toho softvér fungujúci nad touto infraštruktúrou navrhol a vyvinul výrobca. Softvér navrhnutý a vyvinutý výrobcom spĺňa vymedzenie riešenia spracovania údajov na diaľku.

Výrobca priemyselného robota musí v technickej dokumentácii produktu s digitálnymi prvkami zdokumentovať riešenie spracovania údajov na diaľku, ako aj využívanie IaaS poskytovaného treťou stranou vrátane podrobností o zmluvne dohodnutej službe. Výrobca musí takisto tieto prvky zohľadniť pri posúdení rizík, ktoré zahŕňa zamýšľaný účel a odôvodnene predvídateľné používanie produktu s digitálnymi prvkami. Výrobca vykonáva základné požiadavky aktu o kybernetickej odolnosti na základe rizík vo vzťahu k produktu s digitálnymi prvkami vrátane jeho riešení spracovania údajov na diaľku. Plnenie povinností výrobcu takisto podporí vykonávanie náležitej starostlivosti pri výbere poskytovateľa IaaS. Výrobca by napríklad mohol požiadať o dôkaz, že boli splnené povinnosti vyplývajúce zo smernice NIS 2.

8.3.5. *Mobilná sieť*

Smartfón využíva sieť 5G na poskytovanie internetového pripojenia, telefonických hovorov a správ svojim používateľom (mobilné pripojenie). Mobilnú sieť vyvíjajú a navrhujú telekomunikační operátori. Sieť pozostáva z malých bunkových základňových staníc, stožiarov mobilného vysielača a 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 určenie, či produkt s digitálnymi prvkami funguje správne. Sieť je len komunikačným kanálom a nie je nevyhnutná na to, aby produkt s digitálnymi prvkami mohol plniť svoju funkciu „správne sa pripojiť k sieti“. Rovnako ethernetový kábel, smerovač alebo signál Wi-Fi sa nepovažujú za spracovanie údajov, ktorého neexistencia by bránila produktu s digitálnymi prvkami plniť jednu z jeho funkcií, ale skôr za prostriedky umožňujúce komunikáciu/pripojenie.

V dôsledku toho mobilná sieť nespĺňa vymedzenie riešenia spracovania údajov na diaľku. Sieť by sa nemala považovať za komponent tretej strany, keďže do produktu s digitálnymi prvkami nie je integrovaný žiadny softvér; produkt sa na túto sieť iba spolieha. Preto nie je potrebné, aby výrobca vykonával povinnosti náležitej starostlivosti vo vzťahu k poskytovateľovi siete.

9. **ĎALŠIE PRVKY**

9.1. **Oznamovacie povinnosti**

209. Podľa článku 14 ods. 1 a 3 aktu o kybernetickej odolnosti je výrobca povinný súčasne oznámiť jednotke CSIRT určenej za koordinátora a agentúre ENISA: i) každú aktívne zneužívanú zraniteľnosť obsiahnutú v jeho produkte s digitálnymi prvkami, o ktorej sa dozvie a ii) každý závažný incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami a 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 patria do rozsahu pôsobnosti aktu o kybernetickej odolnosti, vrátane produktov s digitálnymi prvkami uvedených na trh pred 11. decembrom 2027. Okrem toho, na rozdiel od povinností týkajúcich sa riešenia zraniteľností, ktoré trvajú len počas obdobia podpory produktu, oznamovacie povinnosti sa naďalej uplatňujú aj po skončení podpory produktu s digitálnymi prvkami. Ak bol produkt s digitálnymi prvkami uvedený na trh pred 11. decembrom 2027 alebo ak sa jeho obdobie podpory skončilo, výrobca nie je povinný plniť povinnosti týkajúce sa riešenia zraniteľností stanovené v prílohe I časti II.

211. Treba pripomenúť, že povinnosť oznámiť takéto udalosti vzniká, keď sa výrobca dozvie, že zraniteľnosť je aktívne zneužívaná alebo že došlo k závažnému incidentu, ktorý viedol k narušeniu bezpečnosti jeho produktu s digitálnymi prvkami. Usmernenia o tom, kedy sa výrobca považuje za osobu, ktorá sa o takejto skutočnosti dozvedela, by preto mali výrobcom pomôcť určiť okamih, od ktorého začínajú plynúť príslušné lehoty na oznámenie.

212. Výrobcovia môžu podliehať porovnateľným oznamovacím povinnostiam podľa rôznych aktov EÚ. S cieľom zabezpečiť jednotný výklad pojmu „dozvedieť sa“ 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 porušenia ochrany osobných údajov podľa všeobecného nariadenia o ochrane údajov.

213. V niektorých prípadoch výrobca zistí podozrivú udalosť alebo tretia strana, ako napríklad fyzická osoba, zákazník, subjekt, orgán, mediálna organizácia alebo iný zdroj, upozorní výrobcu na možný incident alebo zraniteľnosť. V takýchto prípadoch by mal výrobca podozrivú udalosť bezodkladne posúdiť s cieľom určiť, či predstavuje aktívne zneužívanú zraniteľnosť alebo závažný incident, ktorý má vplyv na bezpečnosť produktu s digitálnymi prvkami. Výrobca sa preto považuje za výrobcu, ktorý sa o tejto skutočnosti dozvedel, keď má po takomto úvodnom posúdení primeranú mieru 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, keď možno výrobcu považovať za osobu, ktorá sa o tejto skutočnosti dozvedela, bude preto závisieť od okolností konkrétnej aktívne zneužívanej zraniteľnosti alebo závažného incidentu. V niektorých prípadoch bude od začiatku pomerne jasné, že zraniteľnosť je aktívne zneužívaná alebo že závažný incident má vplyv na bezpečnosť produktu s digitálnymi prvkami. V iných prípadoch môže určitý čas trvať, kým sa zistí, či je produkt s digitálnymi prvkami dotknutý zraniteľnosťou a či túto zraniteľnosť zneužíva škodlivý aktér, alebo či incident má vplyv na bezpečnosť produktu s digitálnymi prvkami. Dôraz by sa však mal klásť na urýchlené vykonanie úvodného posúdenia s cieľom určiť, či sú tieto podmienky skutočne splnené, najmä ak zraniteľnosť môže predstavovať významné riziko, a ak áno, prijať nápravné opatrenia a príslušné skutočnosti oznámiť v súlade s aktom o kybernetickej odolnosti.

215. Štruktúra oznamovacích povinností si navyše vyžaduje, aby výrobcovia svoje oznámenia postupne aktualizovali podľa toho, ako postupuje ich interné vyšetrovanie a ako sa ich poznatky o aktívne zneužívanej zraniteľnosti alebo incidente stávajú podrobnejšími. Výrobcovia sú najmä povinní predložiť včasné varovanie obsahujúce obmedzené množstvo informácií bez zbytočného odkladu a v každom prípade do 24 hodín od okamihu, keď sa o príslušnej skutočnosti dozvedeli. Ďalšie informácie sa následne vyžadujú v rámci oznámenia, ktoré sa má predložiť bez zbytočného odkladu a v každom prípade v lehote 72 hodín od okamihu, keď sa o danej skutočnosti dozvedeli („oznámenie do 72 hodín“). Úplná správa sa musí predložiť do 14 dní od sprístupnenia nápravného alebo zmierňujúceho opatrenia v prípade aktívne zneužívaných zraniteľností alebo do jedného mesiaca od predloženia oznámenia do 72 hodín v prípade závažných incidentov.

216. Ako sa uvádza aj v oddiele *3.3.1. Trvalá podpora a zabezpečenie životaschopnosti slobodného softvéru a softvéru s otvoreným zdrojovým kódom,* správcovia softvéru s otvoreným zdrojovým kódom sú v súlade s článkom 24 ods. 3 povinní hlásiť aktívne zneužívané zraniteľnosti ([30]). Táto povinnosť vzniká okamihom, keď sa daný subjekt dozvie o aktívne zneužívanej zraniteľnosti, a nie už samotnou existenciou zraniteľnosti v kódovej základni slobodného softvéru a softvéru s otvoreným zdrojovým kódom, ktorého je tento subjekt správcom. Keďže komponenty slobodného softvéru a softvéru s otvoreným zdrojovým kódom sú zvyčajne integrované do iných produktov s digitálnymi prvkami smerom k následným používateľom, správca sa v praxi pravdepodobne dozvie o aktívnom zneužívaní prostredníctvom hlásení tretích strán, ktoré identifikujú zneužívanie takýchto komponentov integrovaných do iných produktov s digitálnymi prvkami. Môže ísť napríklad o prípad, keď výrobca produktu s digitálnymi prvkami zistí aktívne zneužívanie komponentu slobodného softvéru a softvéru s otvoreným zdrojovým kódom integrovaného do vlastného produktu a oznámi to správcovi daného komponentu, alebo keď používateľ či výskumník v oblasti bezpečnosti nájde dôkazy o zneužívaní komponentu slobodného softvéru a softvéru s otvoreným zdrojovým kódom integrovaného do produktu s digitálnymi prvkami a toto aktívne zneužívanie oznámi správcovi daného komponentu.

217. Zároveň treba upresniť, že keďže povinnosť oznamovať aktívne zneužívané zraniteľnosti platí vtedy, keď sa výrobca dozvie o aktívnom zneužívaní, výrobca nie je povinný oznamovať zraniteľnosti, o ktorých aktívnom zneužívaní sa dozvedel už pred 11. septembrom 2026 (dátumom, od ktorého sa oznamovacia povinnosť začína uplatňovať). V akte o kybernetickej odolnosti sa preto nevyžaduje retroaktívne oznamovanie takýchto zraniteľností. Naproti tomu táto povinnosť sa uplatňuje, ak výrobca vedel o zraniteľnosti pred 11. septembrom 2026, ale v tom čase nevedel o jej aktívnom zneužívaní (buď preto, že k nemu ešte nedošlo, alebo preto, že sa o ňom výrobca ešte nemal vedomosť). Ak po 11. septembri 2026 následne dôjde k aktívnemu zneužívaniu alebo sa o ňom výrobca dozvie, zraniteľnosť sa považuje za aktívne zneužívanú zraniteľnosť, na ktorú sa vzťahuje oznamovacia povinnosť.

218. Podobne je výrobca povinný oznamovať 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 oznámiť túto aktívne zneužívanú zraniteľnosť. Ak si však výrobca je vedomý, že komponent tretej strany obsahuje zraniteľnosť, ale túto zraniteľnosť i) nie je možné zneužiť v jeho produkte s digitálnymi prvkami (napr. preto, že zraniteľný kód nie je dostupný) alebo ii) nebola zneužitá v jeho produkte s digitálnymi prvkami, takáto zraniteľnosť sa nepovažuje za aktívne zneužívanú zraniteľnosť obsiahnutú v jeho produkte s digitálnymi prvkami, a preto sa na tohto výrobcu nevzťahuje oznamovacia povinnosť. Výrobca môže túto zraniteľnosť napriek tomu oznámiť na dobrovoľnom základe v súlade s článkom 15 aktu o kybernetickej odolnosti. V súlade s článkom 13 ods. 6, a ako sa ďalej vysvetľuje v oddiele *9.2.1. Oznamovanie zraniteľností smerom k pôvodným zdrojom a zdieľanie bezpečnostných opráv*, je zároveň povinný dodržiavať požiadavky na riešenie zraniteľností stanovené v časti II prílohy I k aktu o kybernetickej odolnosti, ako aj oznámiť zraniteľnosť osobe alebo subjektu, ktorý daný komponent vyrába alebo udržiava.

([30]) V rozsahu, v akom sa správca podieľa na vývoji produktu s digitálnymi prvkami.

219. Po tom, ako sa výrobcovia dozvedia o aktívne zneužívanej zraniteľnosti alebo závažnom incidente, takisto sú povinní v súlade s článkom 14 ods. 8 informovať postihnutých používateľov, prípadne všetkých používateľov. Ak tak neurobia včas, jednotky CSIRT, ktoré oznámenie prijali, môžu takéto informácie poskytnúť používateľom, ak sa to považuje za primerané a potrebné na predchádzanie vplyvu danej zraniteľnosti alebo incidentu alebo na jeho zmiernenie.

220. V súlade s prístupom aktu o kybernetickej odolnosti založeným na rizikách sa povinnosť informovať používateľov stanovená v článku 14 ods. 8 uplatňuje primeraným spôsobom založeným na rizikách. Poskytnutie informácií o aktívne zneužívanej zraniteľnosti alebo závažnom incidente najmä neznamená, že tieto informácie musia byť zverejnené alebo sprístupnené bez rozdielu. Ak je to vhodné a s ohľadom na povahu produktu s digitálnymi prvkami, postihnutých používateľov a možný vplyv zraniteľnosti alebo incidentu, výrobcovia môžu obmedziť sprístupnenie podrobných informácií na príslušných dotknutých používateľov alebo zákazníkov. Platí to najmä pre produkty s digitálnymi prvkami používané v citlivých alebo základných prostrediach, kde by verejné sprístupnenie technických podrobností mohlo samo osebe zvýšiť kybernetickobezpečnostné riziká alebo uľahčiť ďalšie zneužívanie.

221. Po primeranom vyriešení alebo zmiernení zraniteľnosti môže byť vhodné širšie sprístupnenie informácií. Mohlo by ísť napríklad o prípad, keď sprístupnenie informácií 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 podrobnosti a načasovanie akéhokoľvek širšieho sprístupnenia informácií mali zostať primerané a mali by zohľadňovať zvyškové riziká zneužitia, povahu produktu s digitálnymi prvkami a záujmy dotknutých používateľov. Okrem toho sa v prílohe I časti II bode 4 vyžaduje, aby výrobcovia po sprístupnení bezpečnostnej aktualizácie verejne sprístupnili informácie o odstránených zraniteľnostiach.

9.2. **Riešenie zraniteľností**

9.2.1. *Oznamovanie zraniteľností smerom k pôvodným zdrojom a zdieľanie bezpečnostných opráv*

222. V článku 13 ods. 6 aktu o kybernetickej odolnosti sa vyžaduje, aby výrobcovia oznamovali zraniteľnosti v integrovaných komponentoch osobe alebo subjektu, ktorý daný komponent vyrába alebo udržiava („oznamovanie smerom k pôvodnému zdroju“).

223. Výrobcovia sú povinní oznamovať zraniteľnosti smerom k pôvodnému zdroju len v súvislosti s verziou komponentu, ktorú integrujú. Ak osoba alebo subjekt, ktorý komponent vyrába alebo udržiava, zaviedol bezpečnostné politiky, procesy koordinovaného zverejňovania zraniteľností alebo určil kanály na oznamovanie zraniteľností, výrobcovia by mali oznamovanie vykonávať v súlade s nimi, najmä ak by predčasné zverejnenie neopravených zraniteľností mohlo zvýšiť kybernetickobezpečnostné riziká. Okrem toho s cieľom znížiť zaťaženie subjektov vykonávajúcich údržbu pri pôvodnom zdroji, najmä v projektoch s otvoreným zdrojovým kódom, výrobcovia nie sú povinní oznamovať zraniteľnosť smerom k pôvodnému zdroju, ak môžu potvrdiť, že osoba alebo subjekt, ktoré komponent vyrábajú alebo udržiavajú, už o existencii zraniteľnosti vedia. Výrobcovia sa vyzývajú, aby prijali primerané opatrenia na predchádzanie podávaniu duplicitných oznámení, napríklad tým, že pred oznámením smerom k pôvodnému zdroju preveria verejne prístupné databázy zraniteľností, bezpečnostné upozornenia týkajúce sa konkrétneho projektu alebo zavedené systémy sledovania problémov.

224. Výrobcovia sú povinní oznamovať smerom k pôvodnému zdroju len tie zraniteľnosti, ktoré existujú v samotnom integrovanom komponente, a nie zraniteľnosti, ktoré vznikajú v dôsledku integrácie medzi komponentom a iným kódom vyvinutým výrobcom alebo v dôsledku integrácie ďalších komponentov. Môžu však nastať situácie, v ktorých integrácia komponentu do konkrétneho produktu s digitálnymi prvkami odhalí určité správanie, interakcie alebo charakteristiky komponentu relevantné z hľadiska bezpečnosti, ktoré neboli pri samostatnom posudzovaní komponentu zjavné alebo ich nebolo možné ľahko identifikovať. V takýchto prípadoch sa výrobcovia vyzývajú, aby tieto informácie oznámili osobe alebo subjektu, ktoré komponenty vyrábajú alebo udržiavajú, s cieľom podporovať správne postupy riešenia zraniteľností, ktoré pomáhajú účinnej náprave a zvyšovaniu celkovej bezpečnosti ekosystému komponentov.

225. Napokon, výrobcovia takisto nie sú povinní oznamovať zraniteľnosť smerom k pôvodnému zdroju, ak komponent už nemá subjekt vykonávajúci údržbu alebo ak výrobca už nie je závislý od pôvodného subjektu vykonávajúceho údržbu, pokiaľ ide o nové verzie alebo bezpečnostné opravy. V takýchto prípadoch sa však výrobcom odporúča informovať používateľov daného komponentu prostredníctvom primeraných alternatívnych opatrení, napríklad prostredníctvom existujúcich komunitných mechanizmov (ako sú e-mailové konferencie alebo hlásenia v systémoch sledovania problémov) alebo prostredníctvom verejných záznamov o zraniteľnostiach.

226. Okrem toho sú podľa článku 13 ods. 6 výrobcovia, ktorí vyvinuli softvérovú úpravu na riešenie zraniteľnosti v integrovanom komponente, povinní túto softvérovú úpravu („bezpečnostnú opravu“) zdieľať s osobou alebo subjektom, ktorý daný komponent vyrába alebo udržiava („zdieľanie smerom k pôvodnému zdroju“).

227. Ak sú výrobcovia povinní zdieľať bezpečnostnú opravu podľa článku 13 ods. 6, táto oprava by sa mala v relevantných prípadoch poskytnúť v strojovo čitateľnom formáte spôsobom, ktorý umožní osobe alebo subjektu, ktoré komponent vyrábajú alebo udržiavajú, jednoduché overenie a prípadne aj integráciu danej opravy. Ak je komponentom komponent slobodného softvéru a softvéru s otvoreným zdrojovým kódom, bezpečnostná oprava by sa mala zdieľať spôsobom kompatibilným s licenciou daného komponentu, napríklad tak, že sa zdieľa pod tou istou licenciou alebo pod licenciou, ktorá subjektu vykonávajúcemu údržbu umožňuje distribuovať opravu pod jeho vlastnou licenciou. Ak subjekt vykonávajúci údržbu daného komponentu stanovil usmernenia týkajúce sa spôsobu zdieľania bezpečnostných opráv, výrobca by mal tieto usmernenia dodržiavať.

228. V akte o kybernetickej odolnosti sa však od výrobcov nevyžaduje, aby zabezpečili, že osoba alebo subjekt, ktorý komponent vyrába alebo udržiava, ich bezpečnostné opravy nevyhnutne prijme. Rovnako sa od nich nevyžaduje, aby zabezpečili, že tieto opravy budú nevyhnutne integrované do úložiska kódu komponentu, napríklad ak subjekt vykonávajúci údržbu uprednostní iný spôsob riešenia daného problému. Podobne výrobcovia nie sú povinní prijať navrhovanú opravu vyvinutú subjektom vykonávajúcim údržbu komponentu a môžu uprednostniť zmiernenie problému inými vhodnými spôsobmi.

229. V niektorých prípadoch mohla osoba alebo subjekt, ktorý komponent vyrába alebo udržiava, už poskytnúť bezpečnostnú opravu na riešenie zraniteľnosti, ale výrobca uplatní inú stratégiu zmiernenia rizika (napríklad zmenou inej konfigurácie). V takýchto prípadoch sa v akte o kybernetickej odolnosti nevyžaduje, aby výrobca zdieľal smerom k pôvodnému zdroju úpravu inej časti systému. Výrobca sa však vyzýva, aby tak urobil, ak to môže podporiť osobu alebo subjekt, ktorý komponent udržiava.

9.2.2. *Známe zneužiteľné zraniteľnosti*

230. V jednej zo základných požiadaviek časti I prílohy I k aktu o kybernetickej odolnosti sa stanovuje, že na základe posúdenia kybernetickobezpečnostných rizík uvedeného v článku 13 ods. 2 a v relevantných prípadoch sa produkty s digitálnymi prvkami musia sprístupňovať na trhu bez známych zneužiteľných zraniteľností.

231. V článku 3 bode 41 sa „zneužiteľná zraniteľnosť“ vymedzuje ako „zraniteľnosť, ktorú môže nepriateľský subjekt účinne využiť za reálnych prevádzkových podmienok“. Nie všetky zraniteľnosti sú zneužiteľné za praktických prevádzkových podmienok a niektoré zraniteľnosti možno zneužiť len za teoretických podmienok (napr. v laboratóriu alebo v simulácii) a/alebo nie za podmienok, ktoré by sa vyskytovali v prevádzkovom prostredí produktu s digitálnymi prvkami.

232. V akte o kybernetickej odolnosti sa vyžaduje, aby výrobcovia mali zavedené primerané politiky a postupy na riešenie a nápravu potenciálnych zraniteľností oznámených z interných alebo externých zdrojov (článok 13 ods. 8). Výslovne sa v ňom však neurčuje, kedy sa má zneužiteľná zraniteľnosť považovať za známu výrobcovi, čím vzniká povinnosť dodržiavať túto základnú požiadavku v okamihu uvedenia na trh.

233. Zraniteľnosť by sa mala považovať za známu, ak je uvedená v relevantných verejne prístupných databázach zraniteľností, ako je európska databáza zraniteľností zriadená podľa článku 12 ods. 2 smernice (EÚ) 2022/2555 alebo iné významné databázy zraniteľností.

234. Zraniteľnosť môže byť navyše známa aj vtedy, keď sa o nej výrobca dozvie prostredníctvom neverejných informácií, napríklad prostredníctvom koordinovaného zverejnenia zo strany výskumníka v oblasti bezpečnosti alebo prostredníctvom vlastného interného testovania a analýzy výrobcu, a to napríklad aj pri využívaní služieb využívajúcich umelú inteligenciu. Rovnako môže byť zraniteľnosť známa aj vtedy, ak bola verejne a výrazne oznámená v dôveryhodných médiách vrátane špecializovaných publikácií o kybernetickej bezpečnosti alebo všeobecných masmédiách.

235. Samotná skutočnosť, že zraniteľnosť bola oznámená alebo zistená, však sama osebe neznamená, že je v praxi zneužiteľná alebo že sa vzťahuje na konkrétny dotknutý produkt s digitálnymi prvkami. Výrobca ju bude musieť preskúmať a potvrdiť pravdivosť takýchto informácií a ich uplatniteľnosť na jeho vlastný produkt s digitálnymi prvkami. Medzi prvým oznámením zraniteľnosti a jej potvrdením preto môže uplynúť určitý obmedzený čas. Ako je uvedené v oddiele *9.1. Oznamovacie povinnosti*, dôraz by sa mal klásť na rýchle konanie zamerané na vyšetrovanie a reakciu.

236. Okrem toho sa povinnosť výrobcov dodržiavať základné požiadavky stanovené v prílohe I časti I v súlade s článkom 13 ods. 1 uplatňuje v okamihu uvedenia na trh. V praxi sa môže stať, že v záverečných fázach životného cyklu vývoja produktu s digitálnymi prvkami sa objavia nové potenciálne zneužiteľné zraniteľnosti, a to aj krátko pred jeho vstupom do distribučného reťazca (a teda pred jeho uvedením na trh).

237. Keďže povinnosť uvádzať na trh produkty s digitálnymi prvkami bez známych zneužiteľných zraniteľností je povinnosťou založenou na rizikách, výrobca musí na základe posúdenia kybernetickobezpečnostných rizík určiť, či možno produkt s digitálnymi prvkami bezpečne uviesť na trh v súlade s aktom o kybernetickej odolnosti. Prípadne môže rozhodnúť, že novú zraniteľnosť, ktorá sa mohla stať známou, je potrebné odstrániť pred uvedením produktu s digitálnymi prvkami na trh. Pri takomto rozhodovaní by výrobcovia mali zohľadniť závažnosť, zneužiteľnosť a potenciálny vplyv zraniteľnosti, ako aj riziká, ktoré vznikajú pre samotný produkt s digitálnymi prvkami po jeho uvedení do používania. Môžu zohľadniť aj riziká spojené s odložením uvedenia produktu na trh až do odstránenia zraniteľnosti, napríklad preto, že nové vydanie zároveň rieši iné zneužiteľné zraniteľnosti alebo je potrebné na zabezpečenie nepretržitej prevádzky kritických systémov. V každom prípade po uvedení produktu s digitálnymi prvkami na trh výrobca naďalej podlieha povinnosti účinne riešiť zraniteľnosti v súlade s požiadavkami na riešenie zraniteľností stanovenými v prílohe I časti II.

9.2.3. *Účinné a pravidelné testy a preskúmania*

238. V prílohe I časti II bode 3 sa od výrobcov vyžaduje, aby počas celého obdobia podpory produktu s digitálnymi prvkami vykonávali účinné a pravidelné testy a preskúmania. Vykonávanie pravidelných testov neznamená mechanické opakovanie nezmenenej testovacej kampane v pevne stanovených intervaloch. Znamená to, že sa pravidelne preskúmava, či si nové vstupné informácie, ako sú novo identifikované hrozby alebo novo objavené zraniteľnosti, nevyžadujú aktualizáciu existujúcich testov, a následne tieto testy primerane vykonávajú.

239. Frekvencia, hĺbka a obsah preskúmania by mali byť primerané rizikovému profilu produktu s digitálnymi prvkami, pokiaľ ide o kybernetickú bezpečnosť, jeho vývoju v priebehu času a aktuálnemu stavu prostredia hrozieb. Ak sa pri preskúmaní zistia relevantné nové vstupné informácie, ktoré majú vplyv na súbor testov, mali by sa navrhnúť a vykonať nové alebo upravené testy produktu s cieľom zabezpečiť, aby žiadne zraniteľnosti nezostanú bez riešenia. Môže to zahŕňať aj opätovné vykonanie existujúcich testov, ak si to vyžaduje úprava produktu s digitálnymi prvkami, napríklad regresné testovanie.

240. Ak sa pri preskúmaní nezistia žiadne takéto nové vstupné informácie, nie je potrebné navrhovať ďalšie testy. Ostatné povinnosti týkajúce sa riešenia zraniteľností vrátane povinnosti riešiť a napravať zraniteľnosti primerane rizikám, ktoré predstavujú, sa naďalej uplatňujú súbežne.

9.3. **Vzájomné prepojenie s ostatnými právnymi predpismi**

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

241. V článku 2 ods. 2 písm. c) aktu o kybernetickej odolnosti 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 definovaných v článku 4 nariadenia (EÚ) 2018/858 a na systémy, komponenty a samostatné technické jednotky navrhnuté a konštruované pre tieto vozidlá“.

242. Podobne boli z rozsahu pôsobnosti aktu o kybernetickej odolnosti vyňaté produkty s digitálnymi prvkami, ktoré patria do rozsahu pôsobnosti nariadenia (EÚ) č. 168/2013, a to 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 časti a zariadenie konštruované a vyrobené pre takéto vozidlá“ (článok 2 ods. 1).

243. Vozidlá, na ktoré sa vzťahujú uvedené nariadenia, nepodliehajú aktu o kybernetickej odolnosti. Okrem toho sú potrebné ďalšie objasnenia, pokiaľ ide o rozsah výnimky pre systémy, komponenty, samostatné technické jednotky, diely a vybavenie (na účely tohto oddielu ďalej len „komponenty“) určené a vyrobené pre takéto vozidlá, ktoré sa považujú za produkty s digitálnymi prvkami v zmysle aktu o kybernetickej odolnosti.

244. Predpokladá sa, že takéto komponenty nepodliehajú aktu o kybernetickej odolnosti, ak sú určené 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 takéhoto komponentu predáva tento komponent priamo výrobcovi vozidiel alebo inému hospodárskemu subjektu v dodávateľskom reťazci automobilového priemyslu, pokiaľ je komponent jednoznačne určený a vhodný len na konečnú integráciu do týchto vozidiel.

245. Naopak, výrobca, ktorý predáva všeobecne použiteľné komponenty, ktoré sú produktmi s digitálnymi prvkami a ktoré možno integrovať do rôznych druhov produktov, a nielen výlučne do vozidiel, na ktoré sa vzťahujú uvedené nariadenia, podlieha aktu o kybernetickej odolnosti.

246. Posúdenie toho, či je komponent uvedený na trh v zmysle aktu o kybernetickej odolnosti, musí vychádzať z objektívnych podmienok, za ktorých sa sprístupňuje na trhu. Ak výrobca ponúka komponent, ktorý nie je výlučne vhodný na konečnú integráciu do týchto vozidiel, prostredníctvom distribučných kanálov otvorených zákazníkom mimo dodávateľského reťazca automobilového priemyslu, ako sú všeobecné maloobchodné predajne alebo online predajné kanály prijímajúce objednávky od širokej verejnosti, tento komponent patrí do rozsahu pôsobnosti aktu o kybernetickej odolnosti bez ohľadu na akékoľvek vyhlásenia týkajúce sa jeho zamýšľaného použitia. Za takýchto okolností komponent nemožno považovať za komponent určený a vyrobený výlučne na integráciu do vozidiel, na ktoré sa vzťahujú nariadenia (EÚ) 2019/2144 a č. 168/2013, a výrobca je povinný dodržiavať akt o kybernetickej odolnosti. Naopak, používanie obmedzených distribučných kanálov medzi podnikmi, ktoré sú vyhradené pre dodávateľský reťazec automobilového priemyslu, môže naznačovať, že komponent je určený a vyrobený výlučne na takúto integráciu.

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

247. V článku 69 ods. 1 aktu o kybernetickej odolnosti 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. Pokračujúca platnosť takýchto certifikátov a rozhodnutí o schválení by sa mala chápať ako obmedzená na kybernetickobezpečnostné riziká a zodpovedajúce požiadavky, ktoré sú upravené príslušnými harmonizačnými právnymi predpismi Únie, na základe ktorých boli vydané. V prípade týchto rizík výrobcovia nie sú povinní opätovne posudzovať ani opätovne preukazovať súlad výlučne na účely aktu o kybernetickej odolnosti počas obdobia platnosti uvedeného v článku 69 ods. 1 pri produktoch s digitálnymi prvkami, ktoré majú v úmysle uviesť na trh 11. decembra 2027 alebo neskôr a do 11. júna 2028 ([31]). Platí to pre certifikáty a rozhodnutia o schválení vydané v prípadoch, keď sa v príslušných harmonizačných právnych predpisoch Únie vyžaduje, aby výrobca vykonal postup posudzovania zhody 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 nezbavuje výrobcov povinnosti vykonať komplexné posúdenie kybernetickobezpečnostných rizík podľa aktu o kybernetickej odolnosti (ani ich nezbavuje iných povinností podľa tohto aktu). Umožňuje im však opierať sa o existujúce certifikácie ako o dôkaz súladu v rámci postupu posudzovania zhody, a to v rozsahu, v akom sú príslušné kybernetickobezpečnostné riziká už pokryté. Ak platnosť certifikátu alebo rozhodnutia o schválení podľa iných harmonizačných právnych predpisov Únie presahuje 11. jún 2028, výrobca sa môže na takýto certifikát alebo rozhodnutie na účely aktu o kybernetickej odolnosti spoliehať len do 11. júna 2028.

250. Ak sa pri posúdení kybernetickobezpečnostných rizík vykonanom v súlade s článkom 13 ods. 2 identifikujú ďalšie riziká, ktoré nie sú pokryté požiadavkami na kybernetickú bezpečnosť, na ktorých je založený existujúci certifikát alebo rozhodnutie o schválení, výrobcovia naďalej zodpovedajú za riešenie týchto rizík v súlade s aktom o kybernetickej odolnosti. V takýchto prípadoch si súlad vyžaduje, aby sa identifikované nedostatky posúdili a zmiernili bez ohľadu na pretrvávajúcu platnosť existujúceho certifikátu alebo rozhodnutia o schválení.

251. Možno to ilustrovať na prípade, keď produkt s digitálnymi prvkami podlieha požiadavkám na kybernetickú bezpečnosť stanoveným v delegovanom nariadení Komisie (EÚ) 2022/30, ktorým sa dopĺňa smernica 2014/53/EÚ (delegovaný akt k smernici o rádiových zariadeniach), a keď bol na základe týchto požiadaviek vydaný certifikát EÚ skúšky typu alebo bolo vydané rozhodnutie o schválení. V takom prípade zostávajú certifikát alebo rozhodnutie v súlade s článkom 69 ods. 1 platné pre tie kybernetickobezpečnostné riziká, ktoré sú zahrnuté v tomto certifikáte a súvisia so základnými požiadavkami na kybernetickú bezpečnosť podľa smernice 2014/53/EÚ (smernica o rádiových zariadeniach).

252. V takýchto prípadoch výrobcovia nie sú na účely aktu o kybernetickej odolnosti povinní opätovne posudzovať ani opätovne preukazovať súlad, pokiaľ ide o riziká, ktoré už boli riešené v rámci týchto certifikátov, a to počas obdobia, v ktorom príslušný certifikát alebo rozhodnutie o schválení zostávajú platné, v každom prípade však najneskôr do 11. júna 2028. Patria sem napríklad kybernetickobezpečnostné riziká súvisiace s ochranou sietí, ochranou osobných údajov a súkromia alebo predchádzaním podvodom (v rozsahu, v akom sú tieto riziká zahrnuté v danom certifikáte), ktoré súvisia s požiadavkami na kybernetickú bezpečnosť podľa smernice o rádiových zariadeniach a sú zohľadnené pri posudzovaní zhody.

253. Ak sa však pri posúdení kybernetickobezpečnostných rizík vykonanom v súlade s článkom 13 ods. 2 aktu o kybernetickej odolnosti identifikujú ďalšie kybernetickobezpečnostné riziká, ktoré nie sú pokryté týmito certifikátmi, výrobcovia naďalej zodpovedajú za riešenie týchto rizík v súlade s aktom o kybernetickej odolnosti. Môže ísť napríklad o riziká súvisiace s procesmi riešenia zraniteľností, minimalizáciou údajov a znižovaním plochy útoku alebo o iné kybernetickobezpečnostné aspekty špecifické pre daný produkt, ktoré nie sú riešené týmito certifikátmi alebo ktoré v každom prípade nie sú pokryté základnými požiadavkami na kybernetickú bezpečnosť podľa smernice o rádiových zariadeniach.

254. Existencia platného certifikátu EÚ skúšky typu alebo rozhodnutia o schválení podľa smernice o rádiových zariadeniach týkajúceho sa jej základných požiadaviek súvisiacich s kybernetickou bezpečnosťou preto sama osebe nepreukazuje úplný súlad s aktom o kybernetickej odolnosti. Namiesto toho umožňuje výrobcom spoliehať sa na takýto certifikát alebo rozhodnutie ako na dôkaz súladu, pokiaľ ide o príslušné riziká, pričom zároveň musia zabezpečiť, aby sa všetky zostávajúce alebo novo identifikované riziká posúdili a zmiernili v súlade s aktom o kybernetickej odolnosti.

([31]) Na produkty s digitálnymi prvkami uvedené na trh pred 11. decembrom 2027 sa vzťahujú právne predpisy Únie platné v čase ich uvedenia na trh a ak boli s nimi v súlade, môžu sa predávať a uvádzať do prevádzky, pokiaľ sa na nich 11. decembra 2027 alebo neskôr nevykonajú podstatné úpravy. Pokiaľ ide o pojmy „uvedenie na trh“ a „sprístupnenie na trhu“, pozri aj oddiel *2.1. Uvedenie na trh* tohto dokumentu, ako aj kapitolu 2 Modrej príručky.

255. Podobne, ak produkt s digitálnymi prvkami podlieha základným požiadavkám na ochranu zdravia a bezpečnosť súvisiacim s kybernetickou bezpečnosťou stanoveným v nariadení (EÚ) 2023/1230 (nariadenie o strojových zariadeniach), ktoré sa v plnom rozsahu uplatňuje od 20. januára 2027, a ak bol na základe týchto požiadaviek vydaný certifikát EÚ skúšky typu alebo rozhodnutie o schválení, tento certifikát alebo rozhodnutie o schválení zostávajú v súlade s článkom 69 ods. 1 aktu o kybernetickej odolnosti platné pre kybernetickobezpečnostné riziká, na ktoré sa vzťahuje nariadenie o strojových zariadeniach.

256. Ide najmä o aspekty kybernetickej bezpečnosti súvisiace s ochranou pred zneužitím a s bezpečnosťou a spoľahlivosťou ovládacích systémov, ako sa stanovuje 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 aktu o kybernetickej odolnosti povinní opätovne posudzovať ani opätovne preukazovať súlad počas obdobia, v ktorom príslušný certifikát alebo rozhodnutie o schválení zostávajú platné, v každom prípade však najneskôr do 11. júna 2028. Platí to v rozsahu, v akom boli tieto riziká riešené v rámci posudzovania zhody podľa nariadenia o strojových zariadeniach.

257. Rovnako ako v prípade uvedených základných požiadaviek smernice o rádiových zariadeniach týkajúcich sa kybernetickej bezpečnosti, ak sa pri posúdení kybernetickobezpečnostných rizík vykonanom podľa článku 13 ods. 2 aktu o kybernetickej odolnosti identifikujú ďalšie kybernetickobezpečnostné riziká, ktoré nie sú pokryté príslušným certifikátom vydaným podľa nariadenia o strojových zariadeniach a ktoré súvisia s požiadavkami tohto nariadenia na kybernetickú bezpečnosť, výrobcovia naďalej zodpovedajú za riešenie týchto rizík v súlade s aktom o kybernetickej odolnosti.