EVROPSKÁ
KOMISE

V Bruselu dne 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020

(Text s významem pro EHP)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Hardwarové a softwarové produkty se stále častěji stávají předmětem úspěšných kybernetických útoků, což do roku 2021 povede k odhadovaným celosvětovým ročním nákladům spojeným s kybernetickou kriminalitou ve výši 5,5 bilionu EUR. Tyto produkty trpí dvěma hlavními problémy, které zvyšují náklady pro uživatele a společnost: 1) nízká úroveň kybernetické bezpečnosti, která se odráží v rozšířené zranitelnosti a nedostatečném a nekonzistentním poskytování bezpečnostních aktualizací k jejímu řešení, a 2) nedostatečné chápání informací a přístup k informacím ze strany uživatelů, což jim znemožňuje vybrat si produkty s odpovídajícími vlastnostmi kybernetické bezpečnosti nebo je používat bezpečným způsobem. V propojeném prostředí může kybernetický bezpečnostní incident v jednom produktu ovlivnit celou organizaci nebo celý dodavatelský řetězec a často se do několika minut rozšířit přes hranice vnitřního trhu. To může vést k vážnému narušení hospodářských a sociálních činností nebo dokonce ohrozit životy.

Kybernetická bezpečnost produktů s digitálními prvky má silný přeshraniční rozměr, neboť produkty vyrobené v jedné zemi se často používají na celém vnitřním trhu. Kromě toho incidenty, které se zpočátku dotýkají jednoho subjektu nebo jednoho členského státu, se často během několika minut rozšíří po celém vnitřním trhu.

Zatímco stávající právní předpisy pro vnitřní trh se na některé produkty s digitálními prvky vztahují, většina hardwarových a softwarových produktů není v současné době upravena žádným právním předpisem EU, který by se zabýval jejich kybernetickou bezpečností. Stávající právní rámec EU se zejména nezabývá kybernetickou bezpečností nevestavěného softwaru, a to ani v případě, že se kybernetické útoky stále více zaměřují na zranitelnosti těchto produktů, což způsobuje značné společenské a hospodářské náklady. Existují četné příklady významných kybernetických útoků vyplývajících z neoptimální bezpečnosti produktů, jako ransomwarový červ WannaCry, který zneužil zranitelnost systému Windows a v roce 2017 postihl 200 000 počítačů ve 150 zemích, přičemž způsobil škodu v řádu miliard USD; útok v dodavatelském řetězci společnosti Kaseya VSA, který využil software pro správu sítě společnosti Kaseya k útoku na více než 1 000 společností a přinutil řetězec supermarketů k uzavření všech 500 prodejen po celém Švédsku; nebo řada incidentů, při nichž dochází k hackerskému útoku na bankovní aplikace s cílem ukrást peníze nic netušícím spotřebitelům.

Byly stanoveny dva hlavní cíle za účelem zajištění řádného fungování vnitřního trhu: 1) vytvořit podmínky pro vývoj bezpečných produktů s digitálními prvky tím, že bude zajištěno, aby hardwarové a softwarové produkty byly uváděny na trh s méně zranitelnostmi a aby výrobci brali vážně bezpečnost v průběhu celého životního cyklu produktu, a 2) vytvořit podmínky umožňující uživatelům, aby při výběru a používání produktů s digitálními prvky zohlednili kybernetickou bezpečnost. Byly stanoveny čtyři konkrétní cíle: i) zajistit, aby výrobci zlepšili bezpečnost produktů digitálními prvky od fáze návrhu a vývoje a během celého životního cyklu; ii) zajistit soudržný rámec kybernetické bezpečnosti, který výrobcům hardwaru a softwaru usnadní dodržování předpisů; iii) zvýšit transparentnost bezpečnostních vlastností produktů s digitálními prvky a iv) umožnit podnikům a spotřebitelům bezpečné používání produktů s digitálními prvky.

Silná přeshraniční povaha kybernetické bezpečnosti a rostoucí počet incidentů, které se přelévají přes hranice a mezi odvětvími a produkty, znamená, že těchto cílů nemohou členské státy účinně dosáhnout samy. Vzhledem ke globální povaze trhů s produkty s digitálními prvky čelí členské státy stejným rizikům u téhož produktu s digitálními prvky na svém území. Vznikající roztříštěný rámec potenciálně odlišných vnitrostátních pravidel může narušit otevřený a konkurenceschopný jednotný trh produktů s digitálními prvky. Pro zvýšení důvěry mezi uživateli a přitažlivosti produktů EU s digitálními prvky je proto nezbytná společná akce na úrovni EU. Prospělo by to i vnitřnímu trhu, neboť by poskytoval právní jistotu a zajistil rovné podmínky pro prodejce produktů s digitálními prvky, což je zdůrazněno i v závěrečné zprávě Konference o budoucnosti Evropy, v níž občané požadují větší roli EU v boji proti kybernetickým hrozbám.

- **Vzájemné působení se stávajícími ustanoveními v této oblasti politiky**

Rámec EU obsahuje několik horizontálních právních předpisů, které upravují některá hlediska související s kybernetickou bezpečností z různých úhlů (produkty, služby, řešení krizí a trestná činnost). V roce 2013 vstoupila v platnost směrnice o útocích na informační systémy[1], která harmonizuje kriminalizaci a sankce za řadu trestných činů namířených proti informačním systémům. V srpnu 2016 vstoupila v platnost směrnice (EU) 2016/1148 o bezpečnosti sítí a informačních systémů (směrnice o bezpečnosti sítí a informací)[2] coby první právní předpis EU o kybernetické bezpečnosti. Její revize, jejímž výsledkem je směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)], zvyšuje společnou úroveň ambicí EU. V roce 2019 vstoupil v platnost akt EU o kybernetické bezpečnosti[3], jehož cílem je posílit bezpečnost produktů, služeb a procesů IKT zavedením dobrovolného evropského rámce pro certifikaci kybernetické bezpečnosti[4].

Kybernetická bezpečnost celého dodavatelského řetězce je zajištěna pouze tehdy, jsou-li kyberneticky bezpečné všechny jeho složky. Výše uvedené právní předpisy EU však v tomto ohledu vykazují značné nedostatky, neboť se nevztahují na povinné požadavky na bezpečnost produktů s digitálními prvky.

Zatímco navrhovaný akt o kybernetické odolnosti se vztahuje na produkty s digitálními prvky uváděné na trh, cílem směrnice [směrnice XXX/XXX (o bezpečnosti sítí a informací 2)] je zajistit vysokou úroveň kybernetické bezpečnosti služeb poskytovaných zásadními a významnými subjekty. Směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] vyžaduje, aby členské státy zajistily, že zásadní a důležité subjekty spadající do oblasti její působnosti, například poskytovatelé zdravotní péče nebo cloud computingu a subjekty veřejné správy, přijmou vhodná a přiměřená technická, provozní a organizační opatření v oblasti kybernetické bezpečnosti. Patří sem mimo jiné požadavek na zajištění bezpečnosti při pořizování, vývoji a údržbě sítí a informačních systémů, včetně zveřejňování informací o

---

1 Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (Úř. věst. L 218, 14.8.2013, s. 8).

2 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194/1, 19.7.2016, s. 1).

3 Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

4 Akt o kybernetické bezpečnosti umožňuje rozvoj specializovaných systémů certifikace. Každý systém obsahuje odkazy na příslušné normy, technické specifikace nebo jiné požadavky na kybernetickou bezpečnost vymezené v daném systému. Rozhodnutí vyvinout certifikaci kybernetické bezpečnosti je založeno na posouzení rizik.

zranitelnostech a jejich řešení. Směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] vyžaduje, aby Komise přijala prováděcí akty, kterými stanoví technické a metodické požadavky vyplývající z uvedených opatření pro určité druhy subjektů, například poskytovatele služeb cloud computingu, a to do 21 měsíců ode dne vstupu této směrnice v platnost. Pro všechny ostatní subjekty může Komise přijmout prováděcí akt, kterým stanoví technické a metodické požadavky, jakož i odvětvové požadavky. Tento rámec zajistí, aby technické specifikace a opatření podobná základním požadavkům na kybernetickou bezpečnost stanoveným v aktu o kybernetické odolnosti byla rovněž prováděna při navrhování, vývoji a řešení zranitelnosti softwaru poskytovaného jako služba (software jako služba). To by se například mohlo stát prostředkem k zajištění vysoké úrovně kybernetické bezpečnosti v takových případech, jako jsou systémy elektronických zdravotních záznamů, a to i tehdy, jsou-li poskytovány ve formě Software jako služba (SaaS) nebo vyvíjeny v rámci zdravotnických institucí (interně), v souladu s navrhovaným [nařízením o evropském prostoru pro zdravotní data].

- **Vzájemné působení s ostatními politikami Unie**

Jak se uvádí ve sdělení „Formování digitální budoucnosti Evropy“[5], pro EU je důležité, aby těžila ze všech výhod digitálního věku a posilovala svůj průmysl a inovační kapacitu v bezpečných a etických mezích. Evropská strategie pro data stanoví čtyři pilíře – ochranu údajů, základní práva, bezpečnost a kybernetickou bezpečnost – jako nezbytné předpoklady pro posílení společnosti díky využívání údajů.

Současný rámec EU[6], který se vztahuje na produkty, které mohou rovněž obsahovat digitální prvky, zahrnuje několik právních předpisů, včetně právních předpisů EU o konkrétních produktech zahrnujících bezpečnostní aspekty a obecných právních předpisů o odpovědnosti za výrobek. Návrh je v souladu se stávajícím regulačním rámcem EU týkajícím se produktů, jakož i s nedávnými legislativními návrhy, například návrhem nařízení [nařízení o umělé inteligenci (UI)] předloženým Komisí[7].

Navrhované nařízení by se vztahovalo na všechna rádiová zařízení spadající do oblasti působnosti nařízení Komise v přenesené pravomoci (EU) 2022/30. Požadavky stanovené tímto nařízením navíc zahrnují všechny prvky základních požadavků podle čl. 3 odst. 3 písm. d), e) a f) směrnice 2014/53/EU, včetně hlavních prvků stanovených v [prováděcím rozhodnutí Komise XXX/2022 o žádosti o normalizaci podané evropským normalizačním organizacím] vydaném na základě uvedeného nařízení v přenesené pravomoci. S cílem zabránit překrývání právních předpisů se předpokládá, že Komise zruší nebo změní nařízení v přenesené pravomoci, pokud jde o rádiová zařízení, na něž se vztahuje navrhované nařízení, aby pro ně platilo, jakmile bude použitelné.

Kromě toho se předpokládá, že Komise a evropské normalizační organizace při přípravě a vypracovávání harmonizovaných norem s cílem usnadnit provádění tohoto nařízení zohlední normalizační práci provedenou v souvislosti s prováděcím rozhodnutím Komise C(2022)5637

---

5 Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů „Formování digitální budoucnosti Evropy“ ze dne 19. února 2020, COM(2020) 67 final.

6 Především právní předpisy týkající se nového právního rámce (NPR).

7 Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci) a mění určité legislativní akty Unie ze dne 21. dubna 2021, COM(2021) 206 final.

o žádosti o normalizaci ohledně nařízení v přenesené pravomoci 2022/30 týkajícího se směrnice o rádiových zařízeních, aby se zabránilo zdvojování práce.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Právním základem tohoto návrhu je článek 114 Smlouvy o fungování Evropské unie (SFEU), který stanoví přijetí opatření nezbytných pro vytvoření a fungování vnitřního trhu. Účelem návrhu je harmonizovat požadavky na kybernetickou bezpečnost produktů s digitálními prvky ve všech členských státech a odstranit překážky volného pohybu zboží.

Článek 114 SFEU lze použít jako právní základ umožňující zabránit vzniku těchto překážek, které vyplývají z rozdílných vnitrostátních právních předpisů a přístupů k řešení právní nejistoty a mezer ve stávajících právních rámcích[8]. Soudní dvůr dále uznal, že použití různorodých technických požadavků by mohlo být platným důvodem pro aktivování článku 114 SFEU[9].

Současný legislativní rámec EU, který se vztahuje na produkty s digitálními prvky, je založen na článku 114 SFEU a zahrnuje několik právních předpisů, včetně právních předpisů o konkrétních produktech a aspektech souvisejících s bezpečností nebo obecných právních předpisů o odpovědnosti za výrobek. Vztahuje se však pouze na některé aspekty spojené s kybernetickou bezpečností hmotných digitálních produktů a případně na software vestavěný do těchto produktů. Na vnitrostátní úrovni začínají členské státy přijímat vnitrostátní opatření, která vyžadují, aby prodejci digitálních produktů posílili svou kybernetickou bezpečnost[10]. Zároveň má kybernetická bezpečnost digitálních produktů obzvláště silný přeshraniční rozměr, neboť produkty vyrobené v jedné zemi jsou často používány organizacemi a spotřebiteli na celém vnitřním trhu. Incidenty, které se zpočátku týkají jednoho subjektu nebo členského státu, se často do několika minut rozšíří napříč organizacemi, odvětvími a několika členskými státy.

Různé akty a iniciativy, které byly dosud přijaty na úrovni EU a na vnitrostátní úrovni, řeší zjištěné problémy pouze částečně, přičemž hrozí, že v rámci vnitřního trhu vznikne právní nejednotnost, čímž se zvýší právní nejistota jak pro prodejce, tak pro uživatele těchto produktů a zvýší se zbytečná zátěž pro společnosti, pokud jde o plnění řady požadavků na podobné druhy produktů.

Navrhované nařízení by harmonizovalo a zefektivnilo regulační prostředí EU tím, že zavede požadavky na kybernetickou bezpečnost produktů s digitálními prvky a zabrání překrývání požadavků vyplývajících z různých právních předpisů. Tím by se zajistila větší právní jistota pro hospodářské subjekty a uživatele v celé Unii, jakož i lepší harmonizace evropského jednotného trhu, a vytvořily by se přijatelnější podmínky pro subjekty, které chtějí vstoupit na trh EU.

---

8 Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 3. prosince 2019, Česká republika v. Evropský parlament a Rada Evropské unie, věc C-482/17, bod 35.

9 Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 2. května 2006, Spojené království Velké Británie a Severního Irska v. Evropský parlament a Rada Evropské unie, věc C-217/04, body 62–63.

10 Například v roce 2019 vytvořilo Finsko na základě norem ETSI systém označování zařízení internetu věcí, například inteligentních televizorů, chytrých telefonů a hraček. Německo nedávno zavedlo spotřebitelské bezpečnostní označení pro širokopásmové routery, inteligentní televizory, fotoaparáty, reproduktory, hračky, jakož i pro úklidové a zahradní roboty.

- **Subsidiarita (v případě nevýlučné pravomoci)**

Silná přeshraniční povaha kybernetické bezpečnosti obecně a rostoucí počet rizik a incidentů, které se přelévají přes hranice a mezi odvětvími a produkty, znamená, že cílů tohoto zásahu nemohou členské státy účinně dosáhnout samy. Vnitrostátní přístupy k řešení problémů, a zejména přístupy zavádějící povinné požadavky, vytvoří další právní nejistotu a právní překážky. To by mohlo společnostem bránit v tom, aby bezproblémově rozšiřovaly svou činnost do jiných členských států, což by připravilo uživatele o výhody plynoucí z jejich produktů.

K zajištění vysoké úrovně důvěry mezi uživateli a zvýšení přitažlivosti produktů EU s digitálními prvky je proto nezbytná společná akce na úrovni EU. Prospěla by rovněž jednotnému digitálnímu trhu a vnitřnímu trhu obecně tím, že by výrobcům produktů s digitálními prvky poskytla právní jistotu a zajistila rovné podmínky.

Závěry Rady ze dne 23. května 2022 o vývoji postoje Evropské unie v kybernetické oblasti v konečném důsledku vyzývají Komisi, aby do konce roku 2022 navrhla společné požadavky na kybernetickou bezpečnost zařízení připojených k internetu.

- **Proporcionalita**

Pokud jde o proporcionalitu navrhovaného nařízení, opatření ve zvažovaných možnostech politiky by nepřekračovala rámec toho, co je nezbytné k dosažení obecných a specifických cílů, a nevedla by k nepřiměřeným nákladům. Konkrétně by zvažovaný zásah zajistil, že produkty s digitálními prvky budou zabezpečeny po celou dobu svého životního cyklu a úměrně rizikům, jimž čelí, a to prostřednictvím požadavků zaměřených na cíle a technologicky neutrálních, které zůstanou přiměřené a budou obecně odpovídat zájmům zúčastněných subjektů.

Základní požadavky na kybernetickou bezpečnost uvedené v návrhu vycházejí z široce používaných norem, přičemž proces normalizace, který bude následovat, by zohlednil technické zvláštnosti produktů. To znamená, že v případě potřeby by se pro danou úroveň rizika upravily bezpečnostní kontroly. Kromě toho by plánovaná horizontální pravidla pouze předpokládala posouzení kritických produktů třetí stranou. To by se týkalo jen malé části trhu produktů s digitálními prvky. Dopad na malé a střední podniky by závisel na jejich přítomnosti na trhu s těmito konkrétními kategoriemi produktů.

Pokud jde o přiměřenost nákladů na posuzování shody, oznámené subjekty provádějící posuzování jako třetí strany by při stanovování svých poplatků zohlednily velikost podniku. Na přípravu provedení by bylo rovněž poskytnuto přiměřené přechodné období v délce 24 měsíců, které by příslušným trhům poskytlo čas na přípravu a zároveň by poskytlo jasné vodítko pro směrování investic do výzkumu a vývoje. Veškeré náklady podniků na dodržování předpisů by byly vyváženy výhodami plynoucími z vyšší úrovně bezpečnosti produktů s digitálními prvky a v konečném důsledku ze zvýšení důvěry uživatelů v tyto produkty.

- **Volba nástroje**

Regulační zásah by znamenal přijetí nařízení, a nikoli směrnice. Je tomu tak proto, že pro tento konkrétní druh právních předpisů týkajících se produktů by nařízení účinněji řešilo zjištěné problémy a splňovalo stanovené cíle, neboť se jedná o zásah, který podmiňuje uvádění velmi široké kategorie produktů na vnitřní trh. Proces provádění v případě směrnice by u tohoto zásahu mohl ponechat příliš velký prostor pro rozhodování na vnitrostátní úrovni, což by mohlo vést k nejednotnosti některých základních požadavků na kybernetickou bezpečnost, právní nejistotě, další roztříštěnosti, nebo dokonce diskriminačním přeshraničním

situacím, a to tím více s ohledem na skutečnost, že produkty, na něž se tato směrnice vztahuje, mohou mít více účelů nebo způsobů použití a že výrobci mohou vyrábět více kategorií těchto produktů.

3. VÝSLEDKY HODNOCENÍ *EX POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

- **Konzultace se zúčastněnými stranami**

Komise konzultovala širokou škálu zúčastněných stran. Členské státy a zúčastněné strany byly vyzvány k účasti na otevřené veřejné konzultaci a na průzkumech a seminářích organizovaných v souvislosti se studií, kterou provádí konsorcium podporující přípravné práce Komise na posouzení dopadů: společnost Wavestone, Centrum pro evropská politická studia (CEPS) a společnost ICF. Mezi konzultované zúčastněné strany patřily vnitrostátní orgány dozoru nad trhem, subjekty Unie zabývající se kybernetickou bezpečností, výrobci hardwaru a softwaru, dovozci a distributoři hardwaru a softwaru, obchodní sdružení, spotřebitelské organizace a uživatelé produktů s digitálními prvky a občané, výzkumní pracovníci a akademická obec, oznámené subjekty a akreditační orgány a odborníci z odvětví kybernetické bezpečnosti.

Konzultační činnosti zahrnovaly:

- první studii provedenou konsorciem tvořeným společnostmi ICF, Wavestone, Carsa a centrem CEPS, která byla zveřejněna v prosinci 2021[11]. Studie zjistila několik selhání trhu a posoudila možné regulační zásahy,
- otevřenou veřejnou konzultaci, která se zaměřila na občany, zúčastněné strany a odborníky na kybernetickou bezpečnost. Bylo předloženo 176 odpovědí. Ty přispěly ke shromáždění různých názorů a zkušeností od všech skupin zúčastněných stran,
- na seminářích organizovaných v rámci studie na podporu přípravných prací Komise na aktu o kybernetické odolnosti se sešlo přibližně 100 zástupců ze všech 27 členských států, kteří zastupovali různé zúčastněné strany,
- byly vedeny odborné rozhovory s cílem dosáhnout hlubšího porozumění současným výzvám v oblasti kybernetické bezpečnosti, které souvisejí s produkty s digitálními prvky, a projednat možnosti politiky pro možný regulační zásah,
- proběhla dvoustranná jednání s vnitrostátními orgány pro kybernetickou bezpečnost, soukromým sektorem a spotřebitelskými organizacemi,
- bylo provedeno cílené kontaktování klíčových zúčastněných stran z řad malých a středních podniků.

- **Sběr a využití výsledků odborných konzultací**

Cílem konzultačních činností bylo získat informace o pěti hlavních hodnotících kritériích vycházejících z pokynů EU pro zlepšování právní úpravy (účinnost, účelnost, relevance,

[11] „Study on the need of cybersecurity requirements for ICT products“ (Studie o potřebě požadavků na kybernetickou bezpečnost pro produkty IKT) – č. 2020-0715, závěrečná zpráva o studii, k dispozici na adrese https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

soudržnost a přidaná hodnota EU), jakož i o potenciálních dopadech možných variant do budoucna. Dodavatel nejen oslovil zúčastněné strany, které by byly navrhovaným nařízením přímo dotčeny, ale zároveň konzultoval širokou škálu odborníků v oblasti kybernetické bezpečnosti.

- **Posouzení dopadů**

Komise provedla posouzení dopadů tohoto návrhu, které přezkoumal Výbor pro kontrolu regulace (RSB) Komise. Dne 6. července 2022 se konalo setkání s výborem RSB, z něhož vyplynulo kladné stanovisko. Posouzení dopadů bylo uzpůsobeno tak, aby zohledňovalo doporučení a připomínky výboru RSB.

Komise přezkoumala různé možnosti politiky za účelem dosažení obecného cíle návrhu:

- Přístup založený na právně nevynutitelných předpisech a dobrovolná opatření (možnost 1): v rámci této možnosti by neexistoval žádný povinný regulační zásah. Namísto toho by Komise vydávala sdělení, pokyny, doporučení a případně kodexy chování na podporu dobrovolných opatření. Nadále by se rozvíjely dobrovolné nebo povinné vnitrostátní systémy, které by vyvážily nedostatek horizontálních pravidel EU.
- Regulační zásah *ad hoc* za účelem kybernetické bezpečnosti hmotných produktů s digitálními prvky a příslušného vestavěného softwaru (možnost 2): tato možnost by znamenala regulační zásah *ad hoc* zaměřený na jednotlivé produkty, který by se omezil na doplnění a/nebo změnu požadavků na kybernetickou bezpečnost v již existujících právních předpisech nebo na zavedení nových právních předpisů v souvislosti s nově se objevujícími riziky, včetně případného nevestavěného softwaru.

Možnosti 3 a 4 zahrnují horizontální regulační zásah, který se liší svým rozsahem a z velké části se řídí novým právním rámcem (NPR). Tento rámec stanoví základní požadavky jako podmínku pro uvedení některých produktů na vnitřní trh. NPR rovněž obvykle stanoví posuzování shody, což je postup, který provádí výrobce s cílem prokázat, že byly splněny stanovené požadavky týkající se určitého produktu.

- Smíšený přístup, včetně horizontálních závazných pravidel pro kybernetickou bezpečnost hmotných produktů s digitálními prvky a příslušným vestavěným softwarem a odstupňovaný přístup k nevestavěnému softwaru (možnost 3): tato možnost by zahrnovala nařízení zavádějící horizontální požadavky na kybernetickou bezpečnost pro všechny hmotné produkty s digitálními prvky a v nich vestavěný software jako podmínku pro uvedení na trh a obsahovala by dvě dílčí možnosti s povinným posouzením třetí stranou a bez něj (3i a 3ii). Nevestavěný software by nebyl regulován.
- Horizontální regulační zásah zavádějící požadavky na kybernetickou bezpečnost pro širokou škálu hmotných a nehmotných produktů s digitálními prvky, včetně nevestavěného softwaru (možnost 4): tato možnost se podobá možnosti 3, s výjimkou oblasti působnosti. Možnost 4 by zahrnovala nevestavěný software (s dvěma dílčími možnostmi, které zahrnují pouze kritický (4a), respektive veškerý software (4b)) v oblasti působnosti případného nařízení. U každé dílčí možnosti by byly zváženy stejné dílčí možnosti týkající se posuzování shody jako v případě možnosti 3.

Možnost 4 (s dílčími možnostmi, které se vztahují na veškerý software a zahrnují povinné posouzení kritických produktů třetí stranou) se ukázala jako upřednostňovaná, a to na základě posouzení účinnosti ve vztahu ke specifickým cílům a účinnosti nákladů v porovnání s přínosy. Tato možnost by zajistila stanovení zvláštních horizontálních požadavků na kybernetickou bezpečnost pro všechny produkty s digitálními prvky, které jsou uváděny nebo dodávány na vnitřní trh, a byla by jedinou možností, která by platila pro celý digitální dodavatelský řetězec. Tento regulační zásah by se vztahoval i na nevestavěný software, který je často ohrožen zranitelností, čímž by se zajistil soudržný přístup ke všem produktům s digitálními prvky s jasným rozdělením odpovědnosti různých hospodářských subjektů.

Tato možnost politiky rovněž přináší přidanou hodnotu tím, že se týká aspektů povinnosti péče a celého životního cyklu po uvedení produktů s digitálními prvky na trh s cílem zajistit mimo jiné patřičné informace o podpoře bezpečnosti a poskytování bezpečnostních aktualizací. Tato možnost politiky by rovněž nejúčinněji doplnila nedávný přezkum rámce pro o bezpečnosti sítí a informací tím, že by zajistila předpoklady pro posílení bezpečnosti dodavatelského řetězce.

Upřednostňovaná možnost by měla významné výhody pro různé zúčastněné strany. V případě podniků by zabránila rozdílným bezpečnostním pravidlům pro produkty s digitálními prvky a snížila by náklady na dodržování příslušných právních předpisů v oblasti kybernetické bezpečnosti. Došlo by ke snížení počtu kybernetických incidentů, nákladů na řešení incidentů a újmy na dobré pověsti. Odhaduje se, že v celé EU by tato iniciativa mohla vést ke snížení nákladů v důsledku incidentů postihujících společnosti o přibližně 180 až 290 miliard EUR ročně. Vedla by ke zvýšení obratu v důsledku využívání produktů s požadavkem na digitální prvky. Zlepšila by se tak celosvětová pověst společností, což by vedlo k nárůstu poptávky i mimo EU. Pro uživatele by upřednostňovaná možnost zvýšila transparentnost bezpečnostních vlastností a usnadnila by využívání produktů s digitálními prvky. Spotřebitelé a občané by rovněž těžili z lepší ochrany svých základních práv, například ochrany soukromí a údajů.

Respondenti, kteří byli požádáni, aby zhodnotili účinnost politických zásahů, souhlasili s tím, že nejúčinnějším opatřením bude možnost 4 (4,08 na stupnici od 1 do 5). Patří sem spotřebitelské organizace (5,00), respondenti, kteří se označují za uživatele (4,22), oznámené subjekty (4,17), orgány dozoru nad trhem (5,00) a výrobci produktů s digitálními prvky (3,85), včetně malých a středních (4,05).

- **Účelnost právních předpisů a zjednodušení**

Tento návrh stanoví požadavky, které se budou vztahovat na výrobce softwaru a hardwaru. Je třeba zajistit právní jistotu a zabránit další roztříštěnosti trhu, pokud jde o požadavky týkající se produktů v oblasti kybernetické bezpečnosti na vnitřním trhu, což dokládá široká podpora horizontálního zásahu ze strany různých zúčastněných subjektů. Návrh minimalizuje regulační zátěž, kterou pro výrobce představuje několik aktů o bezpečnosti produktů. Sladění s novým právním rámcem znamená lepší fungování zásahu a jeho prosazování. Návrh zefektivňuje proces ochranných postupů tím, že před oznámením Komisi zapojí výrobce a členské státy. Velká část výrobců spadajících do oblasti působnosti návrhu je již s fungováním nového právního rámce obeznámena, což přispěje k jeho pochopení a provádění. V případě spotřebitelů a společností návrh podpoří důvěru v produkty s digitálními prvky.

- **Základní práva**

Očekává se, že všechny možnosti politiky do určité míry posílí ochranu základních práv a svobod, například soukromí, ochranu osobních údajů, svobodu podnikání a ochranu majetku nebo osobní důstojnosti a integrity. V tomto ohledu by byla nejúčinnější zejména upřednostňovaná možnost 4, která sestává z horizontálních regulačních zásahů a širokého

rozsahu politiky, neboť je pravděpodobnější, že pomůže snížit počet a závažnost incidentů, včetně porušení zabezpečení osobních údajů. To by rovněž zvýšilo právní jistotu a zajistilo rovné podmínky pro hospodářské subjekty, zvýšilo důvěru mezi uživateli a atraktivitu produktů EU obsahujících digitální prvky jako celku, a tím chránilo majetek a zlepšilo podmínky pro podnikání hospodářských subjektů.

Horizontální požadavky na kybernetickou bezpečnost by přispěly k bezpečnosti osobních údajů tím, že by chránily důvěrnost, integritu a dostupnost informací v produktech s digitálními prvky. Dodržování těchto požadavků usnadní splnění požadavku na bezpečnost zpracování osobních údajů podle nařízení (EU) 2016/679 o obecném nařízení o ochraně osobních údajů (GDPR)[12]. Návrh by zvýšil transparentnost a informovanost uživatelů, včetně těch, kteří by mohli mít méně dovedností v oblasti kybernetické bezpečnosti. Uživatelé by byli rovněž lépe informováni o rizicích, možnostech a omezeních produktů s digitálními prvky, což by jim umožnilo přijmout nezbytná preventivní a zmírňující opatření ke snížení zbytkových rizik.

4. ROZPOČTOVÉ DŮSLEDKY

Aby mohla Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) plnit úkoly přidělené podle tohoto nařízení, agentura ENISA bude muset přerozdělit zdroje ve výši přibližně 4,5 plného pracovního úvazku. Komise by musela přidělit 7 plných pracovních úvazků, aby mohla plnit své povinnosti související s prosazováním podle tohoto nařízení.

Podrobný přehled souvisejících nákladů je uveden ve „finančním výkazu“ souvisejícím s tímto návrhem.

5. OSTATNÍ PRVKY

• Plány provádění a způsob monitorování, hodnocení a podávání zpráv

Komise bude monitorovat provádění, použití a dodržování těchto nových ustanovení s cílem posoudit jejich účinnost. Nařízení bude vyžadovat hodnocení a přezkum ze strany Komise a předložení veřejné zprávy o hodnocení Evropskému parlamentu a Radě, a to do 36 měsíců ode dne použitelnosti a poté každé čtyři roky.

• Podrobné vysvětlení konkrétních ustanovení návrhu

Obecná ustanovení (kapitola I)

Toto navrhované nařízení stanoví a) pravidla pro uvádění produktů s digitálními prvky na trh s cílem zajistit kybernetickou bezpečnost těchto produktů; b) základní požadavky na navrhování, vývoj a výrobu produktů s digitálními prvky a povinnosti hospodářských subjektů v souvislosti s těmito produkty s ohledem na kybernetickou bezpečnost; c) základní požadavky na procesy řešení zranitelnosti zavedené výrobci s cílem zajistit kybernetickou bezpečnost produktů s digitálními prvky během celého životního cyklu a povinnosti hospodářských subjektů v souvislosti s těmito procesy; d) pravidla pro dozor nad trhem a prosazování výše uvedených pravidel a požadavků.

[12] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

Navrhované nařízení se použije na všechny produkty s digitálními prvky, jejichž zamýšlené a důvodně předpokládané použití zahrnuje přímé nebo nepřímé logické nebo fyzické datové připojení k zařízení nebo síti.

Navrhované nařízení se nepoužije na produkty s digitálními prvky spadající do oblasti působnosti nařízení (EU) 2017/745 [humánní zdravotnické prostředky a jejich příslušenství] a nařízení (EU) 2017/746 [humánní diagnostické zdravotnické prostředky *in vitro* a jejich příslušenství], neboť obě nařízení obsahují požadavky týkající se prostředků, včetně softwaru, a obecné povinnosti výrobců vztahující se na celý životní cyklus produktů, jakož i postupy posuzování shody. Z působnosti tohoto nařízení budou vyloučeny produkty s digitálními prvky, které byly certifikovány v souladu s nařízením 2018/1139 [vysoká a jednotná úroveň bezpečnosti civilního letectví], a také produkty, na něž se vztahuje nařízení (EU) 2019/2144 [o požadavcích pro schvalování typu motorových vozidel a jejich přípojných vozidel a systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla].

Kritické produkty s digitálními prvky podléhají zvláštním postupům posuzování shody a jsou rozděleny do třídy I a třídy II, jak je stanoveno v příloze III, s ohledem na úroveň jejich kybernetických bezpečnostních rizik, přičemž třída II představuje vyšší riziko. Produkt s digitálními prvky je považován za kritický, a proto je zařazen do přílohy III s ohledem na vliv možných zranitelností v oblasti kybernetické bezpečnosti, které jsou součástí produktu s digitálními prvky. Při určování kybernetických bezpečnostních rizik je zohledněna funkčnost produktu s digitálními prvky související s kybernetickou bezpečností a zamýšlené použití v citlivých prostředích, jako je mimo jiné průmyslové prostředí.

Komisi je rovněž svěřena pravomoc přijímat akty v přenesené pravomoci za účelem doplnění tohoto nařízení upřesněním kategorií vysoce kritických produktů s digitálními prvky, u nichž jsou výrobci povinni získat evropský certifikát kybernetické bezpečnosti v rámci evropského systému certifikace kybernetické bezpečnosti za účelem prokázání shody se základními požadavky stanovenými v příloze I nebo jejich částmi. Při určování těchto kategorií vysoce kritických produktů s digitálními prvky Komise zohlední úroveň kybernetického bezpečnostního rizika spojeného s kategorií produktů s digitálními prvky s ohledem na jedno nebo více kritérií, které se zvažují za účelem zařazení kritických produktů s digitálními prvky na seznam v příloze III, jakož i s ohledem na posouzení toho, zda zásadní subjekty druhu uvedeného v příloze [příloze I] směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] tuto kategorii produktů používají nebo z ní vycházejí, nebo zda budou mít pro činnosti těchto subjektů případný budoucí význam; nebo je relevantní pro odolnost celého dodavatelského řetězce produktů s digitálními prvky vůči událostem, které způsobují narušení.

Povinnosti hospodářských subjektů (kapitola II)

V návrhu jsou uvedeny povinnosti výrobců, dovozců a distributorů na základě referenčních ustanovení předpokládaných v rozhodnutí č. 768/2008/ES. Základní požadavky a povinnosti v oblasti kybernetické bezpečnosti vyžadují, aby všechny produkty s digitálními prvky byly dodávány na trh pouze tehdy, jestliže v případě, že jsou řádně dodány, patřičně instalovány, udržovány a používány k určenému účelu nebo za podmínek, které lze důvodně předpokládat, splňují základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení.

Základní požadavky a povinnosti by vedly výrobce k tomu, aby zohledňovali kybernetickou bezpečnost při navrhování, vývoji a výrobě produktů s digitálními prvky, aby při navrhování a vývoji svých produktů postupovali s náležitou péčí z hlediska bezpečnosti, byli transparentní v aspektech kybernetické bezpečnosti, o nichž je třeba informovat zákazníky, aby přiměřeným způsobem zajišťovali bezpečnostní podporu (aktualizace) a splňovali požadavky na řešení zranitelností.

Pro hospodářské subjekty, od výrobců až po distributory a dovozce, by byly stanoveny povinnosti týkající se uvádění produktů s digitálními prvky na trh, aby to odpovídalo jejich úloze a povinnostem v dodavatelském řetězci.

Shoda produktu s digitálními prvky (kapitola III)

Předpokládá se, že produkt s digitálními prvky, který je ve shodě s harmonizovanými normami nebo jejich částmi, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie*, je ve shodě se základními požadavky tohoto navrhovaného nařízení. Pokud harmonizované normy neexistují, jsou nedostatečné, nebo pokud v postupu normalizace dochází ke zbytečným průtahům, nebo pokud žádost Komise nebyla evropskými normalizačními organizacemi přijata, může Komise prostřednictvím prováděcích aktů přijmout obecné specifikace.

Kromě toho se předpokládá, že produkty s digitálními prvky, které byly certifikovány nebo pro něž bylo vydáno EU prohlášení o shodě nebo certifikát v rámci evropského systému certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881 a u nichž Komise prostřednictvím prováděcího aktu uvedla, že může předpokládat shodu s tímto nařízením, jsou ve shodě se základními požadavky tohoto nařízení nebo jejich částmi, pokud se na tyto požadavky vztahuje EU prohlášení o shodě nebo certifikát kybernetické bezpečnosti nebo jejich části.

S cílem zabránit nepřiměřené administrativní zátěži pro výrobce by Komise měla dále případně upřesnit, zda certifikát kybernetické bezpečnosti vydaný v rámci tohoto evropského systému certifikace kybernetické bezpečnosti ruší povinnost výrobců nechat provést posouzení shody třetí stranou, jak je pro odpovídající požadavky stanoveno v tomto nařízení.

Výrobce provede posouzení shody produktu s digitálními prvky a postupy řešení zranitelností, které zavedl za účelem prokázání shody se základními požadavky stanovenými v příloze I, a to jedním z postupů stanovených v příloze VI. Výrobci kritických produktů třídy I a II použijí příslušné moduly nezbytné pro dosažení souladu s předpisy. Výrobci kritického produktu třídy II musí do svého posuzování shody zapojit třetí stranu.

Oznamování subjektů posuzování shody (kapitola IV)

Řádné fungování oznámených subjektů je zásadní pro zajištění vysoké úrovně kybernetické bezpečnosti a pro důvěru všech zúčastněných stran v systém nového přístupu. Návrh proto v souladu s rozhodnutím č. 768/2008/ES stanoví požadavky pro vnitrostátní orgány odpovědné za subjekty posuzování shody (oznámené subjekty). Konečnou odpovědnost za jmenování a kontrolu oznámených subjektů ponechává na členských státech. Členské státy určí oznamující orgán odpovědný za vytvoření a provádění nezbytných postupů pro posuzování a oznamování subjektů posuzování shody a za kontrolu oznámených subjektů.

Dozor nad trhem a vymáhání práva (kapitola V)

V souladu s nařízením (EU) 2019/1020 vnitrostátní orgány dozoru nad trhem vykonávají na území daného členského státu dozor nad trhem. Členské státy se mohou rozhodnout, že určí některý stávající nebo nový orgán, který bude působit jako orgán dozoru nad trhem, včetně příslušných vnitrostátních orgánů zřízených podle článku [článku X] směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] nebo určených vnitrostátních orgánů pro certifikaci kybernetické bezpečnosti podle článku 58 nařízení (EU) 2019/881. Hospodářské subjekty se žádají, aby plně spolupracovaly s orgány dozoru nad trhem a dalšími příslušnými orgány.

Přenesené pravomoci a postupy projednávání ve výborech (kapitola VI)

S cílem zajistit, aby regulační rámec mohl být v případě potřeby upraven, se na Komisi přenáší pravomoc přijímat akty v souladu s článkem 290 SFEU, pokud jde o aktualizaci seznamu kritických produktů třídy I a II a upřesnění definic těchto produktů; upřesnění, zda je omezení nebo vyloučení nutné i pro produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie, která stanovují požadavky dosahující stejné úrovně ochrany jako toto nařízení; pověření certifikovat některé vysoce kritické produkty s digitálními prvky na základě kritérií stanovených v tomto nařízení; upřesnění minimálního obsahu EU prohlášení o shodě a doplnění prvků, které mají být obsaženy v technické dokumentaci.

Komisi je rovněž svěřena pravomoc přijímat prováděcí akty s cílem: specifikovat formát nebo prvky povinností podávat zprávy a softwarový kusovník; specifikovat evropské systémy certifikace kybernetické bezpečnosti, které lze použít k prokázání shody se základními požadavky nebo jejich částmi stanovenými v tomto nařízení; přijmout obecné specifikace; stanovit technické specifikace pro umístění označení CE; za výjimečných okolností, které odůvodňují okamžitý zásah v zájmu zachování řádného fungování vnitřního trhu, přijmout nápravná nebo omezující opatření na úrovni Unie.

Důvěrnost a sankce (kapitola VII)

Všechny strany, které uplatňují toto nařízení, respektují důvěrnost informací a údajů získaných při plnění svých úkolů a činností.

S cílem zajistit účinné vymáhání povinností stanovených v tomto nařízení by každý orgán dozoru nad trhem měl mít pravomoc ukládat správní pokuty nebo požadovat uložení správních pokut. Ve stejném duchu toto nařízení určuje maximální úrovně správních pokut, které by měly být stanoveny ve vnitrostátních právních předpisech za nesplnění povinností uvedených v tomto nařízení.

Přechodná a závěrečná ustanovení (kapitola VIII)

Aby měli výrobci, oznámené subjekty a členské státy čas přizpůsobit se novým požadavkům, bude navrhované nařízení použitelné [24 měsíců] po svém vstupu v platnost, s výjimkou povinnosti výrobců podávat zprávy, která by se použila od [12 měsíců] po datu vstupu v platnost.

2022/0272 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[1],

s ohledem na stanovisko Výboru regionů[2],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Je nezbytné zlepšit fungování vnitřního trhu stanovením jednotného právního rámce pro základní požadavky na kybernetickou bezpečnost při uvádění produktů s digitálními prvky na trh Unie. Měly by být řešeny dva hlavní problémy, které zvyšují náklady pro uživatele a pro společnost: nízká úroveň kybernetické bezpečnosti produktů s digitálními prvky, která se odráží v rozšířené zranitelnosti a nedostatečném a nekonzistentním poskytování bezpečnostních aktualizací k jejímu řešení, a nedostatečné chápání informací a přístup k informacím ze strany uživatelů, což jim znemožňuje vybrat si produkty s odpovídajícími kybernetickými bezpečnostními vlastnostmi nebo je používat bezpečným způsobem.

(2) Cílem tohoto nařízení je stanovit mezní podmínky pro vývoj bezpečných produktů s digitálními prvky tím, že bude zajištěno, aby hardwarové a softwarové produkty byly uváděny na trh s méně zranitelnostmi a aby výrobci brali vážně bezpečnost v průběhu celého životního cyklu produktu. Má rovněž vytvořit podmínky umožňující uživatelům, aby při výběru a používání produktů s digitálními prvky zohlednili kybernetickou bezpečnost.

(3) Příslušné právní předpisy Unie, které jsou v současné době v platnosti, zahrnují několik souborů horizontálních pravidel, která se z různých úhlů zabývají určitými aspekty souvisejícími s kybernetickou bezpečností, včetně opatření ke zlepšení bezpečnosti digitálního dodavatelského řetězce. Stávající právní předpisy Unie týkající se kybernetické bezpečnosti, včetně [směrnice XXX/XXXX (o bezpečnosti sítí a

[1] Úř. věst. C , , s. .
[2] Úř. věst. C , , s. .

informací 2)] a nařízení Evropského parlamentu a Rady (EU) 2019/881[3], se však přímo nevztahují na povinné požadavky na bezpečnost produktů s digitálními prvky.

(4) Ačkoli se stávající právní předpisy Unie vztahují na určité produkty s digitálními prvky, neexistuje žádný horizontální regulační rámec Unie, který by stanovil komplexní požadavky na kybernetickou bezpečnost pro všechny produkty s digitálními prvky. Různé akty a iniciativy, které byly dosud přijaty na úrovni Unie a na vnitrostátní úrovni, řeší zjištěné problémy a rizika související s kybernetickou bezpečností pouze částečně, vytvářejí v rámci vnitřního trhu právní nejednotnost, čímž se zvyšuje právní nejistota jak pro výrobce, tak pro uživatele těchto produktů a zvyšuje se zbytečná zátěž pro společnosti, pokud jde o plnění řady požadavků na podobné druhy produktů. Kybernetická bezpečnost těchto produktů má obzvláště silný přeshraniční rozměr, neboť produkty vyrobené v jedné zemi jsou často používány organizacemi a spotřebiteli na celém vnitřním trhu. Proto je nezbytné regulovat tuto oblast na úrovni Unie. Regulační prostředí Unie by mělo být harmonizováno zavedením požadavků na kybernetickou bezpečnost produktů s digitálními prvky. Kromě toho by měla být zajištěna právní jistota pro hospodářské subjekty a uživatele v celé Unii, jakož i lepší harmonizace jednotného trhu, přičemž pro subjekty, které chtějí vstoupit na trh Unie, by se vytvořily přijatelné podmínky.

(5) Na úrovni Unie vyzvaly různé programové a politické dokumenty, například Strategie kybernetické bezpečnosti EU pro digitální dekádu[4], závěry Rady ze dne 2. prosince 2020 a 23. května 2022 nebo usnesení Evropského parlamentu ze dne 10. června 2021[5], k zavedení zvláštních požadavků Unie na kybernetickou bezpečnost pro digitální nebo propojené produkty, přičemž několik zemí po celém světě zavedlo opatření k řešení této otázky z vlastního podnětu. V závěrečné zprávě Konference o budoucnosti Evropy[6] občané požadovali „větší roli EU v boji proti hrozbám kybernetické bezpečnosti“.

(6) Aby se zvýšila celková úroveň kybernetické bezpečnosti všech produktů s digitálními prvky uváděných na vnitřní trh, je nezbytné zavést pro tyto produkty základní požadavky na kybernetickou bezpečnost, které jsou horizontálně orientované a technologicky neutrální.

(7) Za určitých podmínek mohou všechny produkty s digitálními prvky začleněné do většího elektronického informačního systému nebo s ním spojené sloužit jako útočný prostředek pro nepřátelské subjekty. V důsledku toho může i hardware a software, které jsou považovány za méně kritické, usnadnit prvotní ohrožení zařízení nebo sítě, což umožní nepřátelským subjektům získat výsadní přístup k systému nebo se pohybovat napříč systémy. Výrobci by proto měli zajistit, aby všechny propojitelné produkty s digitálními prvky byly navrhovány a vyvíjeny v souladu se základními požadavky stanovenými v tomto nařízení. Patří sem jak produkty, které lze fyzicky

---

3 Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=JOIN:2020:18:FIN.

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_CS.html.

6 *Konference o budoucnosti Evropy – zpráva o konečném výsledku*, květen 2022, návrh 28(2). Konference se konala v době od dubna 2021 do května 2022. Jednalo se o jedinečný test poradní demokracie vedený občany na celoevropské úrovni, do něhož byly zapojeny tisíce evropských občanů, jakož i politických aktérů, sociálních partnerů, zástupců občanské společnosti a klíčových zúčastněných stran.

připojit prostřednictvím hardwarových rozhraní, tak produkty, které jsou propojeny logicky, například prostřednictvím síťových zásuvek, vedení, souborů, rozhraní pro programování aplikací nebo jakýchkoli jiných druhů softwarového rozhraní. Vzhledem k tomu, že kybernetické hrozby se mohou před dosažením určitého cíle šířit prostřednictvím různých produktů s digitálními prvky, například zřetězením více zneužití zranitelnosti, měli by výrobci zajistit kybernetickou bezpečnost i u těch produktů, které jsou propojeny s jinými zařízeními nebo sítěmi pouze nepřímo.

(8) Stanovením požadavků na kybernetickou bezpečnost pro uvádění produktů s digitálními prvky na trh se zvýší kybernetická bezpečnost těchto produktů pro spotřebitele i pro podniky. Zahrnuje to rovněž požadavky na uvádění na trh v případě spotřebních produktů s digitálními prvky určených pro zranitelné spotřebitele, například hraček a dětských chůviček.

(9) Toto nařízení zajišťuje vysokou úroveň kybernetické bezpečnosti produktů s digitálními prvky. Neupravuje služby, například Software jako služba (SaaS), s výjimkou řešení pro zpracování dat na dálku týkajících se produktu s digitálními prvky, čímž se rozumí jakékoli zpracování dat na dálku, pro něž je software navržen a vyvinut výrobcem daného produktu nebo za nějž je tento výrobce odpovědný, a pokud by neexistoval, nebylo by možné, aby tento produkt s digitálními prvky plnil některou ze svých funkcí. [Směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] zavádí požadavky na kybernetickou bezpečnost a hlášení incidentů pro zásadní a důležité subjekty, například kritickou infrastrukturu, s cílem zvýšit odolnost služeb, které poskytují. [Směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] se vztahuje na služby cloud computingu a modely cloudových služeb, například SaaS. Do oblasti působnosti uvedené směrnice spadají všechny subjekty poskytující služby cloud computingu v Unii, které dosahují prahové hodnoty pro střední podniky nebo ji překračují.

(10) Aby nedošlo k narušení inovací nebo výzkumu, nemělo by se toto nařízení vztahovat na bezplatný software s otevřeným zdrojovým kódem vyvinutý nebo dodávaný mimo rámec obchodní činnosti. To platí zejména pro software, včetně jeho zdrojového kódu a upravených verzí, který je otevřeně sdílený a volně přístupný, použitelný, upravitelný a dále distribuovatelný. V kontextu softwaru by se obchodní činnost mohla vyznačovat nejen stanovením ceny za produkt, ale také stanovením ceny za technické podpůrné služby, poskytnutím softwarové platformy, jejímž prostřednictvím výrobce zpeněžuje jiné služby, nebo použitím osobních údajů z jiných důvodů, než je výlučně zlepšení bezpečnosti, kompatibility nebo interoperability softwaru.

(11) Bezpečný internet je nezbytný pro fungování kritických infrastruktur a pro společnost jako celek. [Směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] má za cíl zajistit vysokou úroveň kybernetické bezpečnosti služeb poskytovaných zásadními a důležitými subjekty, včetně poskytovatelů digitální infrastruktury, kteří podporují klíčové funkce otevřeného internetu, zajišťují přístup k internetu a internetové služby. Je proto důležité, aby produkty s digitálními prvky, které poskytovatelé digitální infrastruktury potřebují k zajištění fungování internetu, byly vyvíjeny bezpečným způsobem a aby splňovaly zavedené normy bezpečnosti internetu. Cílem tohoto nařízení, které se vztahuje na všechny propojitelné hardwarové a softwarové produkty, je rovněž usnadnit dodržování požadavků dodavatelského řetězce ze strany poskytovatelů digitální infrastruktury podle [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] tím, že zajistí, aby produkty s digitálními prvky, které používají pro poskytování svých služeb, byly vyvíjeny bezpečným způsobem a aby měli přístup k včasným bezpečnostním aktualizacím těchto produktů.

(12) Nařízení Evropského parlamentu a Rady (EU) 2017/745[7] stanoví pravidla pro zdravotnické prostředky a nařízení Evropského parlamentu a Rady (EU) 2017/746[8] stanoví pravidla pro diagnostické zdravotnické prostředky *in vitro*. Obě nařízení řeší kybernetická bezpečnostní rizika a uplatňují konkrétní přístupy, kterými se toto nařízení rovněž zabývá. Přesněji řečeno, nařízení (EU) 2017/745 a nařízení (EU) 2017/746 stanoví základní požadavky na zdravotnické prostředky, které fungují prostřednictvím elektronického systému nebo které jsou samy softwarem. Tato nařízení se rovněž vztahují na určitý nevestavěný software a na přístup zohledňující celý životní cyklus. Uvedené požadavky ukládají výrobcům, aby vyvíjeli a vytvářeli své produkty uplatňováním zásad řízení rizik a stanovením požadavků týkajících se opatření v oblasti bezpečnosti IT, jakož i odpovídajících postupů posuzování shody. Kromě toho jsou od prosince 2019 zavedeny zvláštní pokyny týkající se kybernetické bezpečnosti zdravotnických prostředků, které výrobcům zdravotnických prostředků, včetně diagnostických prostředků *in vitro*, poskytují informace, jak splnit všechny příslušné základní požadavky přílohy I uvedených nařízení, pokud jde o kybernetickou bezpečnost[9]. Na produkty s digitálními prvky, na něž se vztahuje jedno z těchto nařízení, by se proto toto nařízení nemělo vztahovat.

(13) Nařízení Evropského parlamentu a Rady (EU) 2019/2144[10] stanoví požadavky na schvalování typů vozidel a jejich systémů a součástí, kterým se zavádějí určité požadavky na kybernetickou bezpečnost, včetně požadavků na provoz certifikovaného systému řízení kybernetické bezpečnosti, na aktualizace softwaru týkající se politik a postupů organizací pro kybernetická rizika, která souvisejí s celým životním cyklem vozidel, zařízení a služeb v souladu s platnými předpisy OSN o technických specifikacích a kybernetické bezpečnosti[11], přičemž stanoví konkrétní postupy posuzování shody. V oblasti letectví je hlavním cílem nařízení Evropského parlamentu a Rady (EU) 2018/1139[12] zavést a udržovat vysokou a jednotnou úroveň bezpečnosti civilního letectví v Unii. Vytváří rámec pro základní požadavky na letovou způsobilost

---

7 Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, změně směrnice 2001/83/ES, nařízení (ES) č. 178/2002 a nařízení (ES) č. 1223/2009 a o zrušení směrnic Rady 90/385/EHS a 93/42/EHS (Úř. věst. L 117, 5.5.2017, s. 1).

8 Nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích in vitro a o zrušení směrnice 98/79/ES a rozhodnutí Komise 2010/227/EU (Úř. věst. L 117, 5.5.2017, s. 176).

9 Koordinační skupina pro zdravotnické prostředky 2019-16, schválená Koordinační skupinou pro zdravotnické prostředky zřízenou článkem 103 nařízení (EU) 2017/745.

10 Nařízení Evropského parlamentu a Rady (EU) 2019/2144 ze dne 27. listopadu 2019 o požadavcích pro schvalování typu motorových vozidel a jejich přípojných vozidel a systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla z hlediska obecné bezpečnosti a ochrany cestujících ve vozidle a zranitelných účastníků silničního provozu, o změně nařízení Evropského parlamentu a Rady (EU) 2018/858 a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nařízení Komise (ES) č. 631/2009, (EU) č. 406/2010, (EU) č. 672/2010, (EU) č. 1003/2010, (EU) č. 1005/2010, (EU) č. 1008/2010, (EU) č. 1009/2010, (EU) č. 19/2011, (EU) č. 109/2011, (EU) č. 458/2011, (EU) č. 65/2012, (EU) č. 130/2012, (EU) č. 347/2012, (EU) č. 351/2012, (EU) č. 1230/2012 a (EU) 2015/166 (Úř. věst. L 325, 16.12.2019, s. 1).

11 Předpis OSN č. 155 – Jednotná ustanovení pro schvalování vozidel z hlediska kybernetické bezpečnosti a systému řízení kybernetické bezpečnosti [2021/387].

12 Nařízení Evropského parlamentu a Rady (EU) 2018/1139 ze dne 4. července 2018 o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví, kterým se mění nařízení (ES) č. 2111/2005, (ES) č. 1008/2008, (EU) č. 996/2010, (EU) č. 376/2014 a směrnice Evropského parlamentu a Rady 2014/30/EU a 2014/53/EU a kterým se zrušuje nařízení Evropského parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nařízení Rady (EHS) č. 3922/91 (Úř. věst. L 212, 22.8.2018, s. 1).

leteckých výrobků, dílů a vybavení, včetně softwaru, který zohledňuje povinnosti ochrany před hrozbami pro informační bezpečnost. Na produkty s digitálními prvky, na něž se vztahuje nařízení (EU) 2019/2144, a na produkty certifikované v souladu s nařízením (EU) 2018/1139 se proto nevztahují základní požadavky a postupy posuzování shody stanovené v tomto nařízení. Postup certifikace podle nařízení (EU) 2018/1139 zajišťuje úroveň jistoty, kterou má toto nařízení za cíl.

(14) Toto nařízení stanoví horizontální pravidla kybernetické bezpečnosti, která nejsou specifická pro odvětví nebo určité produkty s digitálními prvky. Nicméně by mohla být zavedena odvětvová pravidla nebo pravidla Unie specifická pro určité produkty, která stanoví požadavky týkající se všech nebo některých rizik, na něž se vztahují základní požadavky stanovené tímto nařízením. V těchto případech může být použití tohoto nařízení na produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie, která stanoví požadavky řešící všechna nebo některá rizika, pro něž platí základní požadavky stanovené v příloze I tohoto nařízení, omezeno nebo vyloučeno, pokud je takové omezení nebo vyloučení v souladu s celkovým regulačním rámcem platným pro tyto produkty a pokud odvětvová pravidla dosahují stejné úrovně ochrany, jakou stanoví toto nařízení. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci za účelem změny tohoto nařízení tím, že tyto produkty a pravidla určí. V případě stávajících právních předpisů Unie, na něž by se tato omezení nebo vyloučení měla vztahovat, obsahuje toto nařízení zvláštní ustanovení, která objasňují jeho vztah k uvedeným právním předpisům Unie.

(15) Nařízení v přenesené pravomoci (EU) 2022/30 stanoví, že základní požadavky uvedené v čl. 3 odst. 3 písm. d) (nepříznivý vliv na síť a zneužití zdrojů sítě), písm. e) (osobní údaje a soukromí) a písm. f) (podvod) směrnice 2014/53/EU se vztahují na určitá rádiová zařízení. [Prováděcí rozhodnutí Komise XXX/2022 o žádosti o normalizaci podané evropským normalizačním organizacím] stanoví požadavky na vypracování konkrétních norem, které dále upřesňují, jak by měly být tyto tři základní požadavky řešeny. Základní požadavky stanovené tímto nařízením zahrnují všechny prvky základních požadavků uvedených v čl. 3 odst. 3 písm. d), e) a f) směrnice 2014/53/EU. Základní požadavky stanovené v tomto nařízení jsou dále v souladu s cíli požadavků týkajících se konkrétních norem obsažených v uvedené žádosti o normalizaci. Pokud tedy Komise zruší nebo změní nařízení v přenesené pravomoci (EU) 2022/30 s tím důsledkem, že se přestane uplatňovat na některé produkty, na něž se vztahuje toto nařízení, měla by Komise a evropské normalizační organizace při přípravě a vypracovávání harmonizovaných norem s cílem usnadnit provádění tohoto nařízení zohlednit normalizační práci provedenou v souvislosti s prováděcím rozhodnutím Komise C(2022)5637 o žádosti o normalizaci pro nařízení v přenesené pravomoci 2022/30 týkající se směrnice o rádiových zařízeních.

(16) Směrnice 85/374/EHS[13] toto nařízení doplňuje. Uvedená směrnice stanoví pravidla odpovědnosti za vadné produkty, aby poškozené osoby mohly požadovat náhradu škody, pokud byla tato škoda způsobena vadnými produkty. Zavádí zásadu, podle níž je výrobce produktu odpovědný za škody způsobené nedostatečnou bezpečností jeho produktu, a to bez ohledu na zavinění („objektivní odpovědnost“). Pokud taková nedostatečná bezpečnost spočívá v neexistenci bezpečnostních aktualizací po uvedení produktu na trh a vznikne tím škoda, mohla by být uplatněna odpovědnost výrobce.

[13] Směrnice Rady 85/374/EHS ze dne 25. července 1985 o sbližování právních a správních předpisů členských států týkajících se odpovědnosti za vadné výrobky (Úř. věst. L 210, 7.8.1985).

Povinnosti výrobců, které se týkají poskytování těchto bezpečnostních aktualizací, by měly být stanoveny v tomto nařízení.

(17) Tímto nařízením by nemělo být dotčeno nařízení Evropského parlamentu a Rady (EU) 2016/679[14], včetně ustanovení o zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu s uvedeným nařízením v případě operací zpracování prováděných správci a zpracovateli. Tyto operace by mohly být začleněny do produktu s digitálními prvky. Klíčovými prvky nařízení (EU) 2016/679 jsou záměrná a standardní ochrana osobních údajů a kybernetická bezpečnost obecně. Tím, že chrání spotřebitele a organizace před kybernetickými bezpečnostními riziky, mají základní požadavky na kybernetickou bezpečnost stanovené v tomto nařízení rovněž přispět ke zvýšení ochrany osobních údajů a soukromí jednotlivců. Synergie v oblasti normalizace i certifikace týkající se aspektů kybernetické bezpečnosti by měly být zohledněny prostřednictvím spolupráce mezi Komisí, evropskými normalizačními organizacemi, Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA), Evropským sborem pro ochranu osobních údajů (EDPB) zřízeným nařízením (EU) 2016/679 a vnitrostátními dozorovými úřady dohlížejícími na ochranu údajů. Synergie mezi tímto nařízením a právními předpisy Unie v oblasti ochrany údajů by měly být rovněž vytvořeny v oblasti dozoru nad trhem a vymáhání práva. Za tímto účelem by vnitrostátní orgány dozoru nad trhem jmenované podle tohoto nařízení měly spolupracovat s orgány vykonávajícími dohled nad právními předpisy Unie v oblasti ochrany údajů. Měly by rovněž mít přístup k informacím, které jsou důležité pro plnění jejich úkolů.

(18) Pokud jejich produkty spadají do oblasti působnosti tohoto nařízení, měli by vydavatelé evropských peněženek digitální identity podle článku [čl. 6a odst. 2 nařízení (EU) č. 910/2014 ve znění návrhu nařízení, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu], splňovat jak horizontální základní požadavky stanovené tímto nařízením, tak konkrétní bezpečnostní požadavky stanovené v článku [článek 6a nařízení (EU) č. 910/2014 ve znění návrhu nařízení, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu]. Aby se usnadnilo dodržování požadavků, měli by být vydavatelé peněženek schopni prokázat soulad evropských peněženek digitální identity s požadavky stanovenými v obou aktech, a to prostřednictvím certifikace svých produktů v rámci evropského systému certifikace kybernetické bezpečnosti zřízeného podle nařízení (EU) 2019/881 a pro něž Komise stanovila prostřednictvím prováděcího aktu předpoklad shody pro toto nařízení, pokud se certifikát nebo jeho části na tyto požadavky vztahují.

(19) Některé úkoly stanovené v tomto nařízení by měla provádět agentura ENISA v souladu s čl. 3 odst. 2 nařízení (EU) 2019/881. Agentura ENISA by měla zejména dostávat oznámení od výrobců o aktivně zneužívaných zranitelnostech obsažených v produktech s digitálními prvky, jakož i o incidentech, které mají dopad na bezpečnost těchto produktů. Agentura ENISA by měla tato oznámení rovněž předat příslušným skupinám pro reakci na počítačové bezpečnostní incidenty (CSIRT) nebo příslušným jednotným kontaktním místům členských států určených v souladu s článkem [článek X] směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] a informovat

[14] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

příslušné orgány dozoru nad trhem o oznámené zranitelnosti. Na základě shromážděných informací by agentura ENISA měla každé dva roky vypracovat technickou zprávu o nových trendech týkajících se kybernetických bezpečnostních rizik u produktů s digitálními prvky a předložit ji skupině pro spolupráci podle směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)]. Kromě toho by agentura ENISA s ohledem na své odborné znalosti a mandát měla být schopna podporovat proces provádění tohoto nařízení. Zejména by měla mít možnost navrhovat společné činnosti, které mají provádět orgány dozoru nad trhem na základě údajů nebo informací o možném nesouladu produktů s digitálními prvky s tímto nařízením v některých členských státech, nebo určit kategorie produktů, pro něž by měly být organizovány souběžné koordinované kontrolní činnosti. Za výjimečných okolností by agentura ENISA měla mít na žádost Komise možnost provádět hodnocení konkrétních produktů s digitálními prvky, které představují významné kybernetické bezpečnostní riziko, je-li pro zachování řádného fungování vnitřního trhu nutný okamžitý zásah.

(20) Produkty s digitálními prvky by měly být opatřeny označením CE, které vyjadřuje jejich shodu s tímto nařízením, aby se mohly volně pohybovat na vnitřním trhu. Členské státy by neměly vytvářet neodůvodněné překážky uvádění na trh u produktů s digitálními prvky, které jsou v souladu s požadavky stanovenými v tomto nařízení a jsou opatřeny označením CE.

(21) Aby bylo zajištěno, že výrobci mohou uvolnit software pro účely testování před tím, než podrobí své produkty posouzení shody, členské státy by neměly bránit zpřístupnění nedokončeného softwaru, například alfa verzí, beta verzí nebo kandidátů na vydání, pokud je daná verze k dispozici pouze po dobu nezbytnou k jejímu testování a získání zpětné vazby. Výrobci by měli zajistit, aby software zpřístupněný za těchto podmínek byl vydán pouze na základě posouzení rizik a aby v co největší míře splňoval bezpečnostní požadavky týkající se vlastností produktů s digitálními prvky, které ukládá toto nařízení. Výrobci by rovněž měli v co největší míře uplatňovat požadavky na řešení zranitelnosti. Výrobci by neměli nutit uživatele k přechodu na verze, které jsou vydávány pouze pro účely testování.

(22) Aby se zajistilo, že produkty s digitálními prvky nepředstavují při uvedení na trh kybernetická bezpečnostní rizika pro osoby a organizace, měly by být pro tyto produkty stanoveny základní požadavky. Pokud jsou produkty následně upraveny, ať už fyzickým, nebo digitálním zásahem, a to způsobem, který výrobce nemohl předvídat a který by mohl znamenat, že produkty již nesplňují příslušné základní požadavky, považuje se taková úprava za podstatnou. Například aktualizace nebo opravy softwaru by mohly být postaveny na roveň operacím údržby, pokud neupravují produkt, který již byl uveden na trh, takovým způsobem, že může být ovlivněn soulad s příslušnými požadavky, nebo že zamýšlené použití, pro které byl produkt posouzen, může být změněno. Stejně jako v případě fyzických oprav nebo změn by měl být produkt s digitálními prvky považován za podstatně změněný tím, že dojde ke změně softwaru, pokud aktualizace softwaru mění původní zamýšlené funkce, druh nebo výkon produktu a tyto změny nebyly v původním posouzení rizik předvídány nebo se změnila povaha nebezpečí nebo se v důsledku aktualizace softwaru zvýšila úroveň rizika.

(23) V souladu s obecně zavedeným pojmem podstatné změny u produktů, na něž se vztahují harmonizační právní předpisy Unie, je vždy vhodné, pokud dojde k podstatné změně, která může ovlivnit soulad produktu s tímto nařízením, nebo pokud se změní zamýšlený účel daného produktu, aby byl u produktu s digitálními prvky ověřen

soulad s předpisy a aby byl případně podroben novému posouzení shody. Pokud výrobce provádí posouzení shody za účasti třetí strany, měly by být v příslušném případě třetí straně oznámeny změny, které by mohly vést k podstatným změnám.

(24) Renovace, údržba a opravy produktu s digitálními prvky, jak jsou definovány v nařízení [nařízení o ekodesignu], nemusí nutně vést k podstatné změně produktu, například pokud se nezmění zamýšlené použití a funkce a úroveň rizika zůstane nedotčena. Modernizace produktu výrobcem by však mohla vést ke změnám v návrhu a vývoji produktu, a mohla by proto ovlivnit zamýšlené použití a soulad produktu s požadavky stanovenými v tomto nařízení.

(25) Produkty s digitálními prvky by měly být považovány za kritické, pokud může být negativní dopad zneužití zranitelností kybernetické bezpečnosti produktu závažný, mimo jiné v důsledku funkcí souvisejících s kybernetickou bezpečností nebo zamýšleného použití. Zranitelnosti produktů s digitálními prvky, které mají funkce související s kybernetickou bezpečností, například zabezpečené prvky, mohou vést k šíření bezpečnostních problémů v celém dodavatelském řetězci. Závažnost dopadu kybernetického bezpečnostního incidentu se může rovněž zvýšit s ohledem na zamýšlené použití produktu, například v průmyslovém prostředí nebo v souvislosti se zásadním subjektem druhu uvedeného v příloze [příloze I] směrnice [XXX/XXXX (o bezpečnosti sítí a informací 2)], nebo při výkonu kritických nebo citlivých funkcí, například zpracování osobních údajů.

(26) Kritické produkty s digitálními prvky by měly podléhat přísnějším postupům posuzování shody, přičemž by měl být zachován přiměřený přístup. Za tímto účelem by kritické produkty s digitálními prvky měly být rozděleny do dvou tříd, které odrážejí úroveň kybernetických bezpečnostních rizik spojených s těmito kategoriemi produktů. Možný kybernetický incident týkající se produktů třídy II by mohl vést k větším negativním dopadům než incident týkající se produktů třídy I, například vzhledem k povaze jejich funkce související s kybernetickou bezpečností nebo vzhledem k zamýšlenému použití v citlivých prostředích, a měl by proto být předmětem přísnějšího postupu posuzování shody.

(27) Produkty, které mají hlavní funkci druhu uvedeného v příloze III tohoto nařízení, by se měly považovat za kategorie kritických produktů s digitálními prvky uvedenými v příloze III tohoto nařízení. Například příloha III tohoto nařízení uvádí produkty, které jsou definovány svou základní funkcí jako mikroprocesory pro všeobecné účely ve třídě II. V důsledku toho podléhají mikroprocesory pro všeobecné účely povinnému posouzení shody třetí stranou. Tak tomu není v případě jiných produktů, které nejsou výslovně uvedeny v příloze III tohoto nařízení a jejichž součástí může být mikroprocesor pro všeobecné účely. Komise by měla [do 12 měsíců od vstupu tohoto nařízení v platnost] přijmout akty v přenesené pravomoci za účelem upřesnění definic kategorií produktů spadajících do třídy I a třídy II uvedených v příloze III.

(28) Toto nařízení řeší kybernetická bezpečnostní rizika cíleným způsobem. Produkty s digitálními prvky však mohou představovat jiná bezpečnostní rizika, která nesouvisejí s kybernetickou bezpečností. Tato rizika by měla být i nadále upravena dalšími příslušnými právními předpisy Unie týkajícími se produktů. Pokud nejsou použitelné žádné jiné harmonizační právní předpisy Unie, měla by se řídit nařízením [nařízení o obecné bezpečnosti výrobků]. S ohledem na cílenou povahu tohoto nařízení by se proto odchylně od čl. 2 odst. 1 třetího pododstavce písm. b) nařízení [nařízení o obecné bezpečnosti výrobků] měly použít na produkty s digitálními prvky kapitola III oddílu 1, kapitoly V a VII a kapitoly IX až XI nařízení [nařízení o obecné bezpečnosti

výrobků], pokud jde o bezpečnostní rizika, na něž se toto nařízení nevztahuje, jestliže tyto produkty nejsou předmětem konkrétních požadavků uložených jinými harmonizačními právními předpisy Unie ve smyslu [čl. 3 bodu 25 nařízení o obecné bezpečnosti výrobků].

(29) Produkty s digitálními prvky klasifikované jako vysoce rizikové systémy UI podle článku 6 nařízení[15] [nařízení o UI], které spadají do oblasti působnosti tohoto nařízení, by měly splňovat základní požadavky stanovené v tomto nařízení. Pokud tyto vysoce rizikové systémy UI splňují základní požadavky tohoto nařízení, mělo by se mít za to, že splňují požadavky na kybernetickou bezpečnost stanovené v článku [článku 15] nařízení [nařízení o UI], pokud se na tyto požadavky vztahuje EU prohlášení o shodě nebo jeho části vydané podle tohoto nařízení. Pokud jde o postupy posuzování shody týkající se základních požadavků na kybernetickou bezpečnost produktu s digitálními prvky, na něž se vztahuje toto nařízení a který je klasifikován jako vysoce rizikový systém UI, měla by se zpravidla namísto příslušných ustanovení tohoto nařízení použít příslušná ustanovení článku 43 nařízení [nařízení o UI]. Toto pravidlo by však nemělo vést ke snížení potřebné míry jistoty u kritických produktů s digitálními prvky, na něž se vztahuje toto nařízení. Odchylně od tohoto pravidla by se proto vysoce rizikové systémy UI, které spadají do oblasti působnosti nařízení [nařízení o UI] a jsou rovněž považovány za kritické produkty s digitálními prvky podle tohoto nařízení, na něž se vztahuje postup posuzování shody založený na vnitřní kontrole podle přílohy VI nařízení [nařízení o UI], měly řídit ustanoveními tohoto nařízení o posuzování shody, pokud jde o základní požadavky tohoto nařízení. V tomto případě by se na všechny ostatní aspekty, na něž se nařízení [nařízení o UI] vztahuje, měla použít příslušná ustanovení o posuzování shody, která jsou založena na vnitřní kontrole stanovené v příloze VI nařízení [nařízení o UI].

(30) Strojní výrobky spadající do oblasti působnosti nařízení [návrh nařízení o strojních zařízeních], které jsou produkty s digitálními prvky ve smyslu tohoto nařízení a pro něž bylo na základě tohoto nařízení vydáno prohlášení o shodě, by měly být považovány za produkty ve shodě se základními požadavky na ochranu zdraví a bezpečnost stanovenými v [bodech 1.1.9 a 1.2.1 přílohy III] nařízení [návrh nařízení o strojních zařízeních], pokud jde o ochranu proti poškození a bezpečnost a spolehlivost kontrolních systémů, jestliže je soulad s těmito požadavky prokázán EU prohlášením o shodě vydaným podle tohoto nařízení.

(31) Nařízení [návrh nařízení o evropském prostoru pro zdravotní data] doplňuje základní požadavky stanovené v tomto nařízení. Systémy elektronických zdravotních záznamů spadající do oblasti působnosti nařízení [návrh nařízení o evropském prostoru pro zdravotní data], které jsou produkty s digitálními prvky ve smyslu tohoto nařízení, by proto měly rovněž splňovat základní požadavky stanovené v tomto nařízení. Jejich výrobci by měli prokázat shodu, jak požaduje nařízení [návrh nařízení o evropském prostoru pro zdravotní data]. Pro usnadnění souladu mohou výrobci vypracovat jedinou technickou dokumentaci obsahující prvky požadované oběma právními akty. Jelikož se toto nařízení nevztahuje na služby SaaS jako takové, systémy elektronických zdravotních záznamů nabízené prostřednictvím modelu udělování licencí a poskytování služeb SaaS nespadají do oblasti působnosti tohoto nařízení. Podobně nespadají do oblasti působnosti tohoto nařízení systémy elektronických

[15] Nařízení [nařízení o UI].

zdravotních záznamů, které jsou vyvíjeny a používány interně, neboť nejsou uváděny na trh.

(32) Aby bylo zajištěno, že produkty s digitálními prvky jsou bezpečné jak v době jejich uvedení na trh, tak během celého jejich životního cyklu, je nezbytné stanovit základní požadavky na řešení zranitelnosti a základní požadavky na kybernetickou bezpečnost týkající se vlastností produktů s digitálními prvky. Výrobci by měli splňovat všechny základní požadavky týkající se řešení zranitelnosti a zajistit, aby všechny jejich produkty byly dodávány bez jakýchkoli známých zneužitelných zranitelností, měli by však určit, které další základní požadavky týkající se vlastností produktu jsou pro dotčený druh produktu relevantní. Za tímto účelem by výrobci měli provést posouzení kybernetických bezpečnostních rizik spojených s produktem s digitálními prvky s cílem určit příslušná rizika a příslušné základní požadavky a náležitě uplatňovat vhodné harmonizované normy nebo obecné specifikace.

(33) V zájmu zlepšení bezpečnosti produktů s digitálními prvky uváděných na vnitřní trh je nezbytné stanovit základní požadavky. Těmito základními požadavky by neměla být dotčena koordinovaná posouzení rizik kritických dodavatelských řetězců na úrovni EU stanovená [článkem X] směrnice [XXX/XXXX (o bezpečnosti sítí a informací 2)][16], která zohledňují technické i případně netechnické rizikové faktory, například nepatřičný vliv třetí země na dodavatele. Dále by neměly být dotčeny výsady členských států stanovit dodatečné požadavky, které zohledňují netechnické faktory za účelem zajištění vysoké úrovně odolnosti, včetně požadavků stanovených v doporučení (EU) 2019/534, v posouzení rizik kybernetické bezpečnosti sítí 5G koordinovaném na úrovni Unie a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci v oblasti bezpečnosti sítí a informací podle [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)].

(34) S cílem zajistit, aby vnitrostátním týmům CSIRT a jednotnému kontaktnímu místu určenému v souladu s článkem [článek X] směrnice [směrnice XX/XXXX (o bezpečnosti sítí a informací 2)] byly poskytovány informace nezbytné k plnění jejich úkolů a zvýšení celkové úrovně kybernetické bezpečnosti zásadních a důležitých subjektů, a aby se zajistilo účinné fungování orgánů dozoru nad trhem, měli by výrobci produktů s digitálními prvky oznamovat agentuře ENISA zranitelnosti, které jsou aktivně zneužívány. Vzhledem k tomu, že většina produktů s digitálními prvky je uváděna na trh na celém vnitřním trhu, jakákoli zneužívaná zranitelnost produktu s digitálními prvky by měla být považována za hrozbu pro fungování vnitřního trhu. Výrobci by rovněž měli zvážit zveřejnění opravených zranitelností v evropské databázi zranitelností zřízené podle směrnice [směrnice XX/XXXX (o bezpečnosti sítí a informací 2)] a spravované agenturou ENISA nebo v jakékoli jiné veřejně přístupné databázi zranitelností.

(35) Výrobci by rovněž měli agentuře ENISA hlásit každý incident, který má dopad na bezpečnost produktu s digitálními prvky. Bez ohledu na povinnosti podávat zprávy o incidentech stanovené ve směrnici [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] je pro zásadní a důležité subjekty klíčové, aby agentura ENISA, jednotná kontaktní místa určená členskými státy v souladu s článkem [článek X] směrnice [XXX/XXXX (o bezpečnosti sítí a informací 2)] a orgány dozoru nad trhem dostávaly

[16] Směrnice Evropského parlamentu a Rady XXX ze dne [datum] [o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 (Úř. věst. L xx, datum, s. x)].

informace od výrobců produktů s digitálními prvky, které jim umožní posoudit bezpečnost těchto produktů. S cílem zajistit, aby uživatelé mohli rychle reagovat na incidenty, které mají dopad na bezpečnost jejich produktů s digitálními prvky, by výrobci měli rovněž informovat své uživatele o každém takovém incidentu a případně o veškerých nápravných opatřeních, která mohou uživatelé zavést za účelem zmírnění dopadu incidentu, například zveřejněním příslušných informací na svých internetových stránkách nebo v případech, kdy je výrobce schopen kontaktovat uživatele a je-li to odůvodněno riziky, tím, že se obrátí přímo na uživatele.

(36) Výrobci produktů s digitálními prvky by měli zavést politiky koordinovaného odhalování zranitelností s cílem usnadnit jednotlivcům nebo subjektům oznamování zranitelností. Politika koordinovaného odhalování zranitelností by měla specifikovat strukturovaný proces, jehož prostřednictvím jsou zranitelná místa hlášena výrobcům takovým způsobem, který výrobci umožní diagnostikovat a odstranit tyto zranitelnosti dříve, než budou podrobné informace o nich sděleny třetím stranám nebo veřejnosti. Vzhledem k tomu, že informace o zneužitelných zranitelnostech široce používaných produktů s digitálními prvky lze na černém trhu prodávat za vysoké ceny, měli by mít výrobci těchto produktů možnost využívat v rámci svých politik programy koordinovaného odhalování zranitelností za účelem motivace k oznamování zranitelností tím, že zajistí, aby jednotlivci nebo subjekty získali za svou snahu uznání a odměnu (tzv. „program odměn za nalezení chyb“).

(37) Aby se usnadnila analýza zranitelností, měli by výrobci zjistit a zdokumentovat součásti obsažené v produktech s digitálními prvky, mimo jiné vypracováním softwarového kusovníku. Softwarový kusovník může poskytnout těm, kdo software vyrábějí, nakupují a provozují, informace, které jim umožní lépe pochopit dodavatelský řetězec, což má řadu výhod, zejména to pomáhá výrobcům a uživatelům při vysledování nově se objevujících zranitelností a rizik. Pro výrobce je obzvláště důležité zajistit, aby jejich produkty neobsahovaly zranitelné součásti vyvinuté třetími stranami.

(38) Za účelem usnadnění posuzování shody s požadavky stanovenými tímto nařízením by měl existovat předpoklad shody u produktů s digitálními prvky, jež jsou ve shodě s harmonizovanými normami, které převádějí základní požadavky tohoto nařízení do podrobných technických specifikací a které jsou přijaty v souladu s nařízením Evropského parlamentu a Rady (EU) č. 1025/2012[17]. Nařízení (EU) č. 1025/2012 stanoví postup pro námitky proti harmonizovaným normám, pokud tyto normy nesplňují v plné míře požadavky tohoto nařízení.

(39) Nařízení (EU) 2019/881 stanoví dobrovolný evropský rámec pro certifikaci kybernetické bezpečnosti pro produkty, procesy a služby IKT. Evropské systémy certifikace kybernetické bezpečnosti se mohou vztahovat na produkty s digitálními prvky, pro něž platí toto nařízení. Toto nařízení by mělo vytvářet součinnost s nařízením (EU) 2019/881. S cílem usnadnit posuzování shody s požadavky stanovenými v tomto nařízení se předpokládá, že produkty s digitálními prvky, které jsou certifikovány nebo pro něž bylo vydáno prohlášení o shodě v rámci systému kybernetické bezpečnosti podle nařízení (EU) 2019/881 a které Komise určila v

[17] Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES, a kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12).

prováděcím aktu, jsou v souladu se základními požadavky tohoto nařízení, pokud se na tyto požadavky vztahuje certifikát kybernetické bezpečnosti nebo prohlášení o shodě nebo jeho části. Potřeba nových evropských systémů certifikace kybernetické bezpečnosti pro produkty s digitálními prvky by měla být posuzována s ohledem na toto nařízení. Tyto budoucí evropské systémy certifikace kybernetické bezpečnosti týkající se produktů s digitálními prvky by měly zohledňovat základní požadavky stanovené v tomto nařízení a usnadňovat s ním soulad. Komise by měla být zmocněna k tomu, aby prostřednictvím prováděcích aktů určila evropské systémy certifikace v oblasti kybernetické bezpečnosti, které lze použít k prokázání shody se základními požadavky stanovenými v tomto nařízení. Aby se zabránilo nepřiměřené administrativní zátěži pro výrobce, měla by Komise dále případně určit, zda certifikát kybernetické bezpečnosti vydaný v rámci těchto evropských systémů certifikace kybernetické bezpečnosti ruší povinnost výrobců nechat si provést posouzení shody třetí stranou, jak je pro příslušné požadavky stanoveno v tomto nařízení.

(40) Po vstupu v platnost prováděcího aktu, kterým se stanoví [prováděcí nařízení Komise (EU) č. .../... ze dne XXX o evropském systému certifikace kybernetické bezpečnosti založeném na jednotných kritériích], jež se týká hardwarových produktů, na něž se vztahuje toto nařízení, například hardwarových bezpečnostních modulů a mikroprocesorů, může Komise prostřednictvím prováděcího aktu určit, jak evropský systém certifikace kybernetické bezpečnosti předpokládá shodu se základními požadavky podle přílohy I tohoto nařízení nebo jejich částmi. Tento prováděcí akt může dále určit, jakým způsobem certifikát vydaný v rámci evropského systému certifikace kybernetické bezpečnosti ruší povinnost výrobců nechat si provést posouzení třetí stranou, jak požaduje toto nařízení pro příslušné požadavky.

(41) Pokud nejsou přijaty žádné harmonizované normy nebo pokud harmonizované normy dostatečně neřeší základní požadavky tohoto nařízení, měla by mít Komise možnost přijmout obecné specifikace prostřednictvím prováděcích aktů. Mezi důvody pro vypracování těchto obecných specifikací namísto toho, aby se vycházelo z harmonizovaných norem, může patřit odmítnutí žádosti o normalizaci některou z evropských normalizačních organizací, nepřiměřená prodleva při vytváření vhodných harmonizovaných norem nebo nesoulad vypracovaných norem s požadavky tohoto nařízení nebo s žádostí Komise. Aby se usnadnilo posuzování shody se základními požadavky stanovenými tímto nařízením, měl by existovat předpoklad shody pro produkty s digitálními prvky, které jsou ve shodě s obecnými specifikacemi přijatými Komisí podle tohoto nařízení za účelem vyjádření podrobných technických specifikací těchto požadavků.

(42) Výrobci by měli vypracovat EU prohlášení o shodě s cílem poskytnout informace požadované podle tohoto nařízení o shodě produktů s digitálními prvky se základními požadavky tohoto nařízení a případně dalších příslušných harmonizačních právních předpisů Unie, které se na produkt vztahují. Od výrobců může být rovněž požadováno, aby vypracovali EU prohlášení o shodě na základě jiného právního předpisu Unie. Aby se pro účely dozoru nad trhem zajistil účinný přístup k informacím, mělo by být vypracováno jediné EU prohlášení o shodě s ohledem na dodržení všech příslušných aktů Unie. Za účelem snížení administrativní zátěže hospodářských subjektů by toto jediné EU prohlášení o shodě mohlo mít podobu složky tvořené příslušnými jednotlivými prohlášeními o shodě.

(43) Označení CE, které vyjadřuje shodu výrobku, je viditelným výsledkem celého postupu zahrnujícího posuzování shody v širším smyslu. Obecné zásady upravující označení CE jsou stanoveny v nařízení Evropského parlamentu a Rady (ES) č. 765/2008[18]. V tomto nařízení by měla být stanovena pravidla týkající se umisťování označení CE na produkty s digitálními prvky. Označení CE by mělo být jediným označením, které zaručuje, že produkt s digitálními prvky splňuje požadavky tohoto nařízení.

(44) Aby mohly hospodářské subjekty prokázat shodu se základními požadavky stanovenými v tomto nařízení a aby orgány dozoru nad trhem mohly zajistit, že produkty s digitálními prvky dodávané na trh tyto požadavky splňují, je nezbytné stanovit postupy posuzování shody. Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES[19] stanoví moduly pro postupy posuzování shody podle míry souvisejícího rizika a požadované úrovně bezpečnosti. S cílem zajistit soudržnost mezi odvětvími a zabránit variantám *ad hoc* byly na těchto modulech založeny postupy posuzování shody vhodné pro ověření shody produktů s digitálními prvky se základními požadavky stanovenými v tomto nařízení. Postupy posuzování shody by měly přezkoumat a ověřit požadavky týkající se produktu i postupu, které se vztahují na celý životní cyklus produktů s digitálními prvky, včetně plánování, návrhu, vývoje nebo výroby, testování a údržby produktu.

(45) Obecně platí, že posuzování shody produktů s digitálními prvky by měl na vlastní odpovědnost provádět výrobce, a to postupem založeným na modulu A rozhodnutí č. 768/2008/ES. Výrobce by si měl ponechat možnost zvolit přísnější postup posuzování shody za účasti třetí strany. Je-li produkt klasifikován jako kritický produkt třídy I, vyžaduje se dodatečná jistota za účelem prokázání shody se základními požadavky stanovenými v tomto nařízení. Pokud chce výrobce provést posouzení shody na vlastní odpovědnost (modul A), měl by uplatňovat harmonizované normy, obecné specifikace nebo systémy certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881, které Komise určila v prováděcím aktu. Pokud výrobce tyto harmonizované normy, obecné specifikace nebo systémy certifikace kybernetické bezpečnosti nepoužije, mělo by u něj proběhnout posouzení shody za účasti třetí strany. S ohledem na administrativní zátěž výrobců a na skutečnost, že kybernetická bezpečnost hraje důležitou úlohu ve fázi návrhu a vývoje hmotných a nehmotných produktů s digitálními prvky, byly jako nejvhodnější pro přiměřené a účinné posouzení souladu kritických produktů s digitálními prvky vybrány postupy posuzování shody založené na modulech B a C nebo modulu H rozhodnutí č. 768/2008/ES. Výrobce, který provádí posouzení shody za účasti třetí strany, si může zvolit postup, který je nejvhodnější z hlediska jeho procesu návrhu a výroby. Vzhledem k ještě většímu kybernetickému bezpečnostnímu riziku spojenému s používáním produktů klasifikovaných jako produkty kritické třídy II by se posuzování shody mělo vždy provádět za účasti třetí strany.

(46) Zatímco vytváření hmotných produktů s digitálními prvky obvykle vyžaduje, aby výrobci vynaložili značné úsilí během fáze návrhu, vývoje a výroby, vytváření produktů s digitálními prvky ve formě softwaru se téměř výhradně zaměřuje na návrh a vývoj, zatímco výrobní fáze hraje vedlejší jen malou roli. V řadě případů však musí

---

[18] Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30).

[19] Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES ze dne 9. července 2008 o společném rámci pro uvádění výrobků na trh a o zrušení rozhodnutí Rady 93/465/EHS (Úř. věst. L 218, 13.8.2008, s. 82).

být softwarové produkty ještě před uvedením na trh zkompilovány, vytvořeny, zabaleny, zpřístupněny ke stažení nebo zkopírovány na fyzické nosiče. Tyto činnosti by měly být považovány za činnosti odpovídající výrobě při použití příslušných modulů posuzování shody s cílem ověřit soulad produktu se základními požadavky tohoto nařízení ve fázi návrhu, vývoje a výroby.

(47) Za účelem provedení posouzení shody produktů s digitálními prvky třetí stranou by subjekty pro posuzování shody měly být oznámeny vnitrostátními oznamujícími orgány Komisi a ostatním členským státům, pokud splňují určitý soubor požadavků, zejména požadavků na nezávislost, způsobilost a neexistenci střetu zájmů.

(48) Za účelem zajištění jednotné úrovně kvality při provádění posuzování shody produktů s digitálními prvky je rovněž nezbytné stanovit požadavky pro oznamující orgány a ostatní subjekty zapojené do posuzování, oznamování a kontroly oznámených subjektů. Systém stanovený v tomto nařízení by měl být doplněn akreditačním systémem stanoveným v nařízení (ES) č. 765/2008. Vzhledem k tomu, že akreditace je základním prostředkem ověřování způsobilosti subjektů posuzování shody, měla by být rovněž používána pro účely oznamování.

(49) Transparentní akreditaci stanovenou v nařízení (ES) č. 765/2008, zajišťující nezbytnou míru důvěry v certifikáty shody, by měly vnitrostátní veřejné orgány v Unii považovat za přednostní způsob prokázání odborné způsobilosti subjektů posuzování shody. Vnitrostátní orgány se však mohou domnívat, že mají vhodné prostředky, aby toto hodnocení prováděly samy. V takovém případě by s cílem zajistit náležitou úroveň věrohodnosti hodnocení prováděného jinými vnitrostátními orgány měly Komisi a ostatním členským státům poskytnout nezbytné doklady o tom, že hodnocené subjekty posuzování shody splňují příslušné regulační požadavky.

(50) Subjekty posuzování shody často zadávají část svých činností souvisejících s posuzováním shody subdodavateli nebo dceřiné společnosti. V zájmu zachování úrovně ochrany požadované pro produkt s digitálními prvky, který má být uveden na trh, je nezbytné, aby subdodavatelé a dceřiné společnosti provádějící posuzování shody splňovali při provádění úkolů posuzování shody stejné požadavky jako oznámené subjekty.

(51) Oznámení subjektu posuzování shody by měl oznamující orgán zaslat Komisi a ostatním členským státům prostřednictvím informačního systému oznámených a jmenovaných organizací podle nového přístupu (NANDO). Systém NANDO je elektronický nástroj pro oznamování vyvinutý a spravovaný Komisí, v němž lze nalézt seznam všech oznámených subjektů.

(52) Vzhledem k tomu, že oznámené subjekty mohou své služby nabízet na území celé Unie, je vhodné dát ostatním členským státům a Komisi možnost vznést námitky týkající se oznámeného subjektu. Je proto důležité stanovit dobu, během níž bude možné vyjasnit veškeré pochyby nebo výhrady týkající se způsobilosti subjektů posuzování shody před tím, než začnou fungovat jako oznámené subjekty.

(53) Z důvodu konkurenceschopnosti je zásadně důležité, aby oznámené subjekty používaly postupy posuzování shody, aniž by zbytečně zatěžovaly hospodářské subjekty. Ze stejného důvodu a v zájmu zajištění rovného zacházení s hospodářskými subjekty je třeba zajistit jednotné technické provádění postupů posuzování shody. Toho by mělo být nejlépe dosaženo vhodnou koordinací a spoluprací mezi oznámenými subjekty.

(54) Dozor nad trhem je základním nástrojem při zajišťování řádného a jednotného uplatňování právních předpisů Unie. Proto je vhodné vytvořit právní rámec, ve kterém může dozor nad trhem vhodným způsobem probíhat. Na produkty s digitálními prvky, na něž se vztahuje toto nařízení, platí pravidla pro dozor nad trhem Unie a kontrolu výrobků vstupujících na trh Unie stanovená v nařízení Evropského parlamentu a Rady (EU) 2019/1020[20].

(55) V souladu s nařízením (EU) 2019/1020 orgány dozoru nad trhem vykonávají na území daného členského státu dozor nad trhem. Toto nařízení by nemělo členským státům bránit, aby si samy zvolily příslušné orgány, které budou tyto úkoly plnit. Každý členský stát by měl na svém území určit jeden nebo více orgánů dozoru nad trhem. Členské státy se mohou rozhodnout, že určí některý stávající nebo nový orgán, který bude působit jako orgán dozoru nad trhem, včetně příslušných vnitrostátních orgánů podle článku [článku X] směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] nebo určených vnitrostátních orgánů pro certifikaci kybernetické bezpečnosti podle článku 58 nařízení (EU) 2019/881. Hospodářské subjekty by měly plně spolupracovat s orgány dozoru nad trhem a dalšími příslušnými orgány. Každý členský stát by měl oznámit Komisi a ostatním členským státům své orgány dozoru nad trhem a působnost každého z nich, přičemž by měl zajistit nezbytné zdroje a dovednosti pro provádění úkolů dozoru souvisejících s tímto nařízením. Podle čl. 10 odst. 2 a 3 nařízení (EU) 2019/1020 by měl každý členský stát jmenovat ústřední styčný úřad, který by měl mimo jiné odpovídat za zastupování koordinovaného postoje orgánů dozoru nad trhem a za pomoc při spolupráci mezi orgány dozoru nad trhem v různých členských státech.

(56) Pro jednotné uplatňování tohoto nařízení by měla být zřízena specializovaná skupina pro správní spolupráci podle čl. 30 odst. 2 nařízení (EU) 2019/1020. Tato skupina pro správní spolupráci by se měla skládat ze zástupců určených orgánů dozoru nad trhem a případně i ze zástupců ústředních styčných úřadů. Komise by měla podporovat a podněcovat spolupráci mezi orgány dozoru nad trhem prostřednictvím sítě Unie pro soulad výrobků s předpisy, zřízené na základě článku 29 nařízení (EU) 2019/1020 a složené ze zástupců každého členského státu, včetně zástupce každého ústředního styčného úřadu podle článku 10 nařízení (EU) 2019/1020 a nepovinného vnitrostátního odborníka, předsedů skupiny pro správní spolupráci a zástupců Komise. Komise by se měla účastnit zasedání sítě, jejích podskupin a této příslušné skupiny pro správní spolupráci. Měla by této skupině pro správní spolupráci rovněž poskytovat pomoc prostřednictvím výkonného sekretariátu, který poskytuje technickou a logistickou podporu.

(57) V zájmu zajištění včasných, přiměřených a účinných opatření ve vztahu k produktům s digitálními prvky, které představují významné kybernetické bezpečnostní riziko, by měl být stanoven ochranný postup Unie, v jehož rámci jsou zúčastněné strany informovány o opatřeních, která mají být v souvislosti s těmito produkty přijata. Tento postup by měl orgánům dozoru nad trhem umožnit, aby ve spolupráci s příslušnými hospodářskými subjekty jednaly v případě potřeby co nejdříve. Pokud se členské státy a Komise shodují, že opatření přijaté členským státem je důvodné, neměl by být vyžadován žádný další zásah Komise, kromě případů, kdy lze nesoulad s právními předpisy přisuzovat nedostatkům v harmonizované normě.

---

[20] Nařízení Evropského parlamentu a Rady (EU) 2019/1020 ze dne 20. června 2019 o dozoru nad trhem a souladu výrobků s předpisy a o změně směrnice 2004/42/ES a nařízení (ES) č. 765/2008 a (EU) č. 305/2011 (Úř. věst. L 169, 25.6.2019, s. 1).

(58) V některých případech však může produkt s digitálními prvky, který je v souladu s tímto nařízením, přesto představovat významné kybernetické bezpečnostní riziko nebo představovat riziko pro zdraví nebo bezpečnost osob, pro dodržování povinností podle unijního nebo vnitrostátního práva, jejichž cílem je ochrana základních práv, dostupnosti, pravosti, integrity nebo důvěrnosti služeb nabízených prostřednictvím elektronického informačního systému zásadními subjekty druhu podle [příloha I směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] nebo pro jiné aspekty ochrany veřejného zájmu. Je proto nezbytné stanovit pravidla, která zajistí zmírnění těchto rizik. V důsledku toho by orgány dozoru nad trhem měly přijmout opatření požadující po hospodářském subjektu, aby zajistil, že produkt již toto riziko nepředstavuje, nebo aby jej v závislosti na riziku stáhl z oběhu. Jakmile orgán dozoru nad trhem takto omezí nebo zakáže volný pohyb produktu, měl by členský stát neprodleně oznámit Komisi a ostatním členským státům prozatímní opatření s uvedením důvodů a odůvodnění. Pokud orgán dozoru nad trhem tato opatření proti produktům představujícím riziko přijme, měla by Komise neprodleně zahájit konzultace s členskými státy a příslušným hospodářským subjektem nebo subjekty a měla by vnitrostátní opatření vyhodnotit. Na základě výsledků tohoto hodnocení by měla Komise rozhodnout, zda je vnitrostátní opatření důvodné, či nikoli. Rozhodnutí Komise by mělo být určeno všem členským státům a Komise jej neprodleně sdělí členským státům a příslušnému hospodářskému subjektu nebo subjektům. Pokud je opatření považováno za oprávněné, může Komise rovněž zvážit přijetí návrhů na revizi příslušných právních předpisů Unie.

(59) U produktů s digitálními prvky, které představují významné kybernetické bezpečnostní riziko, a pokud existuje důvod se domnívat, že nejsou v souladu s tímto nařízením, nebo u produktů, které jsou v souladu s tímto nařízením, avšak představují jiná důležitá rizika, například rizika pro zdraví nebo bezpečnost osob, základní práva nebo poskytování služeb zásadními subjekty druhu podle [příloha I směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)], může Komise požádat agenturu ENISA o provedení hodnocení. Na základě tohoto hodnocení může Komise prostřednictvím prováděcích aktů přijmout nápravná nebo omezující opatření na úrovni Unie, včetně nařízení o stažení příslušných produktů z trhu nebo z oběhu, a to v přiměřené lhůtě úměrné povaze rizika. Komise může tento zásah použít pouze za výjimečných okolností, které odůvodňují okamžitý zásah za účelem zachování řádného fungování vnitřního trhu, a pouze v případě, že kontrolní orgány nepřijaly účinná opatření k nápravě situace. Těmito výjimečnými okolnostmi mohou být mimořádné situace, kdy výrobce například ve velkém měřítku dodává nevyhovující produkt na trh ve více členských státech a tento produkt se používá i v klíčových odvětvích ze strany subjektů, které spadají do oblasti působnosti [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)], přičemž obsahuje známé zranitelnosti, které zneužívají nepřátelské subjekty a pro něž výrobce neposkytuje dostupné opravy. Komise může v těchto mimořádných situacích zasáhnout pouze po dobu trvání mimořádných okolností a v případě, že přetrvává nesoulad s tímto nařízením nebo že přetrvávají uvedená významná rizika.

(60) V případech, kdy existují náznaky nesouladu s tímto nařízením v několika členských státech, by orgány dozoru nad trhem měly mít možnost provádět společné činnosti s jinými orgány za účelem ověření souladu a zjištění kybernetických bezpečnostních rizik produktů s digitálními prvky.

(61) Souběžné koordinované kontrolní akce („sweepy“) jsou konkrétní donucovací opatření orgánů dozoru nad trhem, která mohou dále zvýšit bezpečnost produktů. Kontrolní

akce by měly být prováděny zejména v případech, kdy tržní trendy, stížnosti spotřebitelů nebo jiné náznaky ukazují, že některé kategorie produktů často představují kybernetická bezpečnostní rizika. Agentura ENISA by měla orgánům dozoru nad trhem předkládat návrhy na kategorie produktů, u nichž by mohly být kontrolní akce zorganizovány, mimo jiné na základě obdržených oznámeních o zranitelnosti produktů a o incidentech.

(62) Aby bylo zajištěno, že regulační rámec může být v případě potřeby upraven, měla by být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy, pokud jde o aktualizace seznamu kritických produktů v příloze III a upřesnění definic těchto kategorií produktů. Na Komisi by měla být přenesena pravomoc přijímat akty v souladu s uvedeným článkem za účelem zjištění produktů s digitálními prvky, na něž se vztahují jiná pravidla Unie, jež dosahují stejné úrovně ochrany jako toto nařízení, s upřesněním, zda by bylo nezbytné jejich omezení nebo vyloučení z oblasti působnosti tohoto nařízení, jakož i případně rozsah tohoto omezení. Na Komisi by měla být přenesena pravomoc přijímat akty v souladu s uvedeným článkem, pokud jde o možné pověření certifikací v případě některých vysoce kritických produktů s digitálními prvky na základě kritérií kritičnosti stanovených v tomto nařízení, jakož i za účelem stanovení minimálního obsahu EU prohlášení o shodě a doplnění prvků, které mají být obsaženy v technické dokumentaci. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[21]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

(63) Za účelem zajištění jednotných podmínek k provedení tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci, aby: určila formát a prvky softwarového kusovníku, blíže upřesnila druh informací, formát a postup oznámení o aktivně zneužívaných zranitelnostech a incidentech, které výrobci agentuře ENISA oznamují, specifikovala evropské systémy certifikace kybernetické bezpečnosti přijaté podle nařízení (EU) 2019/881, které lze použít k prokázání shody se základními požadavky nebo jejich částmi stanovenými v příloze I tohoto nařízení, přijala obecné specifikace, pokud jde o základní požadavky stanovené v příloze I, stanovila technické specifikace pro piktogramy nebo jakékoli jiné značky týkající se bezpečnosti produktů s digitálními prvky a mechanismů na podporu jejich používání a rozhodla o nápravných nebo omezujících opatřeních na úrovni Unie za výjimečných okolností, které odůvodňují okamžitý zásah za účelem zachování řádného fungování vnitřního trhu. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011[22].

(64) V zájmu zajištění důvěryhodné a konstruktivní spolupráce orgánů dozoru nad trhem na úrovni Unie a na vnitrostátní úrovni by měly všechny strany zapojené do uplatňování tohoto nařízení respektovat důvěrnost informací a údajů získaných při plnění svých úkolů.

---

21 Úř. věst. L 123, 12.5.2016, s. 1.

22 Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).

(65) S cílem zajistit účinné vymáhání povinností stanovených v tomto nařízení by každý orgán dozoru nad trhem měl mít pravomoc ukládat správní pokuty nebo požadovat uložení správních pokut. Proto by měly být stanoveny maximální úrovně správních pokut za nedodržení povinností stanovených v tomto nařízení, které budou určeny ve vnitrostátních právních předpisech. Při rozhodování o výši správní pokuty v každém jednotlivém případě by měly být zohledněny veškeré relevantní okolnosti konkrétní situace a přinejmenším ty, které jsou výslovně stanoveny v tomto nařízení, včetně skutečnosti, zda jiné orgány dozoru nad trhem již neuložily témuž hospodářskému subjektu správní pokuty za podobná protiprávní jednání. Tyto okolnosti mohou být buď přitěžující v situacích, kdy protiprávní jednání ze strany téhož subjektu trvá na území jiných členských států, než je stát, v němž již byla správní pokuta uložena, nebo polehčující tím, že je zajištěno, že některá jiná správní pokuta uvažovaná jiným orgánem dozoru nad trhem pro stejný hospodářský subjekt nebo stejný druh porušení předpisů již zohledňuje (společně s dalšími relevantními zvláštními okolnostmi) danou sankci a její výši uloženou v jiných členských státech. Ve všech těchto případech by kumulativní správní pokuta, kterou by mohly uložit orgány dozoru nad trhem několika členských států témuž hospodářskému subjektu za stejný druh porušení, měla zajišťovat dodržení zásady proporcionality.

(66) Jsou-li správní pokuty uloženy osobám, které nejsou podnikem, měl by příslušný úřad při rozhodování o odpovídající výši pokuty zohlednit obecnou úroveň příjmů v daném členském státě, jakož i ekonomickou situaci dané osoby. Mělo by být ponecháno na členských státech, aby určily, zda a v jaké míře by měly podléhat správním pokutám orgány veřejné správy.

(67) Ve vztazích s třetími zeměmi usiluje EU o podporu mezinárodního obchodu s regulovanými produkty. V zájmu usnadnění obchodu lze uplatnit širokou škálu opatření, včetně několika právních nástrojů, například dvoustranných (mezivládních) dohod o vzájemném uznávání (MRA) pro posuzování shody a označování regulovaných produktů. Dohody MRA se uzavírají mezi Unií a třetími zeměmi, které jsou na srovnatelné úrovni technického rozvoje a mají slučitelný přístup k posuzování shody. Tyto dohody jsou založeny na vzájemném uznávání certifikátů, označení shody a protokolů o zkouškách vystavených subjekty posuzování shody jedné ze stran v souladu s právními předpisy druhé strany. V současné době platí dohody MRA pro několik zemí. Tyto dohody se uzavírají v řadě konkrétních odvětví, která se mohou v jednotlivých zemích lišit. S cílem dále usnadnit obchod a uznat, že dodavatelské řetězce produktů s digitálními prvky jsou celosvětové, mohou být dohody MRA týkající se posuzování shody uzavřeny pro produkty, na něž se vztahuje toto nařízení, v souladu s článkem 218 Smlouvy o fungování EU. V zájmu posílení kybernetické odolnosti v celosvětovém měřítku je rovněž důležitá spolupráce s partnerskými zeměmi, neboť to v dlouhodobém horizontu přispěje k posílení rámce kybernetické bezpečnosti v rámci EU i mimo ni.

(68) Komise by měla provádět pravidelný přezkum tohoto nařízení za konzultace se zúčastněnými stranami, zejména pokud jde o nutnost změn s ohledem na měnící se společenské, politické, technologické nebo tržní podmínky.

(69) Hospodářským subjektům by měl být poskytnut dostatečný čas na přizpůsobení se požadavkům tohoto nařízení. Toto nařízení by se mělo použít [24 měsíců] od svého vstupu v platnost, s výjimkou povinností podávat zprávy o aktivně zneužívaných zranitelnostech a incidentech, které by se měly použít [12 měsíců] od vstupu tohoto nařízení v platnost.

(70) Jelikož cíle tohoto nařízení nemůže být dosaženo uspokojivě členskými státy, ale spíše jej, z důvodu účinků opatření, může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné k dosažení tohoto cíle,

(71) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725[23] byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne […],

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

Tímto nařízením se stanoví:

a) pravidla pro uvádění produktů s digitálními prvky na trh s cílem zajistit kybernetickou bezpečnost těchto produktů;

b) základní požadavky na navrhování, vývoj a výrobu produktů s digitálními prvky a povinnosti hospodářských subjektů v souvislosti s těmito produkty s ohledem na kybernetickou bezpečnost;

c) základní požadavky na procesy řešení zranitelnosti zavedené výrobci s cílem zajistit kybernetickou bezpečnost produktů s digitálními prvky během celého životního cyklu a povinnosti hospodářských subjektů v souvislosti s těmito procesy;

d) pravidla pro dozor nad trhem a prosazování výše uvedených pravidel a požadavků.

Článek 2

Oblast působnosti

1. Toto nařízení se vztahuje na produkty s digitálními prvky, jejichž zamýšlené nebo důvodně předpokládané použití zahrnuje přímé nebo nepřímé logické nebo fyzické datové připojení k zařízení nebo síti.

2. Toto nařízení se nevztahuje na produkty s digitálními prvky, na něž se vztahují tyto akty Unie:

   a) nařízení (EU) 2017/745;

   b) nařízení (EU) 2017/746;

   c) nařízení (EU) 2019/2144.

[23] Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

3. Toto nařízení se nevztahuje na produkty s digitálními prvky, které byly certifikovány v souladu s nařízením (EU) 2018/1139.

4. Použití tohoto nařízení na produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie stanovující požadavky, které se týkají všech nebo některých rizik, pro které platí základní požadavky stanovené v příloze I, může být omezeno nebo vyloučeno, pokud:

   a) je toto omezení nebo vyloučení v souladu s celkovým regulačním rámcem, který se na tyto produkty vztahuje, a

   b) odvětvová pravidla dosahují stejné úrovně ochrany, jakou stanoví toto nařízení.

   Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 50 za účelem změny tohoto nařízení, přičemž upřesní, zda je toto omezení nebo vyloučení nezbytné, specifikuje dotčené produkty a pravidla, jakož i případně rozsah omezení.

5. Toto nařízení se nevztahuje na produkty s digitálními prvky vyvinuté výlučně pro účely národní bezpečnosti nebo pro vojenské účely, ani na produkty speciálně určené ke zpracování utajovaných informací.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

1) „produktem s digitálními prvky“ jakýkoli softwarový nebo hardwarový produkt a jeho řešení pro zpracování dat na dálku, včetně softwarových nebo hardwarových součástí, které mají být uvedeny na trh samostatně;

2) „zpracováním dat na dálku“ jakékoli zpracování dat na dálku, pro které výrobce navrhuje a vyvíjí software nebo za jehož návrh a vývoj výrobce zodpovídá, přičemž neexistence tohoto softwaru by bránila tomu, aby produkt s digitálními prvky plnil některé ze svých funkcí;

3) „kritickým produktem s digitálními prvky“ produkt s digitálními prvky, který představuje kybernetické bezpečnostní riziko v souladu s kritérii stanovenými v čl. 6 odst. 2 a jehož základní funkce je stanovena v příloze III;

4) „kritickým produktem s digitálními prvky“ produkt s digitálními prvky, který představuje kybernetické bezpečnostní riziko v souladu s kritérii stanovenými v čl. 6 odst. 5;

5) „provozní technologií“ programovatelné digitální systémy nebo zařízení, které interagují s fyzickým prostředím nebo řídí zařízení, která interagují s fyzickým prostředím;

6) „softwarem“ část elektronického informačního systému, která sestává z počítačového kódu;

7) „hardwarem“ fyzický elektronický informační systém nebo jeho části schopné zpracovávat, uchovávat nebo přenášet digitální data;

8) „součástí“ software nebo hardware určený pro začlenění do elektronického informačního systému;

9) „elektronickým informačním systémem“ jakýkoli systém, včetně elektrických nebo elektronických zařízení, který je schopen zpracovávat, uchovávat nebo přenášet digitální data;

10) „logickým připojením“ virtuální forma datového připojení prováděná prostřednictvím softwarového rozhraní;

11) „fyzickým připojením“ jakékoli spojení mezi elektronickými informačními systémy nebo součástmi prováděné fyzickými prostředky, včetně elektrických nebo mechanických rozhraní, vodičů nebo rádiových vln;

12) „nepřímým připojením“ připojení k zařízení nebo síti, které neprobíhá přímo, ale spíše jako součást větší soustavy, která je k tomuto zařízení nebo síti přímo připojena;

13) „výsadou“ přístupové právo udělené konkrétním uživatelům nebo programům k provádění činností souvisejících s bezpečností v rámci elektronického informačního systému;

14) „přednostní výsadou“ přístupové právo udělené konkrétním uživatelům nebo programům k provádění rozšířeného souboru činností souvisejících s bezpečností v rámci elektronického informačního systému, které by v případě zneužití nebo ohrožení mohly umožnit nepřátelskému subjektu získat širší přístup ke zdrojům systému nebo organizace;

15) „koncovým bodem“ jakékoli zařízení, které je připojeno k síti a slouží jako vstupní bod do této sítě;

16) „síťovými nebo výpočetními zdroji“ funkce dat nebo hardwaru či softwaru, která je přístupná buď lokálně, nebo prostřednictvím sítě či jiného připojeného zařízení;

17) „hospodářským subjektem“ výrobce, zplnomocněný zástupce, dovozce, distributor nebo jakákoli jiná fyzická nebo právnická osoba, na kterou se vztahují povinnosti stanovené tímto nařízením;

18) „výrobcem“ fyzická nebo právnická osoba, která vyvíjí nebo vyrábí produkty s digitálními prvky nebo která nechala produkty s digitálními prvky navrhnout, vyvinout nebo vyrobit a uvádí je na trh pod svým jménem nebo ochrannou známkou, ať už za úplatu, nebo bezplatně;

19) „zplnomocněným zástupcem“ fyzická nebo právnická osoba usazená v Unii, která byla písemně pověřena výrobcem, aby jednala jeho jménem při plnění vymezených úkolů;

20) „dovozcem“ jakákoli fyzická nebo právnická osoba usazená v Unii, která uvádí na trh produkt s digitálními prvky označený jménem nebo ochrannou známkou fyzické nebo právnické osoby usazené mimo Unii;

21) „distributorem“ fyzická nebo právnická osoba v dodavatelském řetězci, jiná než výrobce nebo dovozce, která dodává produkt s digitálními prvky na trh Unie, aniž by ovlivňovala jeho vlastnosti;

22) „uvedením na trh“ první dodání produktu s digitálními prvky na trh Unie;

23) „dodáním na trh“ jakékoli dodání produktu s digitálními prvky k distribuci nebo použití na trhu Unie v rámci obchodní činnosti, ať už za úplatu, nebo bezplatně;

24) „určeným účelem“ použití produktu s digitálními prvky určené výrobcem, včetně konkrétního kontextu a podmínek použití, které jsou uvedeny v informacích

dodaných výrobcem v návodu k použití, v propagačních nebo prodejních materiálech a prohlášeních, jakož i v technické dokumentaci;

25) „důvodně předvídatelným použitím“ použití, které není nutně určeným účelem uvedeným výrobcem v návodu k použití, propagačních nebo prodejních materiálech a prohlášeních, jakož i v technické dokumentaci, ale které pravděpodobně vyplývá z důvodně předvídatelného lidského chování nebo technických operací nebo interakcí;

26) „důvodně předvídatelným nesprávným použitím“ použití produktu s digitálními prvky způsobem, který není v souladu s jeho určeným účelem, avšak může vyplývat z důvodně předvídatelného lidského chování nebo z interakce s jinými systémy;

27) „oznamujícím orgánem“ vnitrostátní orgán odpovědný za stanovení a provádění postupů nezbytných pro posuzování, jmenování a oznamování subjektů posuzování shody a za jejich monitorování;

28) „posouzením shody“ postup ověřující, že byly splněny základní požadavky stanovené v příloze I;

29) „subjektem posuzování shody“ subjekt ve smyslu čl. 2 odst. 13 nařízení (EU) č. 765/2008;

30) „oznámeným subjektem“ subjekt posuzování shody určený v souladu s článkem 33 tohoto nařízení a dalšími příslušnými harmonizačními právními předpisy Unie;

31) „podstatnou změnou“ změna produktu s digitálními prvky po jeho uvedení na trh, která ovlivňuje soulad produktu s digitálními prvky se základními požadavky stanovenými v oddílu 1 přílohy I nebo vede ke změně zamýšleného použití, pro které bylo provedeno posouzení produktu s digitálními prvky;

32) „označením CE“ označení, kterým výrobce vyjadřuje, že produkt s digitálními prvky a postupy zavedené výrobcem jsou ve shodě se základními požadavky stanovenými v příloze I a dalšími platnými právními předpisy Unie harmonizujícími podmínky pro uvádění produktů na trh (dále jen „harmonizační právní předpisy Unie“), které upravují umístění tohoto označení;

33) „orgánem dozoru nad trhem“ orgán ve smyslu čl. 3 bodu 4 nařízení (EU) 2019/1020;

34) „harmonizovanou normou“ harmonizovaná norma podle definice v čl. 2 bodu 1 písm. c) nařízení (EU) č. 1025/2012;

35) „kybernetickým bezpečnostním rizikem“ riziko definované v článku [článek X] směrnice [XXX/XXXX (o bezpečnosti sítí a informací 2)];

36) „významným kybernetickým bezpečnostním rizikem“ kybernetické bezpečnostní riziko, o němž lze na základě jeho technických charakteristik předpokládat, že u něj existuje vysoká pravděpodobnost incidentu, který by mohl vést k závažnému negativnímu dopadu, mimo jiné způsobením značné hmotné nebo nehmotné ztráty nebo narušení;

37) „softwarovým kusovníkem (SBOM, software bill of materials)“ formální záznam obsahující podrobnosti o dodavatelském řetězci a vztahy v něm u součástí začleněných do softwarových prvků produktu s digitálními prvky;

38) „zranitelností“ zranitelnost ve smyslu článku X směrnice [XXX/XXXX (o bezpečnosti sítí a informací 2)];

39) „aktivně zneužívanou zranitelností“ zranitelnost, u níž existují spolehlivé důkazy o tom, že subjekt v systému spustil škodlivý kód bez svolení vlastníka systému;

40) „osobními údaji“ osobní údaje ve smyslu čl. 1 odst. 4 nařízení (EU) 2016/679.

Článek 4

Volný pohyb

1. Členské státy nesmí pro hlediska, na něž se vztahuje toto nařízení, bránit tomu, aby byly na trh dodávány produkty s digitálními prvky, které jsou v souladu s tímto nařízením.

2. Na veletrzích, výstavách, předváděcích nebo podobných akcích nesmějí členské státy bránit prezentaci a používání produktu s digitálními prvky, který není v souladu s tímto nařízením.

3. Členské státy nebrání zpřístupnění nedokončeného softwaru, který není v souladu s tímto nařízením, za předpokladu, že software je k dispozici pouze po omezenou dobu nezbytnou pro účely testování a že viditelné označení jasně udává, že není v souladu s tímto nařízením a nebude dodáván na trh k jiným účelům než k testování.

Článek 5

Požadavky na produkty s digitálními prvky

Produkty s digitálními prvky se na trh dodávají pouze tehdy, pokud:

1) splňují základní požadavky stanovené v oddíle 1 přílohy I pod podmínkou, že jsou řádně instalovány, udržovány a používány k určenému účelu nebo za podmínek, které lze rozumně předvídat, a případně aktualizovány, a

2) postupy zavedené výrobcem jsou v souladu se základními požadavky stanovenými v oddíle 2 přílohy I.

Článek 6

Kritické produkty s digitálními prvky

1. Produkty s digitálními prvky, které patří do kategorie uvedené v příloze III, se považují za kritické produkty s digitálními prvky. Produkty, jejichž klíčová funkce spadá do kategorie uvedené v příloze III tohoto nařízení, se považují za produkty spadající do této kategorie. Kategorie kritických produktů s digitálními prvky se rozdělí do třídy I a třídy II, jak je stanoveno v příloze III, přičemž se zohlední úroveň kybernetických bezpečnostních rizik souvisejících s těmito produkty.

2. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 50 za účelem změny přílohy III, a to zařazením nové kategorie na seznam kategorií kritických produktů s digitálními prvky nebo vynětím stávající kategorie z tohoto seznamu. Při posuzování potřeby změnit seznam v příloze III Komise zohlední úroveň kybernetických bezpečnostních rizik souvisejících s kategorií produktů s digitálními prvky. Při určování úrovně kybernetického bezpečnostního rizika se zohlední jedno nebo více z těchto kritérií:

   a) funkce produktu s digitálními prvky související s kybernetickou bezpečností a to, zda má produkt s digitálními prvky alespoň jeden z těchto atributů:

      i) je určen k provozu s přednostní výsadou nebo ke správě výsad;

      ii) má přímý nebo výsadní přístup k síťovým nebo výpočetním zdrojům;

iii) je určen ke kontrole přístupu k údajům nebo provozním technologiím;

iv) plní funkci, která má zásadní význam pro důvěru, zejména bezpečnostní funkce, například řízení sítě, bezpečnost koncových bodů a ochrana sítě;

b) je určen pro použití v citlivém prostředí, včetně použití v průmyslovém prostředí nebo použití zásadními subjekty druhu uvedeného v příloze [příloha I] směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)];

c) je určen pro použití k výkonu kritických nebo citlivých funkcí, například zpracování osobních údajů;

d) potenciální rozsah nepříznivého dopadu, zejména pokud jde o jeho intenzitu a schopnost ovlivnit více osob;

e) do jaké míry již používání produktů s digitálními prvky způsobilo hmotnou či nehmotnou ztrátu nebo narušení nebo vyvolalo vážné obavy v souvislosti s výskytem nepříznivého dopadu.

3. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 50 za účelem doplnění tohoto nařízení tím, že upřesní definice kategorií produktů třídy I a II uvedené v příloze III. Akt v přenesené pravomoci se přijme [do 12 měsíců od vstupu tohoto nařízení v platnost].

4. Kritické produkty s digitálními prvky podléhají postupům posuzování shody podle čl. 24 odst. 2 a 3.

5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 50 za účelem doplnění tohoto nařízení tím, že upřesní kategorie vysoce kritických produktů s digitálními prvky, pro něž jsou výrobci povinni získat evropský certifikát kybernetické bezpečnosti v rámci evropského systému certifikace kybernetické bezpečnosti podle nařízení (EU) 2019/881, aby prokázali shodu se základními požadavky stanovenými v příloze I nebo jejich částmi. Při určování těchto kategorií vysoce kritických produktů s digitálními prvky Komise zohlední úroveň kybernetického bezpečnostního rizika souvisejícího s kategorií produktů s digitálními prvky s ohledem na jedno nebo několik kritérií uvedených v odstavci 2, jakož i s ohledem na posouzení toho, zda je tato kategorie produktů:

a) používána zásadními subjekty druhu uvedeného v příloze [příloha I] směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací NIS2)] nebo se na ni tyto subjekty spoléhají nebo bude mít možný budoucí význam pro činnosti těchto subjektů, nebo

b) zda je relevantní pro odolnost celého dodavatelského řetězce produktů s digitálními prvky vůči událostem, které způsobují narušení.

Článek 7

Obecná bezpečnost produktů

V případě, že se na produkty s digitálními prvky nevztahují zvláštní požadavky stanovené v jiných harmonizačních právních předpisech Unie ve smyslu [čl. 3 bod 25 nařízení o obecné bezpečnosti výrobků], se odchylně od čl. 2 odst. 1 třetího pododstavce písm. b) nařízení [nařízení o obecné bezpečnosti výrobků] použije na tyto produkty s ohledem na bezpečnostní rizika neupravená tímto nařízením oddíl 1 kapitoly III, kapitoly V a VII a kapitoly IX až XI nařízení [nařízení o obecné bezpečnosti výrobků].

Článek 8

Vysoce rizikové systémy UI

1. Produkty s digitálními prvky klasifikované jako vysoce rizikové systémy UI podle článku [článek 6] nařízení [nařízení o UI], které spadají do oblasti působnosti tohoto nařízení a splňují základní požadavky stanovené v oddíle 1 přílohy I tohoto nařízení a u nichž jsou postupy zavedené výrobcem v souladu se základními požadavky stanovenými v oddíle 2 přílohy I, se považují za produkty v souladu s požadavky týkajícími se kybernetické bezpečnosti stanovenými v článku [článek 15] nařízení [nařízení o UI], aniž jsou dotčeny ostatní požadavky týkající se přesnosti a odolnosti uvedené ve výše uvedeném článku, a to pokud je dosažení úrovně ochrany požadované těmito požadavky prokázáno v EU prohlášení o shodě vydaném podle tohoto nařízení.

2. U produktů a požadavků na kybernetickou bezpečnost podle odstavce 1 se použije příslušný postup posuzování shody požadovaný článkem [článek 43] nařízení [nařízení o UI]. Pro účely tohoto posouzení jsou oznámené subjekty, které jsou oprávněny kontrolovat shodu vysoce rizikových systémů UI podle nařízení [nařízení o UI], rovněž oprávněny kontrolovat shodu vysoce rizikových systémů UI spadajících do oblasti působnosti tohoto nařízení s požadavky stanovenými v příloze I tohoto nařízení, pokud byl soulad těchto oznámených subjektů s požadavky stanovenými v článku 29 tohoto nařízení posouzen v rámci postupu oznamování podle nařízení [nařízení o UI].

3. Pokud jde o základní požadavky tohoto nařízení, na kritické produkty s digitálními prvky uvedenými v příloze III tohoto nařízení, u kterých které musí být uplatněny postupy posuzování shody podle čl. 24 odst. 2 písm. a), čl. 24 odst. 2 písm. b), čl. 24 odst. 3 písm. a) a čl. 24 odst. 3 písm. b) tohoto nařízení a které jsou rovněž klasifikovány jako vysoce rizikové systémy UI podle článku [článek 6] nařízení [nařízení o UI] a na něž se vztahuje postup posuzování shody založený na vnitřní kontrole podle přílohy [příloha VI] nařízení [nařízení o UI], se odchylně od odstavce 2 vztahují postupy posuzování shody požadované tímto nařízením.

Článek 9

Strojní výrobky

Strojní výrobky v rozsahu působnosti nařízení [návrh nařízení o strojních zařízeních], které jsou produkty s digitálními prvky ve smyslu tohoto nařízení a pro něž bylo na základě tohoto nařízení vydáno EU prohlášení o shodě, se považují za výrobky, které jsou ve shodě se základními požadavky na ochranu zdraví a bezpečnost stanovenými v příloze [oddíly 1.1.9 a 1.2.1 přílohy III] nařízení [návrh nařízení o strojních zařízeních], pokud jde o ochranu proti poškození a bezpečnost a spolehlivost kontrolních systémů, a jestliže je dosažení úrovně ochrany požadované těmito požadavky prokázáno v EU prohlášení o shodě vydaném podle tohoto nařízení.

KAPITOLA II

POVINNOSTI HOSPODÁŘSKÝCH SUBJEKTŮ

Článek 10

Povinnosti výrobců

1. Při uvádění produktu s digitálními prvky na trh výrobci zajistí, aby byl navržen, vyvinut a vyroben v souladu se základními požadavky stanovenými v oddíle 1 přílohy I.

2. Pro účely splnění povinnosti stanovené v odstavci 1 provedou výrobci posouzení kybernetických bezpečnostních rizik spojených s produktem s digitálními prvky a výsledek tohoto posouzení zohlední během fází plánování, navrhování, vývoje, výroby, dodání a údržby produktu s digitálními prvky s cílem minimalizovat kybernetická bezpečnostní rizika, předcházet bezpečnostním incidentům a minimalizovat dopady těchto incidentů, a to i v souvislosti se zdravím a bezpečností uživatelů.

3. Při uvádění produktu s digitálními prvky na trh zahrne výrobce posouzení kybernetických bezpečnostních rizik do technické dokumentace, jak je stanoveno v článku 23 a příloze V. U produktů s digitálními prvky podle článku 8 a čl. 24 odst. 4, které se řídí i jinými akty Unie, může být posouzení kybernetických bezpečnostních rizik součástí posouzení rizik vyžadovaného těmito příslušnými akty Unie. Pokud se na produkt s digitálními prvky uváděný na trh nevztahují určité základní požadavky, výrobce do této dokumentace zahrne jasné odůvodnění.

4. Pro účely splnění povinnosti stanovené v odstavci 1 musí výrobci při začleňování součástí pocházejících od třetích stran do produktů s digitálními prvky postupovat s náležitou péčí. Zajistí, aby tyto součásti neohrožovaly bezpečnost produktu s digitálními prvky.

5. Výrobce systematicky dokumentuje relevantní aspekty kybernetické bezpečnosti týkající se produktu s digitálními prvky, a to způsobem, který je přiměřený povaze a kybernetickým bezpečnostním rizikům, včetně zranitelností, o nichž se dozví, a veškerých relevantních informací poskytnutých třetími stranami, a případně aktualizuje posouzení rizik produktu.

6. Při uvádění produktu s digitálními prvky na trh a po očekávanou dobu životnosti produktu nebo po dobu pěti let od jeho uvedení na trh (podle toho, která doba je kratší), výrobci zajistí, že je se zranitelnostmi tohoto produktu nakládáno účinně a v souladu se základními požadavky stanovenými v oddíle 2 přílohy I.

   Výrobci mají vhodné politiky a postupy, včetně politik koordinovaného odhalování zranitelností podle oddílu 2 bodu 5 přílohy I, pro zpracování a nápravu možných zranitelností v produktu s digitálními prvky hlášených z interních nebo externích zdrojů.

7. Před uvedením produktu s digitálními prvky na trh vypracují výrobci technickou dokumentaci podle článku 23.

   Provedou nebo nechají provést zvolené postupy posuzování shody podle článku 24.

   Pokud byl tímto postupem posuzování shody prokázán soulad produktu s digitálními prvky stanovenými v oddíle 1 přílohy I a soulad postupů zavedených výrobcem se

základními požadavky stanovenými v oddíle 2 přílohy I, vypracují výrobci EU prohlášení o shodě v souladu s článkem 20 a umístí označení CE v souladu s článkem 22.

8. Výrobci technickou dokumentaci a EU prohlášení o shodě uchovávají pro případnou potřebu orgánů dozoru po dobu deseti let od uvedení produktu s digitálními prvky na trh.

9. Výrobci zajistí, aby byly zavedeny postupy, díky nimž produkty s digitálními prvky, které jsou součástí sériové výroby, zůstanou ve shodě. Výrobce náležitě přihlédne ke změnám ve vývoji a výrobním postupu nebo návrhu nebo vlastnostech produktu s digitálními prvky a změnám harmonizovaných norem, evropských systémů certifikace kybernetické bezpečnosti nebo obecných specifikací uvedených v článku 19, na jejichž základě se prohlašuje nebo ověřuje shoda produktu s digitálními prvky.

10. Výrobci zajistí, aby k produktům s digitálními prvky byly v elektronické nebo fyzické podobě přiloženy informace a pokyny stanovené v příloze II. Tyto informace a pokyny jsou v jazyce snadno srozumitelném uživatelům. Jsou jasné, srozumitelné, snadno pochopitelné a čitelné. Umožňují bezpečnou instalaci, provoz a používání produktů s digitálními prvky.

11. Výrobci buď přiloží EU prohlášení o shodě k produktu s digitálními prvky, nebo uvedou v návodu k používání a informacích uvedených v příloze II internetovou adresu, na níž je přístup k EU prohlášení o shodě.

12. Od uvedení na trh a po dobu očekávané životnosti produktu nebo po dobu pěti let od uvedení produktu s digitálními prvky na trh, podle toho, která doba je kratší, výrobci, kteří vědí nebo mají důvod se domnívat, že produkt s digitálními prvky nebo postupy zavedenými výrobcem nejsou ve shodě se základními požadavky stanovenými v příloze I, přijmou okamžitě nápravná opatření nezbytná k dosažení shody produktu s digitálními prvky nebo postupů výrobce nebo případně ke stažení produktu z trhu nebo z oběhu.

13. Výrobci poskytnou orgánu dozoru nad trhem na základě jeho odůvodněné žádosti v jazyce, kterému snadno rozumí, všechny informace a dokumentaci v papírové nebo elektronické podobě nezbytnou k prokázání shody produktu s digitálními prvky a postupů zavedených výrobcem se základními požadavky stanovenými v příloze I. Na žádost tohoto orgánu s ním spolupracují na veškerých opatřeních přijatých k odstranění kybernetických bezpečnostních rizik představovaných produktem s digitálními prvky, který uvedli na trh.

14. Výrobce, který ukončí svou činnost, a v důsledku toho není schopen splnit povinnosti stanovené v tomto nařízení, informuje před tím, než ukončení činnosti nabude účinku, příslušné orgány dozoru nad trhem o této situaci a v co největší míře také uživatele dotčených produktů s digitálními prvky uváděných na trh.

15. Komise může prostřednictvím prováděcích aktů stanovit formát a prvky softwarového kusovníku uvedeného v oddíle 2 bodě 1 přílohy I. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 51 odst. 2.

Článek 11

Povinnosti výrobců podávat zprávy

1. Výrobce bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy se o ní dozví, oznámí agentuře ENISA každou aktivně zneužívanou zranitelnost

obsaženou v produktu s digitálními prvky. Oznámení obsahuje podrobnosti o této zranitelnosti a případně o přijatých nápravných nebo zmírňujících opatřeních. Agentura ENISA bez zbytečného odkladu, s výjimkou odůvodněných případů souvisejících s kybernetickými bezpečnostními riziky, předá oznámení po jeho obdržení týmu CSIRT určenému pro účely koordinovaného zveřejňování informací o zranitelnostech v souladu s článkem [článek X] směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] dotčených členských států a informuje orgán dozoru nad trhem o oznámené zranitelnosti.

2. Výrobce bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy se o něm dozví, oznámí agentuře ENISA jakýkoli incident, který má dopad na bezpečnost produktu s digitálními prvky. Agentura ENISA bez zbytečného odkladu, s výjimkou odůvodněných důvodů souvisejících s kybernetickými bezpečnostními riziky, předá oznámení jednotnému kontaktnímu místu určenému v souladu s článkem [článek X] směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] dotčených členských států a informuje orgán dozoru nad trhem o oznámených incidentech. Oznámení incidentu obsahuje informace o závažnosti a dopadu incidentu a případně uvádí, zda má výrobce podezření, že incident byl způsoben nezákonným nebo nepřátelským jednáním, nebo zda se domnívá, že má přeshraniční dopad.

3. Agentura ENISA předloží Evropské síti styčných organizací pro řešení kybernetických krizí (EU-CyCLONe) zřízené článkem [článek X] směrnice [XXX/XXXX (o bezpečnosti sítí a informací 2)] informace oznámené podle odstavců 1 a 2, pokud jsou tyto informace relevantní pro koordinované řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí na provozní úrovni.

4. Výrobce informuje uživatele produktu s digitálními prvky o incidentu neprodleně poté, co se o něm dozví, a v případě potřeby také o nápravných opatřeních, která může uživatel zavést ke zmírnění dopadu tohoto incidentu.

5. Komise může prostřednictvím prováděcích aktů dále upřesnit druh informací, formát a postup oznámení předkládaných podle odstavců 1 a 2. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 51 odst. 2.

6. Agentura ENISA na základě oznámení obdržených podle odstavců 1 a 2 vypracuje každé dva roky technickou zprávu o nových trendech týkajících se kybernetických bezpečnostních rizik u produktů s digitálními prvky a předloží ji skupině pro spolupráci podle článku [článek X] směrnice [XXX/XXXX (o bezpečnosti sítí a informací 2)]. První z těchto zpráv se předloží do 24 měsíců ode dne, kdy se začaly uplatňovat povinnosti stanovené v odstavcích 1 a 2.

7. Po zjištění zranitelnosti v součásti, včetně součásti s otevřeným zdrojovým kódem, která je začleněna do produktu s digitálními prvky, oznámí výrobci zranitelnost osobě nebo subjektu, který provádí údržbu této součásti.

Článek 12

Zmocnění zástupci

1. Výrobce může písemně jmenovat zplnomocněného zástupce.

2. Povinnosti stanovené v čl. 10 odst. 1 až 7 první odrážce a odst. 9 nejsou součástí pověření zplnomocněného zástupce.

3. Zplnomocněný zástupce plní úkoly stanovené v pověření, které obdržel od výrobce. Pověření musí zplnomocněnému zástupci umožňovat alespoň:

   a) uchovávat EU prohlášení o shodě podle článku 20 a technickou dokumentaci uvedenou v článku 23 pro potřebu orgánů dozoru nad trhem po dobu deseti let od uvedení produktu s digitálními prvky na trh;

   b) poskytnout příslušnému orgánu dozoru nad trhem na základě jeho odůvodněné žádosti všechny informace a dokumentaci nezbytné k prokázání shody produktu s digitálními prvky;

   c) spolupracovat s orgány dozoru nad trhem na jejich žádost na opatření, jehož cílem je vyloučit rizika vyvolaná produktem s digitálními prvky, na který se vztahuje pověření zplnomocněného zástupce.

Článek 13

Povinnosti dovozců

1. Dovozci uvádějí na trh produkty s digitálními prvky, které splňují základní požadavky stanovené v oddíle 1 přílohy I, a pokud jsou postupy zavedené výrobcem v souladu se základními požadavky stanovenými v oddíle 2 přílohy I.

2. Před uvedením produktu s digitálními prvky na trh dovozci zajistí, aby:

   a) výrobce provedl příslušné postupy posuzování shody podle článku 24;

   b) výrobce vypracoval technickou dokumentaci;

   c) produkt s digitálními prvky byl opatřen označením CE podle článku 22 a byly k němu přiloženy informace a návod k použití podle přílohy II.

3. Jestliže se dovozce domnívá nebo má důvod se domnívat, že produkt s digitálními prvky nebo postupy zavedené výrobcem nejsou ve shodě se základními požadavky stanovenými v příloze I, neuvede dovozce produkt na trh, dokud u tohoto produktu nebo u postupů zavedených výrobcem nebude dosaženo shody se základními požadavky stanovenými v příloze I. Pokud navíc produkt s digitálními prvky představuje významné kybernetické bezpečnostní riziko, informuje o tom dovozce výrobce a orgány dozoru nad trhem.

4. Dovozci uvedou na produktu s digitálními prvky své jméno, zapsaný obchodní název nebo zapsanou ochrannou známku, poštovní adresu a e-mailovou adresu, na níž je lze kontaktovat, nebo není-li to možné, uvedou tyto údaje na obalu nebo v dokladu přiloženém k produktu s digitálními prvky. Kontaktní údaje se uvádějí v jazyce snadno srozumitelném uživatelům a orgánům dozoru nad trhem.

5. Dovozci zajistí, aby byly k produktu s digitálními prvky přiloženy pokyny a informace stanovené v příloze II v jazyce, kterému uživatelé snadno rozumějí.

6. Dovozci, kteří vědí nebo mají důvod se domnívat, že produkt s digitálními prvky, který uvedli na trh, nebo postupy zavedené jeho výrobcem nejsou ve shodě se základními požadavky stanovenými v příloze I, přijmou okamžitě nápravná opatření nezbytná k uvedení produktu s digitálními prvky nebo postupů zavedených jeho výrobcem do souladu se základními požadavky stanovenými v příloze I nebo případně k jeho stažení z trhu nebo z oběhu.

   Po zjištění zranitelnosti produktu s digitálními prvky informují dovozci o této zranitelnosti bez zbytečného odkladu výrobce. Dále, pokud produkt s digitálními

prvky představuje významné kybernetické bezpečnostní riziko, informují o tom distributoři neprodleně orgány dozoru nad trhem členských států, v nichž produkt s digitálními prvky dodali na trh, a uvedou podrobnosti, zejména o neshodnosti a o přijatých nápravných opatřeních.

7. Dovozci po dobu deseti let od uvedení produktu s digitálními prvky na trh uchovávají kopii EU prohlášení o shodě pro potřebu orgánů dozoru nad trhem a zajišťují, aby těmto orgánům mohla být na požádání předložena technická dokumentace.

8. Dovozci poskytnou orgánu dozoru nad trhem na základě jeho odůvodněné žádosti všechny informace a dokumentaci v tištěné nebo elektronické podobě, které jsou nezbytné k prokázání souladu produktu s digitálními prvky se základními požadavky stanovenými v oddíle 1 přílohy I, jakož i postupů zavedených výrobcem se základními požadavky stanovenými v oddíle 2 přílohy I, a to v jazyce snadno srozumitelném tomuto orgánu. Spolupracují s tímto orgánem na jeho žádost na veškerých opatřeních přijatých k odstranění kybernetických bezpečnostních rizik představovaných produktem s digitálními prvky, který uvedli na trh.

9. Pokud se dovozce produktu s digitálními prvky dozví, že výrobce tohoto produkt ukončil svou činnost, a v důsledku toho není schopen splnit povinnosti stanovené v tomto nařízení, informuje o této situaci příslušné orgány dozoru nad trhem a jakýmikoli dostupnými prostředky a v co největší míře také uživatele produktů s digitálními prvky uváděných na trh.

Článek 14

Povinnosti distributorů

1. Při dodávání produktu s digitálními prvky na trh distributoři jednají s řádnou péčí, pokud jde o požadavky tohoto nařízení.

2. Před uvedením produktu s digitálními prvky na trh dovozci ověří, že:

   a) produkt s digitálními prvky je opatřen označením CE;

   b) výrobce a dovozce splnili povinnosti uvedené v čl. 10 odst. 10, čl. 10 odst. 11 a čl. 13 odst. 4.

3. Jestliže se distributor domnívá nebo má důvod se domnívat, že produkt s digitálními prvky nebo postupy zavedené výrobcem nejsou ve shodě se základními požadavky stanovenými v příloze I, nesmí dodat produkt s digitálními prvky na trh, dokud tento produkt nebo postupy zavedené výrobcem nedosáhnou shody. Pokud navíc produkt s digitálními prvky představuje významné kybernetické bezpečnostní riziko, informuje o tom distributor výrobce a orgány dozoru nad trhem.

4. Distributoři, kteří vědí nebo mají důvod se domnívat, že produkt s digitálními prvky, který dodali na trh, nebo postupy zavedené jeho výrobcem nejsou ve shodě se základními požadavky stanovenými v příloze I, zajistí, aby byla přijata nápravná opatření nezbytná k tomu, aby produkt s digitálními prvky nebo postupy zavedené jeho výrobcem dosáhly shody, nebo případně ke stažení tohoto produktu z trhu nebo z oběhu.

   Po zjištění zranitelnosti produktu s digitálními prvky informují distributoři o této zranitelnosti bez zbytečného odkladu výrobce. Dále, pokud produkt s digitálními prvky představuje významné kybernetické bezpečnostní riziko, informují o tom

distributoři neprodleně orgány dozoru nad trhem členských států, v nichž produkt s digitálními prvky dodali na trh, a uvedou podrobnosti, zejména o nesouladu a o přijatých nápravných opatřeních.

5. Distributoři poskytnou orgánu dozoru nad trhem na základě jeho odůvodněné žádosti všechny informace a dokumentaci v tištěné nebo elektronické podobě, které jsou nezbytné k prokázání souladu produktu s digitálními prvky a postupů zavedených jeho výrobcem se základními požadavky stanovenými v příloze I, a to v jazyce snadno srozumitelném tomuto orgánu. Spolupracují s tímto orgánem na jeho žádost na veškerých opatřeních přijatých k odstranění kybernetických bezpečnostních rizik představovaných produktem s digitálními prvky, který dodali na trh.

6. Pokud distributor produktu s digitálními prvky zjistí, že výrobce tohoto produktu ukončil svou činnost, a v důsledku toho není schopen splnit povinnosti stanovené v tomto nařízení, informuje o této situaci příslušné orgány dozoru nad trhem a v co největší míře také uživatele produktů s digitálními prvky uváděných na trh.

Článek 15

Případy, kdy se povinnosti výrobců vztahují na dovozce a distributory

Dovozce nebo distributor je pro účely tohoto nařízení považován za výrobce a vztahují se na něj povinnosti výrobce stanovené v článku 10 a v čl. 11 odst. 1, 2, 4 a 7, pokud tento dovozce nebo distributor uvede na trh produkt s digitálními prvky pod svým jménem nebo ochrannou známkou nebo provede podstatnou změnu produktu s digitálními prvky, který již byl na trh uveden.

Článek 16

Ostatní případy, na něž se vztahují povinnosti výrobců

Fyzická nebo právnická osoba jiná než výrobce, dovozce nebo distributor, která provádí podstatnou změnu produktu s digitálními prvky, se pro účely tohoto nařízení považuje za výrobce.

Na tuto osobu se vztahují povinnosti výrobce stanovené v článku 10 a v čl. 11 odst. 1, 2, 4 a 7, pokud jde o tu část produktu, která je touto podstatnou změnou ovlivněna, nebo jestliže má tato podstatná změna dopad na kybernetickou bezpečnost produktu s digitálními prvky jako celku, pokud jde o celý produkt.

Článek 17

Identifikace hospodářských subjektů

1. Hospodářské subjekty poskytnou orgánům dozoru nad trhem na požádání a v případě, že jsou k dispozici, následující informace:

   a) jméno a adresu každého hospodářského subjektu, který jim dodal produkt s digitálními prvky;

   b) název a adresu každého hospodářského subjektu, kterému dodaly produkt s digitálními prvky.

2. Hospodářské subjekty musí být schopny poskytnout informace uvedené v odstavci 1 po dobu deseti let poté, co jim byl produkt s digitálními prvky dodán, a po dobu deseti let poté, co produkt s digitálními prvky dodaly.

KAPITOLA III

SHODA PRODUKTU S DIGITÁLNÍMI PRVKY

Článek 18

Předpoklad shody

1. Předpokládá se, že produkty s digitálními prvky a postupy zavedené výrobcem, které jsou ve shodě s harmonizovanými normami nebo jejich částmi, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie*, jsou ve shodě se základními požadavky, na které se tyto normy nebo jejich části vztahují, stanovenými v příloze I.

2. Předpokládá se, že produkty s digitálními prvky a postupy zavedené výrobcem, které jsou ve shodě s obecnými specifikacemi uvedenými v článku 19, jsou ve shodě se základními požadavky stanovenými v příloze I v rozsahu, v jakém se tyto obecné specifikace vztahují na uvedené požadavky.

3. Předpokládá se, že produkty s digitálními prvky a postupy zavedené výrobcem, pro něž bylo vydáno EU prohlášení o shodě nebo certifikát v rámci evropského systému certifikace kybernetické bezpečnosti přijatého podle nařízení (EU) 2019/881 a určené podle odstavce 4, jsou ve shodě se základními požadavky stanovenými v příloze I, pokud se na tyto požadavky vztahuje EU prohlášení o shodě nebo certifikát kybernetické bezpečnosti nebo jeho části.

4. Komisi je svěřena pravomoc prostřednictvím prováděcích aktů specifikovat evropské systémy certifikace kybernetické bezpečnosti přijaté podle nařízení (EU) 2019/881, které lze použít k prokázání shody se základními požadavky nebo jejich částmi stanovenými v příloze I. Komise dále případně určí, zda certifikát kybernetické bezpečnosti vydaný v rámci těchto systémů ruší povinnost výrobce nechat provést posouzení shody třetí stranou pro účely příslušných požadavků, jak je stanoveno v čl. 24 odst. 2 písm. a) a b) a v čl. 24 odst. 3 písm. a) a b). Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 51 odst. 2.

Článek 19

Obecné specifikace

Pokud harmonizované normy podle článku 18 neexistují nebo pokud se Komise domnívá, že příslušné harmonizované normy nejsou dostatečné ke splnění požadavků tohoto nařízení nebo k vyhovění žádosti Komise o normalizaci nebo dojde-li k nepřiměřeným prodlevám v postupu normalizace nebo pokud žádost Komise o harmonizované normy nebyla evropskými normalizačními organizacemi přijata, je Komisi svěřena pravomoc přijímat prostřednictvím prováděcích aktů obecné specifikace týkající se základních požadavků stanovených v příloze I. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 51 odst. 2.

Článek 20

EU prohlášení o shodě

1. EU prohlášení o shodě vypracují výrobci v souladu s čl. 10 odst. 7 a bude se v něm uvádět, že bylo prokázáno splnění příslušných základních požadavků stanovených v příloze I.

2. EU prohlášení o shodě je vypracováno podle vzoru uvedeného v příloze IV a obsahuje prvky stanovené v příslušných postupech posuzování shody stanovených v příloze VI. Toto prohlášení je průběžně aktualizováno. Je k dispozici v jazyce nebo jazycích požadovaných členským státem, v němž je produkt s digitálními prvky uváděn nebo dodáván na trh.

3. Pokud se na produkt s digitálními prvky vztahuje více než jeden akt Unie vyžadující EU prohlášení o shodě, vypracuje se pro všechny tyto akty Unie jediné EU prohlášení o shodě. V prohlášení se uvedou dotčené akty Unie, včetně odkazů na jejich zveřejnění.

4. Vypracováním EU prohlášení o shodě přebírá výrobce odpovědnost za soulad produktu s požadavky.

5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 50 za účelem doplnění tohoto nařízení přidáním dalších prvků k minimálnímu obsahu EU prohlášení o shodě stanoveného v příloze IV s cílem zohlednit technologický vývoj.

Článek 21

Obecné zásady, kterými se řídí označení CE

Označení CE podle definice v čl. 3 odst. 32 podléhá obecným zásadám uvedeným v článku 30 nařízení (ES) č. 765/2008.

Článek 22

Pravidla a podmínky pro umístění označení CE

1. Označení CE se viditelně, čitelně a nesmazatelně umístí na produkt s digitálními prvky. Pokud to vzhledem k povaze produktu s digitálními prvky není možné nebo odůvodněné, umístí se označení CE na obal a na EU prohlášení o shodě podle článku 20, které produkt s digitálními prvky doprovází. U produktů s digitálními prvky, které jsou ve formě softwaru, se označení CE umístí buď na EU prohlášení o shodě podle článku 20, nebo na internetové stránky doprovázející softwarový produkt.

2. Vzhledem k povaze produktu s digitálními prvky může být výška označení CE umístěného na produkt s digitálními prvky menší než 5 mm za předpokladu, že označení zůstane viditelné a čitelné.

3. Označení CE se umístí před uvedením produktu s digitálními prvky na trh. Za označením může následovat piktogram nebo jakákoli jiná značka označující zvláštní riziko nebo použití stanovené v prováděcích aktech podle odstavce 6.

4. Za označením CE následuje identifikační číslo oznámeného subjektu, je-li tento subjekt zapojen do postupu posuzování shody založeného na komplexním zabezpečování kvality (na základě modulu H) podle článku 24.

   Identifikační číslo oznámeného subjektu umístí sám subjekt, nebo jej umístí podle jeho pokynů výrobce nebo zplnomocněný zástupce výrobce.

5. Členské státy vycházejí ze stávajících mechanismů, aby zajistily řádné uplatňování režimu označování CE, a přijmou vhodná opatření v případě nesprávného použití tohoto označení. Pokud se na produkt s digitálními prvky vztahují jiné právní předpisy Unie, které rovněž stanoví umístění označení CE, pak se v tomto označení uvede, že produkt splňuje také požadavky těchto jiných právních předpisů.

6. Komise může prostřednictvím prováděcích aktů stanovit technické specifikace pro piktogramy nebo jakékoli jiné značky týkající se bezpečnosti produktů s digitálními prvky a mechanismy na podporu jejich používání. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 51 odst. 2.

Článek 23

Technická dokumentace

1. Technická dokumentace musí obsahovat všechny příslušné údaje nebo podrobnosti o prostředcích, které výrobce použil k zajištění toho, aby produkt s digitálními prvky a postupy zavedené výrobcem byly v souladu se základními požadavky stanovenými v příloze I. Obsahuje alespoň prvky stanovené v příloze V.
2. Technická dokumentace se vypracuje před uvedením produktu s digitálními prvky na trh a v případě potřeby je průběžně aktualizována po dobu očekávané životnosti produktu nebo po dobu pěti let od uvedení produktu s digitálními prvky na trh, podle toho, která doba je kratší.
3. Pro produkty s digitálními prvky podle článku 8 a čl. 24 odst. 4, které se řídí i jinými akty Unie, se vypracuje jediná technická dokumentace obsahující informace podle přílohy V tohoto nařízení a informace požadované těmito příslušnými akty Unie.
4. Technická dokumentace a korespondence týkající se jakéhokoli postupu posuzování shody se vypracuje v úředním jazyce členského státu, v němž je oznámený subjekt usazen, nebo v jazyce pro tento subjekt přijatelném.
5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 50 za účelem doplnění tohoto nařízení o prvky, které mají být zahrnuty do technické dokumentace stanovené v příloze V, s cílem zohlednit technologický vývoj, jakož i vývoj při postupu provádění tohoto nařízení.

Článek 24

Postupy posuzování shody u produktů s digitálními prvky

1. Výrobce provede posouzení shody produktu s digitálními prvky a postupů, které zavedl, s cílem určit, zda jsou splněny základní požadavky stanovené v příloze I. Výrobce nebo jeho zplnomocněný zástupce prokazuje shodu se základními požadavky jedním z těchto postupů:
   a) postup vnitřní kontroly (na základě modulu A) stanovený v příloze VI, nebo
   b) EU přezkoušení typu (na základě modulu B) podle přílohy VI, po kterém následuje shoda s EU typem založená na interním řízení výroby (na základě modulu C) podle přílohy VI, nebo
   c) posuzování shody založené na komplexním zabezpečování kvality (na základě modulu H) podle přílohy VI.
2. Pokud při posuzování souladu kritického produktu s digitálními prvky třídy I stanovenými v příloze III a postupů zavedených jeho výrobcem se základními požadavky stanovenými v příloze I výrobce nebo jeho zplnomocněný zástupce nepoužil (nebo použil pouze částečně) harmonizované normy, obecné specifikace nebo evropské systémy certifikace kybernetické bezpečnosti podle článku 18, nebo jestliže takové harmonizované normy, obecné specifikace nebo evropské systémy certifikace kybernetické bezpečnosti neexistují, dotčený produkt s digitálními prvky

a postupy zavedené výrobcem s ohledem na tyto základní požadavky budou podrobeny jednomu z těchto postupů:

a) EU přezkoušení typu (na základě modulu B) podle přílohy VI, po kterém následuje shoda s EU typem založená na interním řízení výroby (na základě modulu C) podle přílohy VI, nebo

b) posuzování shody založené na komplexním zabezpečování kvality (na základě modulu H) podle přílohy VI.

3. Pokud je produkt kritickým produktem s digitálními prvky třídy II stanovenými v příloze III, výrobce nebo zplnomocněný zástupce výrobce prokáže shodu se základními požadavky stanovenými v příloze I jedním z těchto postupů:

a) EU přezkoušení typu (na základě modulu B) podle přílohy VI, po kterém následuje shoda s EU typem založená na interním řízení výroby (na základě modulu C) podle přílohy VI, nebo

b) posuzování shody založené na komplexním zabezpečování kvality (na základě modulu H) podle přílohy VI.

4. Výrobci produktů s digitálními prvky, které jsou klasifikovány jako systémy elektronických zdravotních záznamů v oblasti působnosti nařízení [nařízení o evropském prostoru pro zdravotní data], prokáží shodu se základními požadavky stanovenými v příloze I tohoto nařízení pomocí příslušného postupu posuzování shody, jak vyžaduje nařízení [kapitola III nařízení o evropském prostoru pro zdravotní data].

5. Oznámené subjekty vezmou při stanovování poplatků za postupy posouzení shody v úvahu specifické zájmy a potřeby malých a středních podniků a na základě těchto specifických zájmů a potřeb přiměřeně poplatky sníží.

KAPITOLA IV

OZNAMOVÁNÍ SUBJEKTŮ POSUZOVÁNÍ SHODY

Článek 25

Oznámení

Členské státy oznámí Komisi a ostatním členským státům subjekty posuzování shody, které jsou oprávněny vykonávat posuzování shody podle tohoto nařízení.

Článek 26

Oznamující orgány

1. Členské státy určí oznamující orgán odpovědný za vytvoření a provádění nezbytných postupů pro posuzování a oznamování subjektů posuzování shody a za kontrolu oznámených subjektů, včetně souladu s článkem 31.

2. Členské státy mohou rozhodnout o tom, že posuzování a kontrolu podle odstavce 1 provádí vnitrostátní akreditační orgán ve smyslu nařízení (ES) č. 765/2008 a v souladu s ním.

Článek 27

Požadavky týkající se oznamujících orgánů

1. Oznamující orgán musí být zřízen takovým způsobem, aby nedošlo k žádnému střetu zájmů se subjekty posuzování shody.

2. Oznamující orgán je organizován a funguje tak, aby chránil objektivitu a nestrannost svých činností.

3. Oznamující orgán je organizován takovým způsobem, aby každé rozhodnutí týkající se oznámení subjektu posuzování shody bylo přijato příslušnými osobami, jinými než osobami, které provedly posouzení.

4. Oznamující orgán nenabízí ani neposkytuje žádné činnosti, které provádějí subjekty posuzování shody, ani neposkytuje poradenské služby na komerčním či konkurenčním základě.

5. Oznamující orgán chrání důvěrnost informací, které obdržel.

6. Oznamující orgán má k dispozici dostatečný počet odborně způsobilých pracovníků, aby mohl řádně vykonávat své úkoly.

Článek 28

Informační povinnost oznamujících orgánů

1. Členské státy informují Komisi o svých postupech pro posuzování a oznamování subjektů posuzování shody a kontrolu oznámených subjektů a o veškerých změnách týkajících se těchto postupů.

2. Komise tyto informace zveřejní.

Článek 29

Požadavky týkající se oznámených subjektů

1. Pro účely oznámení musí subjekt posuzování shody splňovat požadavky stanovené v odstavcích 2 až 12.

2. Subjekt posuzování shody musí být zřízen podle vnitrostátních právních předpisů a mít právní subjektivitu.

3. Subjekt posuzování shody musí být třetí stranou nezávislou na organizaci nebo produktu, které posuzuje.

   Za takovýto subjekt může být považován subjekt patřící k hospodářskému sdružení nebo profesnímu svazu, které zastupují podniky zapojené do projektování, vývoje, výroby, dodávání, montáže, používání nebo údržby produktů s digitálními prvky, které tento subjekt posuzuje, pokud je prokázána jeho nezávislost a neexistence jakéhokoli střetu zájmů.

4. Subjekt posuzování shody, jeho nejvyšší vedení a pracovníci odpovědní za vykonávání úkolů posuzování shody nesmějí být osobami, které projektují, vyvíjejí, vyrábějí, dodávají, instalují, nakupují, vlastní, používají nebo udržují produkty s digitálními prvky, které posuzují, ani zplnomocněnými zástupci jakékoli z těchto stran. To nevylučuje používání posuzovaných produktů, které jsou nezbytné pro činnost subjektu posuzování shody, ani používání takových produktů k osobním účelům.

Subjekt posuzování shody, jeho nejvyšší vedení a pracovníci odpovědní za vykonávání úkolů posuzování shody se nesmějí přímo podílet na projektování, vývoji, výrobě, uvádění na trh, instalaci, používání ani údržbě těchto produktů, ani nesmějí zastupovat strany, které se těmito činnostmi zabývají. Nesmějí vykonávat žádnou činnost, která by mohla ohrozit jejich nezávislý úsudek nebo důvěryhodnost ve vztahu k činnostem posuzování shody, k jejichž vykonávání jsou oznámeni. To platí zejména pro poradenské služby.

Subjekty posuzování shody musí zajistit, aby činnosti jejich dceřiných společností nebo subdodavatelů neohrožovaly důvěrnost, objektivitu a nestrannost jejich činností posuzování shody.

5. Subjekty posuzování shody a jejich pracovníci vykonávají činnosti posuzování shody na nejvyšší úrovni profesionální důvěryhodnosti a požadované odborné způsobilosti v konkrétní oblasti a nesmějí být vystaveni žádným tlakům a podnětům, zejména finančním, které by mohly ovlivnit jejich úsudek nebo výsledky jejich činností posuzování shody, zejména ze strany osob nebo skupin osob, které mají na výsledcích těchto činností zájem.

6. Subjekt posuzování shody musí být schopen plnit všechny úkoly posuzování shody podle přílohy VI a pro něž byl oznámen, bez ohledu na to, zda tyto úkoly plní subjekt posuzování shody sám, nebo jsou plněny jeho jménem a na jeho odpovědnost.

Subjekt posuzování shody musí mít vždy a pro každý postup posuzování shody a každý druh nebo kategorii produktů s digitálními prvky, pro něž byl oznámen, k dispozici nezbytné:

a) zaměstnance s odbornými znalostmi a dostatečnými zkušenostmi potřebnými k plnění úkolů posuzování shody;

b) popisy postupů, podle nichž je posuzování shody prováděno, aby byla zajištěna transparentnost těchto postupů a možnost jejich zopakování. Musí mít zavedenu náležitou politiku a postupy pro rozlišení mezi úkoly, jež vykonává jako oznámený subjekt, a dalšími činnostmi;

c) postupy pro výkon činností, jež řádně zohledňují velikost podniku, odvětví, v němž působí, jeho strukturu, míru složitosti technologie daného produktu a hromadný či sériový způsob výroby.

Musí mít prostředky nezbytné k řádnému plnění technických a administrativních úkolů spojených s činnostmi posuzování shody a musí mít přístup k veškerému potřebnému vybavení nebo zařízením.

7. Pracovníci odpovědní za provádění činností posuzování shody musí:

a) mít dobrou technickou a odbornou přípravu zahrnující všechny činnosti posuzování shody, pro něž byl subjekt posuzování shody oznámen;

b) mít uspokojivou znalost požadavků souvisejících s posuzováním, které provádějí, a odpovídající pravomoc toto posuzování provádět;

c) mít náležité znalosti základních požadavků, použitelných harmonizovaných norem a příslušných ustanovení právních předpisů Unie a jejich prováděcích aktů a rozumět jim;

d) být schopni vypracovávat certifikáty, záznamy a zprávy prokazující provedení posuzování shody.

8. Musí být zaručena nestrannost subjektů posuzování shody, jejich nejvyššího vedení a pracovníků, kteří provádějí posuzování.

   Odměňování nejvyššího vedení a pracovníků subjektu posuzování shody, kteří provádějí posuzování, nesmí záviset na počtu provedených posouzení ani na výsledcích těchto posouzení.

9. Subjekty posuzování shody uzavřou pojištění odpovědnosti za škodu, pokud tuto odpovědnost nepřevzal stát v souladu s vnitrostátními právními předpisy nebo pokud není za posuzování shody přímo odpovědný sám členský stát.

10. Pracovníci subjektu posuzování shody zachovávají služební tajemství, pokud jde o veškeré informace, které obdrželi při plnění svých úkolů podle přílohy VI nebo podle jakéhokoli ustanovení vnitrostátního předpisu, kterými se provádí, s výjimkou styku s příslušnými orgány dozoru nad trhem členského státu, v němž vykonávají svou činnost. Vlastnická práva jsou chráněna. Subjekt posuzování shody musí mít dokumentované postupy zajišťující soulad s tímto odstavcem.

11. Subjekty posuzování shody se podílejí na příslušných normalizačních činnostech a na činnostech koordinační skupiny oznámených subjektů zřízené podle článku 40 nebo zajistí, aby byli jejich pracovníci o těchto činnostech informováni, a řídí se správními rozhodnutími a jinými dokumenty, které mají povahu všeobecných pokynů a které jsou výsledkem práce této skupiny.

12. Pokud jde o poplatky, subjekty posuzování shody působí v souladu se souborem důsledných, spravedlivých a přiměřených podmínek, zejména s přihlédnutím k zájmům malých a středních podniků.

Článek 30

Předpoklad shody oznámených subjektů

Pokud subjekt posuzování shody prokáže svou shodu s kritérii stanovenými v příslušných harmonizovaných normách nebo jejich částech, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie*, předpokládá se, že splňuje požadavky stanovené v článku 29 v rozsahu, v němž se harmonizované normy na tyto požadavky vztahují.

Článek 31

Pobočky a subdodavatelé oznámených subjektů

1. Pokud oznámený subjekt zadá konkrétní úkoly týkající se posuzování shody subdodavateli nebo dceřiné společnosti, zajistí, aby subdodavatel nebo dceřiná společnost splňovali požadavky stanovené v článku 29, a informuje o tom oznamující orgán.

2. Oznámené subjekty nesou plnou odpovědnost za úkoly provedené subdodavateli nebo dceřinými společnostmi bez ohledu na to kde jsou tito subdodavatelé nebo dceřiné společnosti usazeni.

3. Činnosti lze zadat subdodavateli nebo dceřiné společnosti pouze se souhlasem výrobce.

4. Oznámený subjekt uchovává pro potřebu oznamujícího orgánu příslušné doklady týkající se posouzení kvalifikací subdodavatele nebo dceřiné společnosti a práce provedené subdodavatelem nebo dceřinou společností podle tohoto nařízení.

Článek 32

Žádost o oznámení

1. Subjekt posuzování shody podává žádost o oznámení oznamujícímu orgánu členského státu, v němž je usazen.

2. Součástí žádosti je popis činností posuzování shody, postupu nebo postupů posuzování shody a produktu nebo produktů, pro něž se subjekt prohlašuje za způsobilý, jakož i osvědčení o akreditaci, pokud existuje, vydané vnitrostátním akreditačním orgánem, které potvrzuje, že subjekt posuzování shody splňuje požadavky stanovené v článku 29.

3. Nemůže-li dotčený subjekt posuzování shody předložit osvědčení o akreditaci, poskytne oznamujícímu orgánu veškeré doklady nezbytné k ověření, uznání a pravidelné kontrole svého souladu s požadavky stanovenými v článku 29.

Článek 33

Postup oznamování

1. Oznamující orgány mohou oznámit pouze subjekty posuzování shody, které splňují požadavky stanovené v článku 29.

2. Oznamující orgán uvědomí Komisi a ostatní členské státy prostřednictvím informačního systému oznámených a jmenovaných organizací podle nového přístupu (NANDO), který vyvinula a spravuje Komise.

3. Oznámení obsahuje veškeré podrobnosti o činnostech posuzování shody, modulu nebo modulech posuzování shody, dotčeném produktu nebo produktech a příslušné osvědčení o akreditaci.

4. Pokud se oznámení nezakládá na osvědčení o akreditaci uvedeném v čl. 32 odst. 2, poskytne oznamující orgán Komisi a ostatním členským státům podklady, které dokládají způsobilost subjektu posuzování shody, a informuje je o opatřeních, jež zajišťují, aby byl subjekt pravidelně kontrolován a i v budoucnu splňoval požadavky uvedené v článku 29.

5. Dotčený subjekt může vykonávat činnosti oznámeného subjektu, pouze pokud proti tomu Komise nebo ostatní členské státy nevznesly námitky do dvou týdnů po oznámení, pokud se použije osvědčení o akreditaci, nebo do dvou měsíců po oznámení, pokud se akreditace nepoužije.

   Pouze takový subjekt se pro účely tohoto nařízení považuje za oznámený subjekt.

6. Komisi a ostatním členským státům je třeba oznámit jakékoli následné významné změny týkající se oznámení.

Článek 34

Identifikační čísla a seznamy oznámených subjektů

1. Komise oznámenému subjektu přidělí identifikační číslo.

   Přidělí mu jediné číslo i v případě, že je subjekt oznámen podle několika aktů Unie.

2. Komise zveřejní seznam subjektů oznámených podle tohoto nařízení, včetně identifikačních čísel, která jim byla přidělena, a činností, pro něž byly oznámeny.

   Komise zajistí, aby byl tento seznam průběžně aktualizován.

Článek 35

Změny v oznámeních

1. Pokud oznamující orgán zjistí nebo je upozorněn na to, že oznámený subjekt již nesplňuje požadavky stanovené v článku 29 nebo neplní své povinnosti, omezí, pozastaví nebo případně zruší oznámení podle toho, jak je neplnění těchto požadavků nebo povinností závažné. Informuje o tom neprodleně Komisi a ostatní členské státy.

2. V případě omezení, pozastavení nebo zrušení oznámení nebo v případě, že oznámený subjekt ukončil svou činnost, zajistí oznamující členský stát, aby byly spisy tohoto subjektu buď zpracovány jiným oznámeným subjektem, nebo byly na vyžádání k dispozici příslušným oznamujícím orgánům a orgánům dozoru nad trhem.

Článek 36

Zpochybnění způsobilosti oznámených subjektů

1. Komise vyšetří všechny případy, v nichž má pochybnosti nebo je upozorněna na pochybnosti o způsobilosti oznámeného subjektu nebo o tom, zda oznámený subjekt nadále plní požadavky a povinnosti, které jsou mu uloženy.

2. Oznamující členský stát předloží Komisi na vyžádání všechny informace týkající se podkladů pro oznámení nebo zachování způsobilosti dotčeného subjektu.

3. Komise zajistí, aby se se všemi citlivými informacemi získanými v průběhu tohoto šetření nakládalo jako s důvěrnými.

4. Pokud Komise zjistí, že oznámený subjekt nesplňuje nebo přestal splňovat požadavky pro své oznámení, informuje o tom oznamující členský stát a vyzve ho, aby přijal nezbytná nápravná opatření, včetně případného zrušení oznámení.

Článek 37

Povinnosti týkající se činnosti oznámených subjektů

1. Oznámené subjekty provádějí posuzování shody v souladu s postupy posuzování shody stanovenými v článku 24 a příloze VI.

2. Posuzování shody se provádí přiměřeným způsobem, aby se zabránilo zbytečné zátěži hospodářských subjektů. Subjekty posuzování shody při výkonu své činnosti řádně zohlední velikost podniku, odvětví, v němž působí, jeho strukturu, míru složitosti technologie daného produktu a hromadnou nebo sériovou povahu výrobního procesu.

3. Oznámený subjekt však musí dodržovat míru přísnosti a úroveň ochrany, jež jsou vyžadovány, aby byl produkt v souladu s ustanoveními tohoto nařízení.

4. Pokud oznámený subjekt zjistí, že výrobce nesplnil požadavky stanovené v příloze I nebo v odpovídajících harmonizovaných normách nebo v obecných specifikacích podle článku 19, vyzve výrobce, aby přijal vhodná nápravná opatření, a nevydá certifikát shody.

5. Pokud v průběhu kontroly shody po vydání certifikátu oznámený subjekt zjistí, že produkt již nesplňuje požadavky stanovené v tomto nařízení, vyzve výrobce, aby přijal vhodná nápravná opatření, a v případě nutnosti certifikát pozastaví nebo odejme.

6. Pokud nejsou nápravná opatření přijata nebo pokud nemají požadovaný účinek, oznámený subjekt podle potřeby omezí, pozastaví nebo odejme příslušné certifikáty.

Článek 38

Informační povinnost oznámených subjektů

1. Oznámené subjekty informují oznamující orgán:

   a) o každém zamítnutí, omezení, pozastavení nebo odnětí certifikátu;

   b) o všech okolnostech majících vliv na rozsah a podmínky oznámení;

   c) o každé žádosti o informace týkající se činností posuzování shody, kterou obdržely od orgánů dozoru nad trhem;

   d) na vyžádání o činnostech posuzování shody vykonaných v rámci působnosti jejich oznámení a o jakékoli jiné vykonané činnosti, včetně přeshraničních činností a zadávání subdodávek.

2. Oznámené subjekty poskytnou ostatním subjektům oznámeným podle tohoto nařízení, které vykonávají obdobné činnosti posuzování shody a zabývají se stejnými produkty, příslušné informace o otázkách týkajících se negativních a na vyžádání pozitivních výsledků posuzování shody.

Článek 39

Výměna zkušeností

Komise organizačně zabezpečuje výměnu zkušeností mezi vnitrostátními orgány členských států, které jsou odpovědné za politiku oznamování.

Článek 40

Koordinace oznámených subjektů

1. Komise zajistí zavedení a řádné provádění vhodné koordinace a spolupráce mezi oznámenými subjekty ve formě meziodvětvové skupiny oznámených subjektů.

2. Členské státy zajistí, aby se jimi oznámené subjekty účastnily práce této skupiny, a to přímo nebo prostřednictvím určených zástupců.

KAPITOLA V

DOZOR NAD TRHEM A VYMÁHÁNÍ PRÁVA

Článek 41

Dozor nad trhem a kontrola produktů s digitálními prvky na trhu Unie

1. Na produkty s digitálními prvky spadající do oblasti působnosti tohoto nařízení se použije nařízení (EU) 2019/1020.

2. Pro účely zajištění účinného provádění tohoto nařízení každý členský stát určí jeden nebo více orgánů dozoru nad trhem. Členské státy mohou určit stávající nebo nový orgán, který bude působit jako orgán dozoru nad trhem pro účely tohoto nařízení.

3. Orgány dozoru nad trhem případně spolupracují s vnitrostátními orgány certifikace kybernetické bezpečnosti určenými podle článku 58 nařízení (EU) 2019/881 a vyměňují si pravidelně informace. Pokud jde o dohled nad plněním povinností podávat zprávy podle článku 11 tohoto nařízení, určené orgány dozoru nad trhem spolupracují s agenturou ENISA.

4. Orgány dozoru nad trhem případně spolupracují s dalšími orgány dozoru nad trhem určenými na základě jiných harmonizačních právních předpisů Unie pro jiné produkty a pravidelně si vyměňují informace.

5. Orgány dozoru nad trhem podle potřeby spolupracují s orgány dohledu nad právními předpisy Unie v oblasti ochrany údajů. Tato spolupráce zahrnuje informování těchto orgánů o veškerých zjištěních relevantních pro plnění jejich pravomocí, a to i při vydávání pokynů a poradenství podle odstavce 8 tohoto článku, pokud se tyto pokyny a poradenství týkají zpracování osobních údajů.

   Orgány vykonávající dohled nad právními předpisy Unie v oblasti ochrany údajů mají pravomoc požadovat jakoukoli dokumentaci vytvořenou nebo vedenou podle tohoto nařízení a přístup k ní, pokud je přístup k této dokumentaci nezbytný pro plnění jejich úkolů. O každé takové žádosti informují určené orgány dozoru nad trhem dotčeného členského státu.

6. Členské státy zajistí, aby určeným orgánům dozoru nad trhem byly poskytnuty odpovídající finanční a lidské zdroje, které jim umožní plnit úkoly podle tohoto nařízení.

7. Komise usnadňuje výměnu zkušeností mezi určenými orgány dozoru nad trhem.

8. Orgány dozoru nad trhem mohou s podporou Komise poskytovat hospodářským subjektům pokyny a poradenství ohledně provádění tohoto nařízení.

9. Orgány dozoru nad trhem každoročně podávají Komisi zprávy o výsledcích příslušných činností v oblasti dozoru nad trhem. Určené orgány dozoru nad trhem neprodleně ohlásí Komisi a příslušným vnitrostátním orgánům pro hospodářskou soutěž veškeré informace zjištěné v průběhu činností v oblasti dozoru nad trhem, které by mohly mít potenciální význam pro uplatňování právních předpisů Unie v oblasti hospodářské soutěže.

10. V případě produktů s digitálními prvky spadajících do oblasti působnosti tohoto nařízení, které jsou klasifikovány jako vysoce rizikové systémy UI podle článku [článek 6] nařízení [nařízení o UI], jsou orgány dozoru nad trhem určené pro účely nařízení [nařízení o UI] orgány odpovědné za činnosti dozoru nad trhem požadované podle tohoto nařízení. Orgány dozoru nad trhem určené podle nařízení [nařízení o UI] spolupracují podle potřeby s orgány dozoru nad trhem určenými podle tohoto nařízení a s agenturou ENISA, pokud jde o dohled nad plněním povinností podávat zprávy podle článku 11. Orgány dozoru nad trhem určené podle nařízení [nařízení o UI] zejména informují orgány dozoru nad trhem určené podle tohoto nařízení o veškerých zjištěních, která jsou relevantní pro plnění jejich úkolů v souvislosti s prováděním tohoto nařízení.

11. Pro jednotné uplatňování tohoto nařízení se zřizuje specializovaná skupina pro správní spolupráci podle čl. 30 odst. 2 nařízení (EU) 2019/1020. Tato skupina pro správní spolupráci se skládá ze zástupců určených orgánů dozoru nad trhem a případně i ze zástupců ústředních styčných úřadů.

Článek 42

Přístup k údajům a dokumentaci

Je-li to nezbytné k posouzení shody produktů s digitálními prvky a postupů zavedených jejich výrobci se základními požadavky stanovenými v příloze I a na základě odůvodněné žádosti, udělí se orgánům dozoru nad trhem přístup k údajům požadovaným pro posouzení návrhu, vývoje, výroby a řešení zranitelnosti těchto produktů, včetně související interní dokumentace příslušného hospodářského subjektu.

Článek 43

Postup na vnitrostátní úrovni týkající se produktů s digitálními prvky představujících významné kybernetické bezpečnostní riziko

1. Pokud má orgán dozoru nad trhem členského státu dostatečné důvody domnívat se, že produkt s digitálními prvky, včetně řešení jeho zranitelnosti, představuje významné kybernetické bezpečnostní riziko, provede hodnocení dotčeného produktu s digitálními prvky z hlediska jeho souladu se všemi požadavky stanovenými v tomto nařízení. Příslušné hospodářské subjekty s orgánem dozoru nad trhem podle potřeby spolupracují.

   Pokud v průběhu tohoto hodnocení orgán dozoru nad trhem zjistí, že produkt s digitálními prvky nesplňuje požadavky stanovené v tomto nařízení, neprodleně vyzve příslušný hospodářský subjekt, aby přijal veškerá vhodná nápravná opatření k uvedení produktu do souladu s těmito požadavky nebo k jeho stažení z trhu nebo z oběhu ve lhůtě, kterou může stanovit a která je přiměřená povaze rizika.

   Orgán dozoru nad trhem o tom informuje příslušný oznámený subjekt. Na vhodná nápravná opatření se použije článek 18 nařízení (EU) 2019/1020.

2. Domnívá-li se orgán dozoru nad trhem, že se nesoulad netýká pouze území jeho členského státu, informuje Komisi a ostatní členské státy o výsledcích hodnocení a o opatřeních, která má subjekt na jeho žádost přijmout.

3. Výrobce zajistí, aby byla přijata všechna vhodná nápravná opatření ohledně všech produktů s digitálními prvky, které dodal na trh v celé Unii.

4. Pokud výrobce produktů s digitálními prvky ve lhůtě uvedené ve druhém pododstavci odstavce 1 nepřijme přiměřená nápravná opatření, přijme orgán dozoru nad trhem všechna vhodná dočasná opatření k omezení nebo zákazu dodávání tohoto produktu na trh svého členského státu nebo k zajištění toho, že je stažen z trhu nebo z oběhu.

   O takových opatřeních tento orgán neprodleně informuje Komisi a ostatní členské státy.

5. Součástí informací uvedených v odstavci 4 jsou všechny dostupné podrobnosti, zejména údaje nezbytné pro identifikaci nevyhovujícího produktu s digitálními prvky, údaje o původu produktu s digitálními prvky, povaze údajného nesouladu a souvisejícího rizika, povaze a době trvání opatření přijatých na vnitrostátní úrovni a údaje o stanovisku příslušného subjektu. Orgán dozoru nad trhem zejména uvede, zda je důvodem nesouladu jeden nebo více těchto nedostatků:

   a) produkt nebo postupy zavedené výrobcem nesplňují základní požadavky stanovené v příloze I;

b) nedostatky v harmonizovaných normách, systémech certifikace kybernetické bezpečnosti nebo obecných specifikacích uvedených v článku 18.

6. Orgány dozoru nad trhem členských států jiné než orgán dozoru nad trhem členského státu, který zahájil tento postup, neprodleně informují Komisi a ostatní členské státy o veškerých opatřeních, která přijaly, a o všech doplňujících údajích týkajících se nesouladu dotčeného produktu, které mají k dispozici, a v případě nesouhlasu s oznámeným vnitrostátním opatřením o svých námitkách.

7. Jestliže do tří měsíců od přijetí informací uvedených v odstavci 4 nevznese žádný členský stát ani Komise námitku proti předběžnému opatření přijatému členským státem, považuje se uvedené opatření za důvodné. Tím nejsou dotčena procesní práva dotčeného subjektu v souladu s článkem 18 nařízení (EU) 2019/1020.

8. Orgány dozoru nad trhem všech členských států zajistí, aby byla v souvislosti s dotčeným produktem bezodkladně přijata náležitá restriktivní opatření, například stažení daného produktu z jejich trhů.

Článek 44

Ochranný postup Unie

1. Pokud do tří měsíců od obdržení oznámení uvedeného v čl. 43 odst. 4 vznese některý členský stát námitky proti opatření přijatému jiným členským státem nebo pokud se Komise domnívá, že je dané opatření v rozporu s právními předpisy Unie, zahájí Komise neprodleně konzultaci s dotčeným členským státem a hospodářským subjektem nebo subjekty a provede hodnocení tohoto vnitrostátního opatření. Na základě výsledků tohoto hodnocení Komise do devíti měsíců od oznámení uvedeného v čl. 43 odst. 4 rozhodne, zda je dané vnitrostátní opatření odůvodněné či nikoli, a toto rozhodnutí oznámí dotčenému členskému státu.

2. Pokud je vnitrostátní opatření považováno za odůvodněné, všechny členské státy přijmou nezbytná opatření k zajištění toho, aby byl nevyhovující produkt s digitálními prvky stažen z jejich trhu, a informují o tom Komisi. Je-li vnitrostátní opatření považováno za neodůvodněné, dotčený členský stát toto opatření zruší.

3. Pokud je vnitrostátní opatření považováno za důvodné a je-li nesoulad produktu s digitálními prvky přisuzován nedostatkům v harmonizovaných normách, použije Komise postup stanovený v článku 10 nařízení (EU) č. 1025/2012.

4. Pokud je vnitrostátní opatření považováno za důvodné a je-li nesoulad produktu s digitálními prvky přisuzován nedostatkům v evropském systému certifikace kybernetické bezpečnosti podle článku 18, Komise zváží, zda změnit nebo zrušit prováděcí akt uvedený v čl. 18 odst. 4, který stanoví předpoklad shody týkající se daného systému certifikace.

5. Pokud je vnitrostátní opatření považováno za důvodné a je-li nesoulad produktu s digitálními prvky přisuzován nedostatkům v obecných specifikacích podle článku 19, Komise zváží, zda změnit nebo zrušit prováděcí akt uvedený v článku 19, kterým se stanoví tyto obecné specifikace.

Článek 45

Postup na úrovni EU týkající se produktů s digitálními prvky představujících významné kybernetické bezpečnostní riziko

1. Pokud má Komise dostatečné důvody se domnívat, a to i na základě informací poskytnutých agenturou ENISA, že produkt s digitálními prvky, který představuje významné kybernetické bezpečnostní riziko, není v souladu s požadavky stanovenými v tomto nařízení, může požádat příslušné orgány dozoru nad trhem, aby provedly hodnocení souladu a řídily se postupy uvedenými v článku 43.

2. Za výjimečných okolností, které odůvodňují okamžitý zásah za účelem zachování řádného fungování vnitřního trhu, a pokud má Komise dostatečné důvody domnívat se, že produkt uvedený v odstavci 1 stále nesplňuje požadavky stanovené v tomto nařízení a příslušné orgány dozoru nad trhem nepřijaly účinná opatření, může Komise požádat agenturu ENISA, aby provedla hodnocení souladu. Komise v tom smyslu informuje příslušné orgány dozoru nad trhem. Příslušné hospodářské subjekty s agenturou ENISA podle potřeby spolupracují.

3. Na základě hodnocení agentury ENISA může Komise rozhodnout, že je zapotřebí nápravného nebo omezujícího opatření na úrovni Unie. Za tímto účelem neprodleně konzultuje dotčené členské státy a příslušný hospodářský subjekt nebo subjekty.

4. Na základě konzultace uvedené v odstavci 3 může Komise přijmout prováděcí akty s cílem rozhodnout o nápravných nebo omezujících opatřeních na úrovni Unie, včetně nařízení stažení z trhu nebo z oběhu, a to v přiměřené lhůtě úměrné povaze rizika. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 51 odst. 2.

5. Komise o svém rozhodnutí podle odstavce 4 neprodleně uvědomí příslušný hospodářský subjekt či subjekty. Členské státy tyto akty podle odstavce 4 neodkladně provedou a odpovídajícím způsobem informují Komisi.

6. Odstavce 2 až 5 se použijí po dobu trvání výjimečné situace, která odůvodňovala zásah Komise, a dokud příslušný produkt není uveden do souladu s tímto nařízením.

Článek 46

Vyhovující produkty s digitálními prvky, které představují významné kybernetické bezpečnostní riziko

1. Pokud po provedení hodnocení podle článku 43 orgán dozoru nad trhem členského státu zjistí, že ačkoli jsou produkt s digitálními prvky a postupy zavedené výrobcem v souladu s tímto nařízením, představují významné kybernetické bezpečnostní riziko, a navíc představují riziko pro zdraví nebo bezpečnost osob, pro dodržování povinností podle unijního nebo vnitrostátního práva, jejichž cílem je ochrana základních práv, pro pravost, důvěryhodnost nebo důvěrnost služeb nabízených prostřednictvím elektronického informačního systému zásadními subjekty druhu uvedeného v [příloha I směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] nebo pro jiné aspekty ochrany veřejného zájmu, vyzve orgán dozoru příslušný subjekt, aby přijal veškerá vhodná opatření k zajištění toho, že produkt s digitálními prvky a postupy zavedené dotčeným výrobcem při uvedení na trh již toto riziko nepředstavují, nebo aby produkt s digitálními prvky stáhl z trhu nebo z oběhu ve lhůtě přiměřené povaze rizika.

2. Výrobce nebo jiné příslušné subjekty zajistí, aby bylo přijato nápravné opatření ve vztahu ke všem dotčeným produktům s digitálními prvky, které dodali na trh v rámci celé Unie, ve lhůtě stanovené orgánem dozoru nad trhem členského státu uvedeného v odstavci 1.

3. Členský stát neprodleně informuje Komisi a ostatní členské státy o opatřeních přijatých podle odstavce 1. Tato informace musí obsahovat všechny dostupné podrobnosti, zejména údaje nezbytné pro identifikaci dotčeného produktu s digitálními prvky, údaje o původu a dodavatelském řetězci těchto produktů s digitálními prvky, údaje o povaze souvisejícího rizika a údaje o povaze a době trvání opatření přijatých na vnitrostátní úrovni.

4. Komise neprodleně zahájí konzultaci s členskými státy a příslušným hospodářským subjektem a vyhodnotí přijatá vnitrostátní opatření. Na základě výsledků tohoto hodnocení Komise rozhodne, zda je opatření důvodné či nikoli, a pokud je to nutné, navrhne vhodná opatření.

5. Rozhodnutí Komise je určeno všem členským státům.

6. Pokud má Komise dostatečné důvody se domnívat, a to i na základě informací poskytnutých agenturou ENISA, že produkt s digitálními prvky, ačkoli je v souladu s tímto nařízením, představuje rizika uvedená v odstavci 1, může požádat příslušný orgán nebo orgány dozoru nad trhem, aby provedly hodnocení souladu a řídily se postupy uvedenými v článku 43 a odstavcích 1, 2 a 3 tohoto článku.

7. Za výjimečných okolností, které odůvodňují okamžitý zásah za účelem zachování řádného fungování vnitřního trhu, a pokud má Komise dostatečné důvody domnívat se, že produkt uvedený v odstavci 6 nadále představuje rizika podle odstavce 1 a příslušné vnitrostátní orgány dozoru nad trhem nepřijaly účinná opatření, může Komise požádat agenturu ENISA, aby provedla hodnocení rizik, která tento produkt představuje, a informuje o tom příslušné orgány dozoru nad trhem. Příslušné hospodářské subjekty s agenturou ENISA podle potřeby spolupracují.

8. Na základě hodnocení agentury ENISA podle odstavce 7 může Komise stanovit, že je zapotřebí nápravného nebo omezujícího opatření na úrovni Unie. Za tímto účelem neprodleně konzultuje dotčené členské státy a příslušný subjekt nebo subjekty.

9. Na základě konzultace uvedené v odstavci 8 může Komise přijmout prováděcí akty s cílem rozhodnout o nápravných nebo omezujících opatřeních na úrovni Unie, včetně nařízení stažení z trhu nebo z oběhu, a to v přiměřené lhůtě úměrné povaze rizika. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 51 odst. 2.

10. Komise o svém rozhodnutí podle odstavce 9 neprodleně uvědomí příslušný subjekt či subjekty. Členské státy tyto akty neodkladně provedou a odpovídajícím způsobem informují Komisi.

11. Odstavce 6 až 10 se použijí po dobu trvání výjimečné situace, která odůvodňovala zásah Komise, a po dobu, po kterou příslušný produkt nadále představuje rizika uvedená v odstavci 1.

Článek 47

Formální nesoulad

1. Orgán dozoru nad trhem daného členského státu požádá příslušného výrobce, aby odstranil dotčený nesoulad, pokud zjistí jeden z těchto nedostatků:

   a) označení shody bylo umístěno v rozporu s články 21 a 22;

   b) označení shody nebylo umístěno;

   c) nebylo vypracováno EU prohlášení o shodě;

d) EU prohlášení o shodě nebylo vypracováno správně;

e) nebylo umístěno identifikační číslo oznámeného subjektu, který je případně zapojen do postupu posuzování shody;

f) technická dokumentace chybí nebo je neúplná.

2. Pokud nesoulad uvedený v odstavci 1 nadále trvá, přijme dotčený členský stát veškerá vhodná opatření s cílem omezit nebo zakázat dodávání produktu s digitálními prvky na trh, nebo zajistit, aby byl stažen z oběhu nebo z trhu.

Článek 48

Společné činnosti orgánů dozoru nad trhem

1. Orgány dozoru nad trhem se mohou dohodnout s dalšími příslušnými orgány na provádění společných činností zaměřených na zajištění kybernetické bezpečnosti a ochrany spotřebitelů, pokud jde o konkrétní produkty s digitálními prvky uváděné nebo dodávané na trh, zejména produkty, u nichž se často zjistí, že představují kybernetická bezpečnostní rizika.

2. Komise nebo agentura ENISA mohou navrhnout společné činnosti pro kontrolu souladu s tímto nařízením, které budou provádět orgány dozoru nad trhem na základě údajů nebo informací o možném nesouladu produktů spadajících do oblasti působnosti tohoto nařízení v několika členských státech s požadavky stanovenými tímto nařízením.

3. Orgány dozoru nad trhem a případně Komise zajistí, aby dohoda o provádění společných činností nevedla k nekalé soutěži mezi hospodářskými subjekty a nepříznivě nenarušovala objektivitu, nezávislost a nestrannost stran dohody.

4. Orgán dozoru nad trhem může použít jakékoli informace vyplývající ze společných činností vykonávaných v rámci jakéhokoli jeho šetření, které provádí.

5. Dotčený orgán dozoru nad trhem a případně Komise zveřejní dohodu o společných činnostech, včetně jmen zúčastněných stran.

Článek 49

Společné kontrolní akce (tzv. sweepy)

1. Orgány dozoru nad trhem se mohou rozhodnout provádět souběžné koordinované kontrolní akce („sweepy“) u konkrétních produktů s digitálními prvky nebo jejich kategorií za účelem kontroly souladu s tímto nařízením nebo odhalení porušení tohoto nařízení.

2. Pokud se zapojené příslušné orgány dozoru nad trhem nedohodnou jinak, jsou společné kontrolní akce koordinovány Komisí. Koordinátor společné kontrolní akce může dle potřeby zveřejnit agregované výsledky.

3. Agentura ENISA může při plnění svých úkolů, mimo jiné na základě oznámení obdržených podle čl. 11 odst. 1 a 2, určit kategorie produktů, u nichž mohou být organizovány kontrolní akce. Návrh kontrolních akcí se předkládá možnému koordinátorovi podle odstavce 2 k posouzení orgánů dozoru nad trhem.

4. Zapojené orgány dozoru nad trhem mohou při provádění společných kontrolních akcí účinně využívat vyšetřovací pravomoci stanovené v článcích 41 až 47 a jakékoli další pravomoci, které jim svěřuje vnitrostátní právo.

5. Orgány dozoru nad trhem mohou k účasti na společných kontrolních akcích přizvat úředníky Komise a další doprovázející osoby pověřené Komisí.

KAPITOLA VI

PŘENESENÉ PRAVOMOCI A POSTUP PROJEDNÁVÁNÍ VE VÝBORU

Článek 50

Výkon přenesení pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 2 odst. 4, čl. 6 odst. 2, čl. 6 odst. 3, čl. 6 odst. 5, čl. 20 odst. 5 a čl. 23 odst. 5 je svěřena Komisi.

3. Evropský parlament nebo Rada mohou přenesení pravomocí uvedené v čl. 2 odst. 4, čl. 6 odst. 2, čl. 6 odst. 3, čl. 6 odst. 5, čl. 20 odst. 5 a čl. 23 odst. 5 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie*, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Před přijetím aktu v přenesené pravomoci vede Komise konzultace s odborníky jmenovanými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů.

5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

6. Akt v přenesené pravomoci přijatý podle čl. 2 odst. 4, čl. 6 odst. 2, čl. 6 odst. 3, čl. 6 odst. 5, čl. 20 odst. 5 a čl. 23 odst. 5 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 51

Postup projednávání ve výboru

1. Komisi je nápomocen výbor. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

3. Má-li být stanovisko výboru získáno písemným postupem, je tento postup ukončen bez výsledku, pokud tak o tom ve lhůtě stanovené pro vydání stanoviska rozhodne předseda výboru nebo pokud o to požádá člen výboru.

KAPITOLA VII

DŮVĚRNOST A SANKCE

Článek 52

Zachování důvěrnosti

1. Všechny strany, které se podílejí na uplatňování tohoto nařízení, zachovávají důvěrnost informací a údajů, které získají při provádění svých úkolů a činností, takovým způsobem, aby chránily zejména:

   a) práva duševního vlastnictví a důvěrné obchodní informace nebo obchodní tajemství fyzických nebo právnických osob, včetně zdrojového kódu, s výjimkou případů, na které se vztahuje článek 5 směrnice Evropského parlamentu a Rady 2016/943[24];

   b) účinné provádění tohoto nařízení, zejména za účelem inspekcí, šetření nebo auditů;

   c) veřejné a národní bezpečnostní zájmy;

   d) integritu trestního nebo správního řízení.

2. Aniž je dotčen odstavec 1, informace vyměňované důvěrně mezi orgány dozoru nad trhem a mezi orgány dozoru nad trhem a Komisí se nezpřístupní bez předchozí dohody s orgánem dozoru nad trhem, od kterého informace pocházejí.

3. Ustanoveními odstavců 1 a 2 nejsou dotčena práva a povinnosti Komise, členských států a oznámených subjektů ohledně vzájemného informování a šíření výstrah ani povinnosti dotčených osob poskytovat informace podle trestního práva členských států.

4. Komise a členské státy si mohou v případě potřeby vyměňovat citlivé informace s relevantními orgány třetích zemí, s nimiž uzavřely dvoustranná nebo vícestranná ujednání o ochraně důvěrnosti zaručující přiměřenou úroveň ochrany.

Článek 53

Sankce

1. Členské státy stanoví pravidla pro sankce za porušení tohoto nařízení hospodářskými subjekty a přijmou veškerá opatření nezbytná k jejich prosazování. Tyto sankce musí být účinné, přiměřené a odrazující.

2. Členské státy bez prodlení uvědomí o takových pravidlech a takových opatřeních Komisi a neprodleně ji informují o jakýchkoli pozdějších změnách těchto pravidel nebo opatření.

3. Za nedodržení základních požadavků na kybernetickou bezpečnost stanovených v příloze I a povinností stanovených v článcích 10 a 11 se uloží správní pokuty až do výše 15 000 000 EUR, nebo, dopustí-li se porušení podnik, až do výše 2,5 % jeho

[24] Směrnice Evropského parlamentu a Rady (EU) 2016/943 ze dne 8. června 2016 o ochraně nezveřejněného know-how a obchodních informací (obchodního tajemství) před jejich neoprávněným získáním, využitím a zpřístupněním (Úř. věst. L 157, 15.6.2016, s. 1).

celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší.

4. Za nedodržení jakýchkoli jiných povinností podle tohoto nařízení se uloží správní pokuty až do výše 10 000 000 EUR nebo, dopustí-li se porušení podnik, až do výše 2 % jeho celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší.

5. Za poskytnutí nesprávných, neúplných nebo zavádějících informací oznámeným subjektům a orgánům dozoru nad trhem v reakci na žádost se uloží správní pokuty až do výše 5 000 000 EUR, nebo, dopustí-li se porušení podnik, až do výše 1 % jeho celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší.

6. Při rozhodování o výši správní pokuty v jednotlivých případech se zohlední všechny příslušné okolnosti konkrétní situace s náležitým přihlédnutím k následujícím okolnostem:

   a) povaha, závažnost a doba trvání porušení těchto ustanovení a jeho následky;

   b) zda již byly stejnému subjektu za podobné protiprávní jednání uloženy správní pokuty jinými orgány dozoru nad trhem;

   c) velikost subjektu, který se porušení dopustil, a jeho podíl na trhu.

7. Orgány dozoru nad trhem, které ukládají správní pokuty, sdílejí tyto informace s orgány dozoru nad trhem jiných členských států prostřednictvím informačního a komunikačního systému podle článku 34 nařízení (EU) 2019/1020.

8. Každý členský stát stanovuje pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.

9. V závislosti na právním systému členských států lze pravidla pro správní pokuty použít tak, aby pokuty byly ukládány příslušnými vnitrostátními soudy nebo jinými orgány v souladu s pravomocemi stanovenými na vnitrostátní úrovni v těchto členských státech. Uplatňování těchto pravidel v uvedených členských státech má rovnocenný účinek.

10. Správní pokuty mohou být uloženy v závislosti na okolnostech každého jednotlivého případu spolu s jakýmikoli dalšími nápravnými nebo omezujícími opatřeními, které uplatní orgány dozoru nad trhem v souvislosti se stejným protiprávním jednáním.

KAPITOLA VIII

PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ

Článek 54

Změna nařízení (EU) 2019/1020

V příloze I nařízení (EU) 2019/1020 se doplňuje nový bod, který zní:

„71. [nařízení XXX] [akt o kybernetické odolnosti]“.

Článek 55

Přechodná ustanovení

1. Certifikáty EU přezkoušení typu a rozhodnutí o schválení vydané v souvislosti s požadavky na kybernetickou bezpečnost produktů s digitálními prvky, které podléhají jiným harmonizačním právním předpisům Unie, zůstávají v platnosti po dobu [42 měsíců ode dne vstupu tohoto nařízení v platnost], pokud jejich platnost neskončí před tímto datem nebo pokud není stanoveno jinak v jiných právních předpisech Unie, přičemž v tomto případě zůstávají v platnosti podle uvedených právních předpisů Unie.
2. Produkty s digitálními prvky, které byly uvedeny na trh před [datum použitelnosti tohoto nařízení uvedené v článku 57], se řídí požadavky tohoto nařízení pouze tehdy, pokud po uvedeném datu procházejí tyto produkty podstatnými změnami svého návrhu nebo zamýšleného účelu.
3. Odchylně od odstavce 2 se povinnosti stanovené v článku 11 vztahují na všechny produkty s digitálními prvky spadající do oblasti působnosti tohoto nařízení, které byly uvedeny na trh před [datum použitelnosti tohoto nařízení uvedené v článku 57].

Článek 56

Hodnocení a přezkum

Do [36 měsíců ode dne použitelnosti tohoto nařízení] a poté každé čtyři roky předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení. Tyto zprávy se zveřejní.

Článek 57

Vstup v platnost a použitelnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Použije se ode dne [24 měsíců po vstupu tohoto nařízení v platnost]. Článek 11 se však použije ode dne [12 měsíců po vstupu tohoto nařízení v platnost].

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda/předsedkyně	*předseda/předsedkyně*

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

1.2. Příslušné oblasti politik

1.3. Návrh/podnět se týká:

1.4. Cíle

1.4.1. Obecné cíle

1.4.2. Specifické cíle

1.4.3. Očekávané výsledky a dopady

1.4.4. Ukazatele výkonnosti

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

1.5.4. Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

1.6. Doba trvání a finanční dopad návrhu/podnětu

1.7. Předpokládaný způsob řízení

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

2.3. Opatření k zamezení podvodů a nesrovnalostí

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

3.2. Odhadovaný finanční dopad návrhu na prostředky

3.2.1. Odhadovaný souhrnný dopad na operační prostředky

3.2.2. Odhadovaný výstup financovaný z operačních prostředků

3.2.3. Odhadovaný souhrnný dopad na správní prostředky

3.2.4. Slučitelnost se stávajícím víceletým finančním rámcem

3.2.5. Příspěvky třetích stran

3.3. Odhadovaný dopad na příjmy

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Návrh nařízení o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky (akt o kybernetické odolnosti)

1.2. Příslušné oblasti politik

Komunikační sítě, obsah a technologie

1.3. Návrh/podnět se týká:

× **nové akce**

☐ **nové akce následující po pilotním projektu / přípravné akci**[37]

☐ **prodloužení stávající akce**

☐ **sloučení jedné či více akcí v jinou/novou akci nebo přesměrování jedné či více akcí na jinou/novou akci**

1.4. Cíle

1.4.1. Obecné cíle

Návrh má dva hlavní cíle za účelem zajištění řádného fungování vnitřního trhu: 1) **vytvořit podmínky pro vývoj bezpečných produktů s digitálními prvky** tím, že bude zajištěno, aby hardwarové a softwarové produkty byly uváděny na trh s méně zranitelnostmi a aby výrobci brali vážně bezpečnost v průběhu celého životního cyklu produktu, a 2) **vytvořit podmínky umožňující uživatelům, aby při výběru a používání produktů s digitálními prvky zohlednili kybernetickou bezpečnost**.

1.4.2. Specifické cíle

Byly stanoveny **čtyři specifické cíle**: i) zajistit, aby výrobci zlepšili bezpečnost produktů digitálními prvky od fáze návrhu a vývoje a během celého životního cyklu; ii) zajistit soudržný rámec kybernetické bezpečnosti, který výrobcům hardwaru a softwaru usnadní dodržování předpisů; iii) zvýšit transparentnost bezpečnostních vlastností produktů s digitálními prvky a iv) umožnit podnikům a spotřebitelům bezpečné používání produktů s digitálními prvky.

Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Návrh by měl významné výhody pro různé zúčastněné strany. V případě podniků by zabránil rozdílným bezpečnostním pravidlům pro produkty s digitálními prvky a snížil by náklady na dodržování příslušných právních předpisů v oblasti kybernetické bezpečnosti. Došlo by ke snížení počtu kybernetických incidentů, nákladů na řešení incidentů a újmy na dobré pověsti. Odhaduje se, že v celé EU by tato iniciativa mohla vést ke snížení nákladů v důsledku incidentů postihujících společnosti o

[37] Uvedené v čl. 58 odst. 2 písm. a) nebo b) finančního nařízení.

přibližně 180 miliard EUR až 290 miliard EUR ročně[38]. Vedla by ke zvýšení obratu v důsledku využívání produktů s požadavkem na digitální prvky. Zlepšila by se tak celosvětová pověst společností, což by vedlo k nárůstu poptávky i mimo EU. Pro uživatele by upřednostňovaná možnost zvýšila transparentnost bezpečnostních vlastností a usnadnila by využívání produktů s digitálními prvky. Spotřebitelé a občané by rovněž těžili z lepší ochrany svých základních práv, například ochrany soukromí a údajů.

Návrh by zároveň zvýšil náklady na dodržování předpisů a vymáhání pro podniky, oznámené subjekty a veřejné orgány, včetně akreditačních orgánů a orgánů dozoru nad trhem. Vývojářům softwaru a výrobcům hardwaru se zvýší přímé náklady na dodržování nových bezpečnostních požadavků, povinností posuzování shody, dokumentačních povinností a povinností v oblasti podávání zpráv, což povede k souhrnným nákladům na dodržování předpisů ve výši přibližně 29 miliard EUR při odhadované tržní hodnotě obratu 1 485 miliard EUR[39]. Uživatelé, včetně podnikatelských uživatelů, spotřebitelů a občanů, mohou čelit vyšším cenám produktů s digitálními prvky. Je však třeba na ně nahlížet v kontextu výše popsaných významných přínosů.

1.4.3. Ukazatele výkonnosti

Upřesněte ukazatele pro sledování pokroku a dosažených výsledků.

S cílem ověřit, zda výrobci zlepšují bezpečnost svých produktů s digitálními prvky od fáze návrhu a vývoje i během celého životního cyklu těchto produktů, lze vzít v úvahu několik ukazatelů. Mohlo by se jednat o počet závažných incidentů v Unii způsobených zranitelnostmi, podíl výrobců hardwaru a softwaru, kteří dodržují systematický bezpečný životní cyklus vývoje, kvalitativní analýzu bezpečnosti produktů s digitálními prvky, kvantitativní a kvalitativní posouzení databází zranitelností, četnost bezpečnostních oprav poskytovaných výrobci nebo průměrný počet dní mezi odhalením zranitelnosti a poskytnutím bezpečnostních oprav.

Ukazatelem soudržného rámce kybernetické bezpečnosti by mohla být neexistence cílených vnitrostátních právních předpisů v oblasti kybernetické bezpečnosti zaměřených na konkrétní produkty.

Ukazatelem zvýšené transparentnosti, pokud jde o bezpečnostní vlastnosti produktů s digitálními prvky, by mohl být podíl produktů s digitálními prvky, které jsou dodávány s informacemi o bezpečnostních vlastnostech. Kromě toho by podíl produktů s digitálními prvky, které jsou dodávány s uživatelskými pokyny pro bezpečné použití, mohl sloužit jako ukazatel toho, zda organizace a spotřebitelé mohou produkty s digitálními prvky bezpečně používat.

Pokud jde o sledování dopadu nařízení, pro tento účel by byly zváženy některé ukazatele, které Komise posoudí případně i za pomoci agentury ENISA. V závislosti na operativním cíli, kterého má být dosaženo, existují následující ukazatele sledování, na jejichž základě by byl hodnocen úspěch horizontálních požadavků na kybernetickou bezpečnost, tyto:

Pro posouzení úrovně kybernetické bezpečnosti produktů s digitálními prvky:

[38] Viz [pracovní dokument útvarů Komise o zprávě o posouzení dopadů doprovázející nařízení o horizontálních požadavcích na kybernetickou bezpečnost u produktů s digitálními prvky].

[39] Viz [pracovní dokument útvarů Komise o zprávě o posouzení dopadů doprovázející nařízení o horizontálních požadavcích na kybernetickou bezpečnost u produktů s digitálními prvky].

- Statistika a kvalitativní analýza incidentů postihujících produkty s digitálními prvky a způsobu, jak byly řešeny. Mohla by je shromažďovat a posuzovat Komise za podpory agentury ENISA.

- Záznamy o známých zranitelnostech a analýzy toho, jak byly řešeny. Tuto analýzu by mohla provádět agentura ENISA na základě Evropské databáze zranitelností zřízené na základě [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)].

- Průzkumy mezi výrobci hardwaru a softwaru za účelem sledování pokroku.

V případě posuzování úrovně informací o bezpečnostních prvcích, bezpečnostní podpoře, konci životnosti a povinnosti péče: výsledky průzkumů, které provede Komise s podporou agentury ENISA jak u uživatelů, tak u podniků.

V případě posuzování provádění by Komise usilovala o zajištění účinného provádění posuzování shody. Za tímto účelem bude vydána žádost o normalizaci a bude se sledovat její provádění. Komise rovněž ověří kapacitu oznámených subjektů a případně certifikačních subjektů.

Pokud jde o použitelnost, Komise prostřednictvím zpráv členských států ověří, zda se vnitrostátní iniciativy netýkají aspektů, na něž se vztahuje nařízení.

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu

Nařízení by mělo být plně použitelné 24 měsíců po svém vstupu v platnost. Některé prvky správní struktury by však měly být zavedeny ještě dříve. Členské státy mají jmenovány stávající orgány a/nebo zřízeny nové orgány, které plní úkoly stanovené již dříve v právních předpisech.

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

Silná přeshraniční povaha kybernetické bezpečnosti a rostoucí počet incidentů, které se přelévají přes hranice a mezi odvětvími a produkty znamená, že tyto cíle nemohou členské státy účinně dosáhnout samy. Vzhledem ke globální povaze trhů s produkty s digitálními prvky čelí členské státy stejným rizikům u téhož produktu s digitálními prvky na svém území. Vznikající nejednotný rámec potenciálně odlišných vnitrostátních pravidel může také narušit otevřený a konkurenceschopný jednotný trh produktů s digitálními prvky. Pro zvýšení důvěry mezi uživateli a přitažlivosti produktů EU s digitálními prvky je proto nezbytná společná akce na úrovni EU. Prospěla by rovněž vnitřnímu trhu tím, že by prodejcům produktů s digitálními prvky poskytla právní jistotu a zajistila rovné podmínky.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Akt o kybernetické odolnosti je prvním nařízením svého druhu, které zavádí požadavky na kybernetickou bezpečnost pro uvádění produktů s digitálními prvky na trh. Vychází však ze stanovení nového legislativního rámce a ze zkušeností získaných v procesu provádění stávajících harmonizačních právních předpisů Unie

týkajících se různých produktů, zejména pokud jde o přípravu na provádění, včetně aspektů, jako je například příprava harmonizovaných norem.

1.5.4. Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji

Nařízení o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky definuje nové požadavky na kybernetickou bezpečnost pro všechny produkty s digitálními prvky uváděné na trh EU, které jdou nad rámec požadavků stanovených stávajícími právními předpisy. Návrh zároveň vychází ze stávajícího uspořádání právních předpisů tvořících nový právní rámec. Proto by vycházel ze stávajících struktur a postupů nového právního rámce, například spolupráce oznámených subjektů a dozoru nad trhem, modulů posuzování shody a vypracování harmonizovaných norem. Nový návrh by se rovněž opíral o některé struktury vytvořené podle jiných právních předpisů v oblasti kybernetické bezpečnosti, například směrnice 2016/1148 (směrnice o bezpečnosti sítí a informací), [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] nebo nařízení 2019/881 (akt o kybernetické bezpečnosti).

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

Řízení oblastí činnosti přidělených agentuře ENISA odpovídá jejímu stávajícímu mandátu a všeobecným úkolům. Tyto oblasti činnosti mohou vyžadovat specifické profily nebo nové úkoly, které by však nebyly významné a mohly by být zvládnuty pomocí stávajících zdrojů agentury ENISA a vyřešeny přerozdělením nebo propojením různých úkolů. Například jedna z hlavních oblastí činnosti agentury ENISA se týká shromažďování a zpracovávání oznámení výrobců o zneužívaných zranitelností produktů. [Směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] již agenturu ENISA pověřila zřízením evropské databáze zranitelností, v níž mohou být dobrovolně zpřístupňovány a registrovány veřejně známé zranitelnosti, aby uživatelé mohli přijmout vhodná zmírňující opatření. Zdroje přidělené na tento účel by mohly být rovněž použity na nové, výše uvedené úkoly týkající se oznamování zranitelnosti produktů. Mohlo by se tak zajistit účinné využívání stávajících zdrojů a vytvořilo by to rovněž nezbytné synergie mezi těmito úkoly, které by mohly přinášet lepší informace pro analýzy agentury ENISA týkající se kybernetických bezpečnostních rizik a hrozeb.

1.6. Doba trvání a finanční dopad návrhu/podnětu

☐ **časově omezená doba trvání**

– ☐ s platností od [DD.MM.]RRRR do [DD.MM.]RRRR,

– ☐ finanční dopad od RRRR do RRRR u prostředků na závazky a od RRRR do RRRR u prostředků na platby.

× **časově neomezená doba trvání**

– Provádění s obdobím rozběhu od roku 2025,

– poté plné fungování.

1.7. Předpokládaný způsob řízení[40]

☐ **Přímé řízení** Komisí

– × prostřednictvím jejích útvarů, včetně jejích zaměstnanců v delegacích Unie,

– ☐ prostřednictvím výkonných agentur.

☐ **Sdílené řízení** s členskými státy

☐ **Nepřímé řízení**, při kterém jsou úkoly souvisejícími s plněním rozpočtu pověřeny:

– ☐ třetí země nebo subjekty určené těmito zeměmi,

– ☐ mezinárodní organizace a jejich agentury (upřesněte),

– ☐ EIB a Evropský investiční fond,

– ☐ subjekty uvedené v článcích 70 a 71 finančního nařízení,

– ☐ veřejnoprávní subjekty,

– ☐ soukromoprávní subjekty pověřené výkonem veřejné služby v rozsahu, v jakém jim byly poskytnuty dostatečné finanční záruky,

– ☐ soukromoprávní subjekty členského státu pověřené uskutečňováním partnerství veřejného a soukromého sektoru a poskytující dostatečné finanční záruky,

– ☐ osoby pověřené prováděním specifických akcí v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU a určené v příslušném základním právním aktu.

– *Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.*

Poznámky

Tímto nařízením se agentuře ENISA svěřují určité činnosti v souladu s jejím stávajícím mandátem, a zejména s čl. 3 odst. 2 nařízení 2019/881, který stanoví, že agentura ENISA by měla plnit úkoly, které jí byly svěřeny právními akty Unie, jež stanoví opatření pro sbližování právních a správních předpisů členských států týkajících se kybernetické bezpečnosti. Agentura ENISA má zejména za úkol přijímat oznámení od výrobců o aktivně zneužívaných zranitelnostech obsažených v produktech s digitálními prvky, jakož i o incidentech, které mají dopad na bezpečnost těchto produktů. Agentura ENISA by měla tato oznámení rovněž předávat příslušným skupinám pro reakci na počítačové bezpečnostní incidenty (CSIRT) nebo

[40] Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

příslušným jednotným kontaktním místům členských států určených v souladu s článkem [článek X] směrnice [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)] a informovat příslušné orgány dozoru nad trhem o oznámené zranitelnosti. Na základě shromážděných informací by agentura ENISA měla každé dva roky vypracovat technickou zprávu o nových trendech týkajících se kybernetických bezpečnostních rizik u produktů s digitálními prvky a předložit ji skupině pro spolupráci v oblasti bezpečnosti sítí a informací. Kromě toho může agentura ENISA s ohledem na své odborné znalosti, shromážděné informace a analýzy hrozeb podpořit postup provádění tohoto nařízení tím, že navrhne společné činnosti, které mají provádět vnitrostátní orgány dozoru nad trhem na základě údajů nebo informací o možném nesouladu produktů s digitálními prvky s tímto nařízením v některých členských státech, nebo určí kategorie produktů, pro něž mohou být organizovány souběžné koordinované kontrolní činnosti. Komise může agenturu ENISA požádat, aby za výjimečných okolností provedla hodnocení konkrétních produktů ve vztahu s produkty s digitálními prvky, které představují významné kybernetické bezpečnostní riziko, a je-li k zachování řádného fungování vnitřního trhu nutný okamžitý zásah.

Všechny tyto úkoly se odhadují na přibližně 4,5 plného pracovního úvazku ze stávajících zdrojů agentury ENISA, přičemž se již vychází z odborných znalostí a přípravných prací, které agentura ENISA v současné době provádí, mimo jiné na podporu nadcházejícího provádění [směrnice XXX/XXXX (o bezpečnosti sítí a informací 2)], pro kterou byly zdroje agentury ENISA doplněny.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Do 36 měsíců ode dne použitelnosti tohoto nařízení a poté každé čtyři roky předloží Komise Evropskému parlamentu a Radě zprávu o svém hodnocení a přezkumu. Tyto zprávy se zveřejní.

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

Toto nařízení zavádí novou politiku, pokud jde o harmonizované požadavky na kybernetickou bezpečnost produktů s digitálními prvky uváděných na vnitřní trh během celého jejich životního cyklu. Po právním aktu budou následovat žádosti Komise adresované evropským normalizačním orgánům o vypracování norem.

K plnění těchto nových úkolů je nutné poskytnout útvarům Komise náležité zdroje. Odhaduje se, že pro prosazování nového nařízení bude potřeba 7 plných pracovních úvazků (z toho jeden VNO) s cílem plnit následující úkoly:

- příprava žádosti o normalizaci a/nebo obecných specifikací prostřednictvím prováděcích aktů bez úspěšného procesu normalizace,
- vypracování aktu v přenesené pravomoci [do 12 měsíců od vstupu tohoto nařízení v platnost], kterým se stanoví definice kritických produktů s digitálními prvky,
- případná příprava aktů v přenesené pravomoci pro aktualizaci seznamu kritických produktů třídy I a II, upřesnění, zda je omezení nebo vyloučení nutné i pro produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie, která stanovují požadavky dosahující stejné úrovně ochrany jako toto nařízení, pověření certifikovat některé vysoce kritické produkty s digitálními prvky na základě kritérií stanovených v tomto nařízení, upřesnění minimálního obsahu EU prohlášení o shodě a doplnění prvků, které mají být obsaženy v technické dokumentaci,
- případná příprava prováděcích aktů týkajících se formátu nebo prvků oznamovací povinnosti, softwarového kusovníku, obecných specifikací nebo umístění označení CE,
- případně příprava okamžitého zásahu za účelem uložení nápravných nebo omezujících opatření za výjimečných okolností s cílem zachovat řádné fungování vnitřního trhu, včetně přípravy prováděcího aktu,
- organizace a koordinace oznámení oznámených subjektů členskými státy a koordinace oznámených subjektů,
- podpora koordinace orgánů dozoru nad trhem členských států.

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

S cílem zajistit, aby si oznámené subjekty a orgány dozoru nad trhem vyměňovaly informace a dobře spolupracovaly, je za jejich koordinaci odpovědná Komise. Pro technické a tržní odborné znalosti by byla vytvořena skupina odborníků.

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

2.3. Pokud jde o výdaje na zasedání, vzhledem k nízké hodnotě na transakci (například úhrada cestovních nákladů delegátovi vyslanému na zasedání) se jeví jako dostatečné standardní kontrolní postupy. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření, např. opatření uvedená ve strategii pro boj proti podvodům.

Stávající opatření k předcházení podvodům vztahující se na Komisi budou zahrnovat dodatečné prostředky potřebné pro toto nařízení.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

- Stávající rozpočtové položky

Schéma

- Nové rozpočtové položky, jejichž vytvoření se požaduje

nepoužije se

3.2. Odhadovaný finanční dopad návrhu na prostředky

3.2.1. Odhadovaný souhrnný dopad na operační prostředky

– ☑ Návrh/podnět nevyžaduje využití operačních prostředků.

– ☐ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	Číslo	

GŘ: <…….>			Rok **N**[41]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			**CELKEM**
• Operační prostředky										
Rozpočtová položka[42]	Závazky	(1a)								
	Platby	(2a)								
Rozpočtová položka	Závazky	(1b)								
	Platby	(2b)								
Prostředky správní povahy financované z rámce na zvláštní programy[43]										
Rozpočtová položka		(3)								
Prostředky na GŘ <…….> CELKEM	Závazky	=1a+1b +3								
	Platby	=2a+2b +3								

[41] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

[42] Podle oficiální rozpočtové nomenklatury.

[43] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

• Operační prostředky CELKEM	Závazky	(4)								
	Platby	(5)								
• Prostředky správní povahy financované z rámce na zvláštní programy CELKEM		(6)								
Prostředky z OKRUHU <….> víceletého finančního rámce **CELKEM**	Závazky	=4+6								
	Platby	=5+6								

Pokud je návrhem/podnětem dotčen více než jeden operační okruh, zopakuje se výše uvedený oddíl:

• Operační prostředky CELKEM (všechny operační okruhy)	Závazky	(4)								
	Platby	(5)								
Prostředky správní povahy financované z rámce na zvláštní programy (všechny operační okruhy) CELKEM		(6)								
Prostředky z OKRUHŮ 1 až 6 víceletého finančního rámce **CELKEM** (referenční částka)	Závazky	=4+6								
	Platby	=5+6								

Okruh víceletého finančního rámce	**7**	Správní výdaje

Tento oddíl se vyplní pomocí „rozpočtových údajů správní povahy“, jež se nejprve uvedou v příloze legislativního finančního výkazu (příloha V interních pravidel), která se pro účely konzultace mezi útvary vloží do aplikace DECIDE.

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
GŘ: CNECT						
• Lidské zdroje		1,030	1,030	1,030	1,030	**4,120**
• Ostatní správní výdaje		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
CELKEM GŘ CNECT	Prostředky	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

Prostředky na GŘ <…….> z OKRUHU 7 víceletého finančního rámce **CELKEM**	(Závazky celkem = platby celkem)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
Prostředky z OKRUHŮ 1 až 7 víceletého finančního rámce **CELKEM**	Závazky	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Platby	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Odhadovaný výstup financovaný z operačních prostředků

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy ⇩			Rok **N**		Rok **N+1**		Rok **N+2**		Rok **N+3**		Vložit počet let podle trvání finančního dopadu (viz bod 1.6)						**CELKEM**	
	VÝSTUPY																	
	Druh [44]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL č. 1[45]…																		
– Výstup																		
– Výstup																		
– Výstup																		
Mezisoučet za specifický cíl č. 1																		
SPECIFICKÝ CÍL č. 2 …																		
– Výstup																		
Mezisoučet za specifický cíl č. 2																		
CELKEM																		

[44] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

[45] Popsaný v bodě 1.4.2. „Specifické cíle…“.

3.2.3. Odhadovaný souhrnný dopad na správní prostředky

– ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

– ☑ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	
OKRUH 7 CELKEM					
Lidské zdroje	1,030	1,030	1,030	1,030	**4,120**
Ostatní správní výdaje	0,222	0,222	0,222	0,222	**0,888**
Mezisoučet za OKRUH 7 víceletého finančního rámce	1,252	1,252	1,252	1,252	**5,008**

Mimo OKRUH 7[46] víceletého finančního rámce					
Lidské zdroje					
Ostatní výdaje správní povahy					
Mezisoučet mimo OKRUH 7 víceletého finančního rámce					

CELKEM	1,252	1,252	1,252	1,252	**5,008**

Potřebné prostředky na oblast lidských zdrojů a na ostatní výdaje správní povahy budou pokryty z prostředků GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přerozděleny v rámci GŘ a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

[46] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

3.2.3.1. Odhadované potřeby v oblasti lidských zdrojů

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.

– ☑ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v přepočtu na plné pracovní úvazky

		Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**
20 01 02 01 (v ústředí a v zastoupeních Komise)		6	6	6	6
20 01 02 03 (při delegacích)					
01 01 01 01 (v nepřímém výzkumu)					
01 01 01 11 (v přímém výzkumu)					
Jiné rozpočtové položky (upřesněte)					
• Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE)[47]					
20 02 01 (SZ, VNO, ZAP z celkového rámce)		1	1	1	1
20 02 03 (SZ, MZ, VNO, ZAP a MOD při delegacích)					
XX 01 xx **yy zz** [48]	– v ústředí				
	– při delegacích				
01 01 01 02 (SZ, VNO, ZAP v nepřímém výzkumu)					
01 01 01 12 (SZ, VNO, ZAP v přímém výzkumu)					
Jiné rozpočtové položky (upřesněte)					
CELKEM		**7**	**7**	**7**	**7**

XX je oblast politiky nebo dotčená hlava rozpočtu.

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Úředníci a dočasní zaměstnanci 6 plných pracovních úvazků x 157 000 EUR/rok = 942 000 EUR	Jak je popsáno v bodě 2.2.1: – příprava žádosti o normalizaci a/nebo obecných specifikací prostřednictvím prováděcích aktů bez úspěšného procesu normalizace, – vypracování aktu v přenesené pravomoci [do 12 měsíců od vstupu tohoto nařízení v platnost], kterým se stanoví definice kritických produktů s digitálními prvky, – případná příprava aktů v přenesené pravomoci pro aktualizaci seznamu kritických produktů třídy I a II, upřesnění, zda je omezení nebo vyloučení nutné i pro produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie, která stanovují požadavky dosahující stejné úrovně ochrany jako toto nařízení, pověření certifikovat některé vysoce kritické produkty s digitálními prvky na základě kritérií stanovených v tomto nařízení, upřesnění minimálního obsahu EU prohlášení o shodě a doplnění prvků, které mají být obsaženy v technické dokumentaci, – případná příprava prováděcích aktů týkajících se formátu nebo prvků oznamovací povinnosti, softwarového kusovníku, obecných specifikací

[47] SZ = smluvní zaměstnanec; MZ = místní zaměstnanec; VNO = vyslaný národní odborník; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci.

[48] Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

	nebo umístění označení CE, – případně příprava okamžitého zásahu za účelem uložení nápravných nebo omezujících opatření za výjimečných okolností s cílem zachovat řádné fungování vnitřního trhu, včetně přípravy prováděcího aktu, – organizace a koordinace oznámení oznámených subjektů členskými státy a koordinace oznámených subjektů, – podpora koordinace orgánů dozoru nad trhem členských států.
Externí zaměstnanci 1 VNO x 88 000 EUR/rok	Jak je popsáno v bodě 2.2.1: – příprava žádosti o normalizaci a/nebo obecných specifikací prostřednictvím prováděcích aktů bez úspěšného procesu normalizace, – vypracování aktu v přenesené pravomoci [do 12 měsíců od vstupu tohoto nařízení v platnost], kterým se stanoví definice kritických produktů s digitálními prvky, – případná příprava aktů v přenesené pravomoci pro aktualizaci seznamu kritických produktů třídy I a II, upřesnění, zda je omezení nebo vyloučení nutné i pro produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie, která stanovují požadavky dosahující stejné úrovně ochrany jako toto nařízení, pověření certifikovat některé vysoce kritické produkty s digitálními prvky na základě kritérií stanovených v tomto nařízení, upřesnění minimálního obsahu EU prohlášení o shodě a doplnění prvků, které mají být obsaženy v technické dokumentaci, – případná příprava prováděcích aktů týkajících se formátu nebo prvků oznamovací povinnosti, softwarového kusovníku, obecných specifikací nebo umístění označení CE, – případně příprava okamžitého zásahu za účelem uložení nápravných nebo omezujících opatření za výjimečných okolností s cílem zachovat řádné fungování vnitřního trhu, včetně přípravy prováděcího aktu, – organizace a koordinace oznámení oznámených subjektů členskými státy a koordinace oznámených subjektů, – podpora koordinace orgánů dozoru nad trhem členských států.

3.2.4. Slučitelnost se stávajícím víceletým finančním rámcem

Návrh/podnět:

– x může být v plném rozsahu financován přerozdělením prostředků v rámci příslušného okruhu víceletého finančního rámce (VFR).

Není vyžadována žádná úprava.

– ☐ vyžaduje použití nepřiděleného rozpětí v rámci příslušného okruhu VFR a/nebo použití zvláštních nástrojů definovaných v nařízení o VFR.

–

– ☐ vyžaduje revizi VFR.

–

3.2.5. Příspěvky třetích stran

Návrh/podnět:

– x nepočítá se spolufinancováním od třetích stran.

– ☐ počítá se spolufinancováním od třetích stran podle následujícího odhadu:

prostředky v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **N**[49]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			Celkem
Upřesněte spolufinancující subjekt								
Spolufinancované prostředky CELKEM								

[49] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

3.3. Odhadovaný dopad na příjmy

– ☐ Návrh/podnět nemá žádný finanční dopad na příjmy.

– ☐ Návrh/podnět má tento finanční dopad:

  – ☐ na vlastní zdroje

  – ☐ na jiné příjmy

  – uveďte, zda je příjem účelově vázán na výdajové položky ☐

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová rozpočtová položka:	Prostředky dostupné v běžném rozpočtovém roce	Dopad návrhu/podnětu[50]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
Článek …….								

U účelově vázaných příjmů upřesněte dotčené výdajové rozpočtové položky.

Jiné poznámky (např. způsob/vzorec výpočtu dopadu na příjmy nebo jiné údaje).

[50] Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 20 % nákladů na výběr.