https://doi.org/10.5817/RPT2023-1-1

AKT O KYBERNETICKÉ ODOLNOSTI[1]

ZUZANA LIMBERGOVÁ[2]

ABSTRAKT

Článek se věnuje legislativnímu návrhu Evropské Komise na horizontální právní regulaci požadavků na kybernetickou bezpečnost produktů s digitálními prvky, označovanému jako „akt o kybernetické odolnosti“. Po nastínění hlavních principů navrhované regulace a jejích důvodů a cílů je pozornost věnována vztahu k existující unijní legislativě a oblasti působnosti. V další části je pak představeno věcné jádro návrhu, konkrétně vymezení základních pojmů a předmětu právní úpravy, dále požadavky stanovené pro uvádění a dodávání produktů s digitálními prvky na trh a představení principů posuzování shody. Další část je věnována představení hlavních povinností výrobců a ostatních hospodářských subjektů a základním pravidlům dozoru nad trhem a vymáhání. Poslední část se věnuje nastínění některých potenciálně problematických dopadů návrhu nové regulace jako podnětu k diskuzi.

KLÍČOVÁ SLOVA

Akt o kybernetické odolnosti; kybernetická bezpečnost; uvádění produktů na trh; produkty s digitálními prvky; posuzování shody; nový legislativní rámec

---

[1] Tento článek vznikl za podpory projektu "Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur" reg. č.: CZ.02.1.01/0.0/0.0/16_019/0000822 financovaného z EFRR.

[2] JUDr. Zuzana Limbergová, LL.M. je odbornou pracovnicí Ústavu práva a technologií Masarykovy univerzity a advokátkou v Praze, kontaktní e-mail: zuzana.limbergova@aklimbergova.cz.

ABSTRACT

The article focuses on the European Commission's legislative proposal for horizontal regulation of cybersecurity requirements for products with digital elements, referred to as the "Cyber Resilience Act". After outlining the main principles of the proposed regulation and its rationale and objectives, attention is given to its relationship with existing EU legislation and scope. The next section presents the substantive core of the proposal, namely the definition of the basic terms and the subject matter of the legislation, as well as the requirements set out for the making available and placing of products with digital elements on the market and the introduction of the principles of conformity assessment. The next part is devoted to an introduction to the main obligations of manufacturers and other economic operators and the basic rules on market surveillance and enforcement. The last part is devoted to outlining some potentially problematic impacts of the new regulation as the points for discussion.

KEY WORDS

Cyber Resilience Act; Cyber Security; Placing of Products on the Market; Products with Digital Elements; Conformity Assessment; NLF

1. ÚVOD

Legislativní orgány Evropské unie jsou v souladu se strategickými a programovými dokumenty[3] v poslední době velmi činné na poli regulace „digitální oblasti“, ať se jedná o správu a využívání dat, digitální trhy, digitální služby, umělou inteligenci nebo kybernetickou bezpečnost. V září roku 2022 byl Evropskou Komisí předložen legislativní návrh zkráceně ozna-

[3] Např. Společné sdělení Evropskému parlamentu a Radě Strategie kybernetické bezpečnosti EU pro digitální dekádu. JOIN (2020) 18 final. [online]. 2020. [cit. 1. 11. 2022] Dostupné z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. Projev předsedkyně Komise von der Leyenové o stavu Unie v roce 2021. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701. nebo Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Digitální kompas 2030: Evropské pojetí digitální dekády. COM (2021) 118 final, [online]. 2020. [cit. 1. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

čovaný jako akt o kybernetické odolnosti[4] plným názvem návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020[5]. Jak samotný název napovídá, nové nařízení cílí na regulatorní zajištění kybernetické bezpečnosti v produktové oblasti a mělo by se jednat o další dílek v evropské legislativní skládačce regulace kybernetické bezpečnosti. Akt o kybernetické odolnosti odpovídá zásadám právních předpisů nového legislativního rámce[6] v oblasti produktové bezpečnosti. Regulatorní přístup návrhu je postaven zejména na následujících principech:

- záměrná a standardní implementace požadavků kybernetické bezpečnosti od počátku a po celý životní cyklus produktu[7];
- zajištění kybernetické bezpečnosti v celém dodavatelském řetězci;
- přístup založený na riziku;
- horizontální (mezioborová) působnost.

Nová regulace má stanovit podmínky pro uvádění na trh všech produktů zahrnujících hardware nebo software a jeho řešení pro zpracování dat na dálku, včetně hardwarových a softwarových komponent uváděných na trh samostatně. Vztahovat se bude jak na software obsažený v hmotných produktech, tak na software nabízený zcela samostatně. Podmínkou je, že zamýšlené nebo důvodně předpokládané použití příslušného produktu zahrnuje přímé nebo nepřímé logické nebo fyzické datové připojení k zařízení nebo síti, což ovšem v dnešní době splní valná většina hardwarových i soft-

[4] V originále „Cyber Resilience Act“ uveřejněný dne 15. 9. 2022, viz European Comision. Shaping Europe’s digital future. Cyber Resilience Act. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act..

[5] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020, COM/2022/454 final. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52022PC0454&qid=1667332176493. Pro zjednodušení bude používán v tomto článku zkrácený název „akt o kybernetické odolnosti“ případně, tam kde je to s ohledem na kontext vhodné a není to na úkor jednoznačnosti významu, bude používáno také označení „návrh“ nebo „nařízení“.

[6] „New Legislative Framework (NLF)“. Podrobněji k vysvětlení NLF viz Sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 9-10. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC.

[7] „Security by default and by design“.

warových produktů. Jak bude dále uvedeno, jsou některé typy produktů nebo jejich modely distribuce z působnosti vyňaty, ne vždy jsou však tyto výjimky formulovány jednoznačně a dostatečně určitě. Osobní působnost je pak vymezena jak vůči výrobcům, tak i dalším článkům distribučního řetězce, jako jsou dovozci a distributoři.

Předmětem tohoto článku je legislativní návrh ve znění předloženém Komisí a uveřejněném dne 15. září 2022. V době psaní tohoto příspěvku byl legislativní proces v raném stadiu, v průběhu projednávání návrhu v Radě a Evropském parlamentu může dojít ještě k řadě změn. Cílem tohoto článku je představit čtenáři hlavní obsah aktu o kybernetické odolnosti a upozornit za účelem vyvolání další diskuze na některé potenciálně problematické souvislosti.

2. DŮVODY A CÍLE NÁVRHU

Hlavním deklarovaným důvodem návrhu nové právní úpravy je nutnost posílení kybernetické odolnosti hardwaru i softwaru proti kybernetickým útokům pro všechny produkty s digitálními prvky, na které se nevztahuje žádná speciální úprava. Posílení kybernetické odolnosti jednotlivých produktů by mělo vést s ohledem na vzájemnou propojenost informačních systémů, sítí a prostředí k posílení kybernetické odolnosti v rámci celého vnitřního trhu Unie. Zajištění vyšší kybernetické odolnosti má vést ke snížení případných majetkových škod a nemajetkové újmy způsobených úspěšnými kybernetickými útoky, nákladů vynakládaných v souvislosti s kybernetickými útoky a jejich prevencí včetně souvisejících nepřímých nákladů např. na pojištění. Zprostředkovaně pak má nová právní úprava přispět k lepší ochraně práv jednotlivců, která mohou být důsledky kybernetických útoků negativně dotčena.

Komise definuje dva hlavní problémy a jim odpovídající dva hlavní cíle, kterých má být přijetím nové právní úpravy dosaženo[8]:

[8] Blíže viz akt o kybernetické odolnosti. Důvodová zpráva. a Commission staff working document. Impact Assessment Report. Part 1/3. SWD (2022) 282 final. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

1. Prvním problémem je nízká úroveň kybernetické bezpečnosti produktů s digitálními prvky. Odpovídajícím cílem je tak vytvoření podmínek pro vývoj bezpečných produktů s digitálními prvky zajištěním toho, aby produkty byly uváděny na trh s méně zranitelnostmi a aby výrobci zohledňovali bezpečnost v průběhu celého životního cyklu produktu.
2. Druhým problémem je nízká informovanost a z toho vyplývající nedostatečné porozumění otázce kybernetické bezpečnosti produktů na straně uživatelů. Odpovídajícím cílem k řešení tohoto problému je vytvoření podmínek umožňujících uživatelům zohlednění kybernetické bezpečnosti při výběru a používání produktů s digitálními prvky.

V návaznosti na dva hlavní cíle sleduje akt o kybernetické odolnosti čtyři konkrétní cíle: (i) zajištění zlepšení bezpečnosti produktů s digitálními prvky na straně výrobců od fáze návrhu a vývoje a během celého životního cyklu, (ii) zajištění soudržného rámce kybernetické bezpečnosti na celém vnitřním trhu, který výrobcům usnadní dodržování předpisů, (iii) zvýšení transparentnosti bezpečnostních vlastností produktů s digitálními prvky a (iv) umožnění bezpečného používání produktů s digitálními prvky uživatelům z řad podniků i spotřebitelů.

Základem aktu o kybernetické odolnosti v primárním právu je vcelku nepřekvapivě článek 114 Smlouvy o fungování Evropské unie, tedy přijetí opatření nezbytných pro vytvoření a fungování vnitřního trhu, protože přijímání právních úprav této problematiky na úrovni členských států by vedlo k fragmentaci regulace a vytváření překážek fungování vnitřního trhu.

3. VZTAH K EXISTUJÍCÍ LEGISLATIVĚ A PŮSOBNOST

V případě přijetí bude akt o kybernetické odolnosti třetím unijním normativním aktem věnovaným specificky problematice kybernetické bezpečnosti. Prvním z těchto aktů byla v roce 2016 směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné

úrovně bezpečnosti sítí a informačních systémů v Unii[9], nahrazená v roce 2022 novou směrnicí zkráceně označovanou jako „směrnice NIS2“[10]. V roce 2019 následoval akt o kybernetické bezpečnosti[11].

Zatímco směrnice NIS (a stejně tak nová verze v podobě směrnice NIS2) vyžaduje transpozici vnitrostátním právním aktem a jejím hlavním cílem je zajistit kybernetickou bezpečnost vybraných sítí a služeb s významný společenským dopadem, akt o kybernetické odolnosti bude mít jako nařízení přímou a horizontální působnost, protože by se měl vztahovat na všechny produkty s digitálními prvky dodávané na vnitřním trhu EU bez ohledu na to, jak a kým jsou používány. Akt o kybernetické odolnosti by měl usnadnit dodržování požadavků na bezpečnost dodavatelského řetězce ze strany povinných subjektů podle NIS2 zajištěním bezpečnosti jimi používaných produktů po celou dobu jejich životního cyklu, tedy včetně zajištění bezpečnostních záplat a aktualizací.[12] Naopak akt o kybernetické odolnosti se nevztahuje na poskytování služeb včetně software formou služby (k tomuto tématu podrobněji v dalším textu), což by měla převážně pokrývat právě směrnice NIS2 prostřednictvím regulace poskytovatelů cloudových služeb. Zároveň by ale oba právní předpisy měly být vzájemně v souladu a navzájem se podporovat. Akt o kybernetické odolnosti přejímá ze směrnice NIS2 některé definice a předpokládá zapojení agentury ENISA a národních CSIRT týmů zřizovaných na základě směrnice NIS2 do plnění některých úkolů zejména v oblasti sdílení informací.

Akt o kybernetické bezpečnosti, který má rovněž formu nařízení, využívá obdobné nástroje jako akt o kybernetické odolnosti v podobě posouzení

[9] V souladu s obvyklým územ bude v článku pro tuto směrnici používáno zkrácené označení „směrnice NIS“.

[10] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 („směrnice NIS 2“).

[11] 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“).

[12] Viz recitál 11 aktu o kybernetické odolnosti.

shody, ať formou prohlášení o shodě nebo posuzování shody třetí stranou. Významným rozdílem je ale dobrovolnost užití certifikačních schémat přijatých na základě aktu o kybernetické bezpečnosti oproti povinnému posouzení kybernetické bezpečnosti a bezpečnostních rizik na základě aktu o kybernetické odolnosti. Certifikační schémata přijatá na základě aktu o kybernetické bezpečnosti mohou mít širší věcnou působnost, když se kromě produktové kybernetické bezpečnosti mohou vztahovat rovněž na služby a procesy[13]. Zároveň vymezení produktů podle aktu o kybernetické bezpečnosti nezahrnuje všechny produkty s digitálními prvky, jak je definuje akt o kybernetické odolnosti[14]. Subjekty určené k posuzování shody třetí osobou se v obou nařízeních částečně překrývají, stejně tak institucionální zaštítění tvorby příslušných norem posuzování shody. Z níže uvedeného shrnutí vyplývá, že obě nařízení vykazují v oblasti posuzování shody rovněž odlišnosti, nic to však nemění na tom, že se obě úpravy navzájem částečně duplikují.

Tabulka srovnání dílčích parametrů posuzování shody a certifikace.

	Akt o kybernetické bezpečnosti (CSA)	**Akt o kybernetické odolnosti (CRA)**
předmět posouzení/ certifikace	• produkt IKT = prvek nebo skupina prvků sítě nebo informačního systému • služba IKT = služba spočívající plně nebo převážně v přenosu, ukládání, získávání či zpracovávání informací prostřednictvím sítí a informačních systémů • proces IKT = soubor činností prováděných za účelem navrhování, vývoje, poskytování nebo údržby produktů nebo služeb IKT	produkt s digitálními prvky = softwarový nebo hardwarový produkt a jeho řešení pro zpracování dat na dálku, včetně softwarových nebo hardwarových součástí, které mají být uvedeny na trh samostatně

[13] Viz čl. 46 aktu o kybernetické bezpečnosti.

[14] Srov. čl. 3 bod 12 aktu o kybernetické bezpečnosti a čl. 3 bod 1 aktu o kybernetické odolnosti.

povinnost posouzení/ certifikace	certifikace pro uvedení na trh nepovinná, ledaže zvláštní předpis stanoví jinak	posouzení shody pro uvedení na trh povinné
výstup posouzení	evropský certifikát kybernetické bezpečnosti nebo EU prohlášení o shodě	prohlášení o shodě; certifikát EU přezkoušení typu nebo rozhodnutí o posouzení systému kvality při posouzení třetí osobou
norma pro posouzení shody/ certifikaci	evropský systém certifikace kybernetické bezpečnosti (certifikační schéma) - prováděcí akt Komise	příloha č. I CRA; harmonizované normy; obecné specifikace – prováděcí akt Komise
institucionální zajištění tvorby norem pro posouzení shody/ certifikaci	**ENISA** – navrhuje certifikační schéma; **Komise** – schvaluje certifikační schéma formou prováděcího aktu	evropské normalizační organizace na žádost Komise (harmonizované normy); Komise (obecné specifikace); Rada + EP – příloha č. I CRA
Institucionální zajištění posouzení shody třetí osobou	akreditovaný subjekt[15]; nebo vnitrostátní orgán certifikace kybernetické bezpečnosti; nebo akreditovaný veřejný subjekt	oznámený subjekt posuzování shody splňující požadavky CRA, primárně se předpokládá využití akreditovaných subjektů
možnost vlastního posouzení shody výrobcem	ano, pouze pro kategorii certifikace „základní“, a pokud to umožňuje certifikační schéma	ano, pokud nejde o kritický produkt třídy II, nebo třídy I, pro který nebyly použity/neexistují odpovídající normy

[15] Jedná se o akreditaci podle nařízení Evropského parlamentu a Rady (ES) 765/2008 kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

Dozor a vymáhání	vnitrostátní orgán certifikace kybernetické bezpečnosti	vnitrostátní orgán dozoru nad trhem – spolupracuje s orgánem certifikace kybernetické bezpečnosti podle CSA
sankce	výši a pravidla ukládání stanoví členský stát	konkrétní výši a pravidla ukládání stanoví členský stát, maximální limity určuje CRA
vzájemná nahraditelnost posouzení/ certifikace	ne (certifikaci nelze nahradit posouzením podle CRA)	ano, pokud tak stanoví Komise aktem v přenesené pravomoci; povinně pro vysoce kritické produkty, pokud tak stanoví Komise

Mezi oběma nařízeními budou existovat styčné plochy a interakce, nařízení by proto měla být vzájemně kompatibilní. Akt o kybernetické odolnosti má svěřit Komisi pravomoc prostřednictvím přijetí aktu v přenesené pravomoci upřesnit kategorie vysoce kritických produktů s digitálními prvky, pro které budou výrobci povinni získat evropský certifikát kybernetické bezpečnosti v rámci evropského systému certifikace, aby prokázali shodu se základními požadavky stanovenými aktem o kybernetické odolnosti[16]. Protože vymezení těchto vysoce kritických produktů je ponecháno na prováděcích předpisech a uvážení Komise, znamená to pro výrobce značnou nejistotu, jakým procesem posuzování shody budou muset vyvíjené produkty projít, kterou ještě posiluje skutečnost, že certifikační schémata podle aktu o kybernetické bezpečnosti stále nebyla schválena.

Komisi je rovněž svěřena pravomoc prostřednictvím prováděcích aktů specifikovat evropské systémy certifikace kybernetické bezpečnosti, které lze použít k prokázání shody se základními požadavky podle aktu o kybernetické odolnosti, a dále případně určit, zda certifikát kybernetické bezpečnosti vydaný v rámci těchto systémů ruší povinnost výrobce nechat

[16] Viz čl. 6 odst. 5 aktu o kybernetické odolnosti.

provést posouzení shody třetí stranou [17]. Zároveň by potřeba nových evropských systémů certifikace kybernetické bezpečnosti pro produkty s digitálními prvky měla být posuzována s ohledem na existenci a obsah aktu o kybernetické odolnosti, zohledňovat základní požadavky v něm stanovené a usnadňovat s ním soulad.[18]Tato ustanovení přímo vyvolávají otázku, z jakého důvodu není přímo aktem o kybernetické odolnosti bez dalšího umožněno nahrazení posouzení shody certifikací podle aktu o kybernetické bezpečnosti a jaký má vůbec paralelní udržování dvou systémů posuzování shody, navíc prováděného často stejnými subjekty, smysl. Na nejasnost vztahu mezi certifikačními orgány ve smyslu aktu o kybernetické odolnosti a orgány oprávněnými k certifikaci kybernetické bezpečnosti podle jiných použitelných předpisů ostatně upozornil ve svém stanovisku i Evropský hospodářský a sociální výbor[19].

Akt o kybernetické odolnosti by měl mít povahu horizontální úpravy vztahující se na všechny produkty s digitálními prvky, jejichž zamýšlené nebo důvodně předpokládané použití zahrnuje přímé nebo nepřímé logické nebo fyzické datové připojení k zařízení nebo síti. S ohledem na existenci speciálních unijních právních předpisů pro některé kategorie produktů návrh stanoví výčtem těchto speciálních předpisů konkrétní výjimky z obecné působnosti aktu o kybernetické odolnosti[20], a dále obecné podmínky, za kterých může být použití aktu o kybernetické odolnosti na produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie, omezeno nebo vyloučeno.[21] Generální výjimka z působnosti by pak měla platit pro produkty s digitálními prvky vyvinuté výlučně pro účely národní bezpečnosti nebo

[17] Viz čl. 18 odst. 4 aktu o kybernetické odolnosti.

[18] Viz recitál 39 aktu o kybernetické odolnosti.

[19] Viz Stanovisko Evropského hospodářského a sociálního výboru k návrhu nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020 (COM(2022) 454 final – 2022/0272 (COD). (2023/C 100/15). [online]. 2022. [cit. 16. 3. 2023] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:52022AE4103.

[20] Viz čl. 2 odst. 2, 3 aktu o kybernetické odolnosti. Jedná se např. o diagnostické a zdravotnické prostředky nebo motorová vozidla.

[21] Viz čl. 2 odst. 4 aktu o kybernetické odolnosti.

pro vojenské účely a produkty speciálně určené ke zpracování utajovaných informací.

Navrhované nařízení má řešit pouze požadavky na kybernetickou bezpečnost produktů s digitálními prvky, nikoli požadavky na jejich bezpečnost všeobecně. Na ty se budou vztahovat buď speciální unijní předpisy, nebo nařízení o obecné bezpečnosti výrobků, jehož návrh je také v legislativním procesu[22].

Speciální pravidla jsou stanovena pro strojní výrobky a produkty s digitálními prvky, které jsou zároveň vysoce rizikovými systémy umělé inteligence, kdy by v zásadě splnění požadavků podle aktu o kybernetické odolnosti mělo dokládat zároveň soulad s požadavky na kybernetickou bezpečnost stanovenými ve speciálních úpravách[23].

4. PŘEDMĚT PRÁVNÍ ÚPRAVY A ZÁKLADNÍ POJMY

Předmětem aktu o kybernetické odolnosti bude:

1) stanovení pravidel pro uvádění produktů s digitálními prvky na trh;
2) stanovení základních požadavků na navrhování, vývoj a výrobu produktů s digitálními prvky a povinností hospodářských subjektů v souvislosti s těmito produkty;
3) stanovení základních požadavků na procesy řešení zranitelnosti zavedené výrobci a povinností hospodářských subjektů v souvislosti s těmito procesy;

to vše s cílem zajistit kybernetickou bezpečnost produktů s digitálními prvky během celého jejich životního cyklu, a dále

4) stanovení pravidel pro dozor nad trhem a prosazování stanovených pravidel a požadavků.

Ústředním pojmem, ke kterému se vztahují všechny povinnosti a pravidla stanovená aktem o kybernetické odolnosti, je *produkt s digitálními*

[22] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o obecné bezpečnosti výrobků, o změně nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 a o zrušení směrnice Rady 87/357/EHS a směrnice Evropského parlamentu a Rady 2001/95/ES. COM/2021/346 final. [online]. 2022. [cit. 6. 11. 2022] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A52021PC0346.

[23] Podrobněji viz čl. 8 a čl. 9 aktu o kybernetické odolnosti.

prvky. Návrh tento pojem definuje jako *„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“*[24]. Definice zahrnuje jak komplexní produkty s digitálními prvky složené z hardwarových i softwarových komponentů, tak hardware nebo software[25] uváděné na trh samostatně, podmínkou ovšem je, aby se jednalo o produkty, jejichž zamýšlené nebo předpokládané použití zahrnuje přímé či nepřímé logické nebo fyzické datové připojení k zařízení nebo síti. Produkty s digitálními prvky, které jsou výhradně off-line, do působnosti navrhovaného nařízení nespadají. Využití produktu koncovým uživatelem je nerozhodné, nezáleží na tom, zda se jedná o software pro řízení průmyslové výroby, server používaný neziskovou organizací nebo chytré hodinky určené pro spotřebitele.

Návrh obsahuje speciální vymezení vůči obchodnímu modelu poskytování software formou služby (SaaS). Recitál 9 stanoví, že *„Toto nařízení zajišťuje vysokou úroveň kybernetické bezpečnosti produktů s digitálními prvky. Neupravuje služby, například Software jako služba (SaaS)…“*[26], což je logické, protože nařízení spadá stejně jako ostatní předpisy NLF do oblasti produktové bezpečnosti, nedává smysl vztahovat je na služby. Text recitálu ale pokračuje: „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“*[27], což výklad působnosti nařízení komplikuje. Z textace není zcela zřejmé, zda se v případě zpracování dat na dálku, které je nutné pro plné fungování produktu s digitálními prvky a které je vyvíjeno týmž výrobcem nebo pod jeho odpovědností, má akt o kybernetické odolnosti vztahovat na celé toto řešení, i pokud je poskytováno formou služby, nebo zda tímto způsobem je pouze zdůrazněno,

[24] Viz čl. 3 bod 1) aktu o kybernetické odolnosti.

[25] Oba tyto dílčí pojmy aktu o kybernetické odolnosti rovněž samostatně definuje, viz čl. 3 body 6) a 7).

[26] Viz recitál 9 aktu o kybernetické odolnosti.

[27] Viz recitál 9 aktu o kybernetické odolnosti.

že *software* výrobce využívaný pro zpracování dat na dálku, byť by byl nabízen formou poskytování služby, nemá být z působnosti nařízení vyňat. Zpracováním dat na dálku je „*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*“, definice je natolik široká, že spíše zahrnuje i zpracování dat formou služby, je-li k ní využíván software vyvíjený výrobcem či pod jeho odpovědností než pouze tento software. V případech, kdy produkt využívá SaaS třetí strany, za který nenese výrobce odpovědnost, se však působnost nařízení na tuto službu vztahovat nebude.

Účelem nařízení je zajistit, aby na společný trh byly dodávány pouze produkty s digitálními prvky splňující stanovené bezpečnostní požadavky, což by ale nemělo bránit technologickému vývoji a výzkumu. Proto je umožněno uvolnění testovacích nebo předváděcích verzí produktů s digitálními prvky bez toho, aby splňovaly stanovené požadavky, pouze však v omezeném režimu[28]. Z obdobných důvodů se nemá nařízení vztahovat na software s otevřeným zdrojovým kódem (tzv. open source software)[29], je-li nabízen bezplatně a mimo rámec obchodní činnosti, tedy i bez poskytování podpůrných nebo souvisejících služeb (typicky služby typu maintenance) na komerční bázi. Za obchodní činnost je navíc obdobně jako ve směrnici o poskytování digitálního obsahu[30] označováno i použití osobních údajů z jiných důvodů než výlučně zlepšení bezpečnosti, kompatibility nebo interoperability software. Vynětí open source softwaru je však uvedeno pouze v recitálu návrhu, nikoli již dále v normativním textu. Zároveň mohou vznikat nejasnosti, co ještě lze považovat za dodávání *mimo rámec obchodní činnosti*, když uvedení na trh zahrnuje i bezplatné dodání[31].

Akt o kybernetické odolnosti produkty s digitálními prvky dále kategorizuje a vyčleňuje dvě skupiny produktů, které podléhají speciálnímu zpřísněnému režimu. Jedná se o *kritické produkty s digitálními prvky a vysoce*

[28] Blíže viz čl. 4 odst. 2 a 3 a recitál 21 aktu o kybernetické odolnosti.

[29] Viz recitál 10 aktu o kybernetické odolnosti.

[30] Směrnice Evropského parlamentu a Rady (EU) 2019/770 ze dne 20. května 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb.

[31] Viz čl. 3 body 22) a 23 aktu o kybernetické odolnosti.

kritické produkty s digitálními prvky. Tyto dvě kategorie mají stanovena přísnější kritéria pro dodávání na trh než ostatní produkty s digitálními prvky.

Kritické produkty s digitálními prvky jsou produkty s digitálními prvky, které představují kybernetické bezpečnostní riziko v souladu se stanovenými kritérii a jejichž základní funkce odpovídá funkcím uvedeným v příloze III aktu o kybernetické odolnosti. Tato kategorie je pak dále dělena do dvou tříd podle výčtu uvedeného v příloze III. Do I. třídy náleží např. samostatné i vestavěné prohlížeče, správci hesel, systémy řízení sítě nebo software pro správu mobilních zařízení, do II. – kritičtější – třídy náleží např. operační systémy pro servery, stolní počítače a mobilní zařízení, čipové karty, čtečky čipových karet a tokeny nebo mikroprocesory[32]. Seznam uvedený v příloze III může být měněn aktem Komise přijatým v přenesené pravomoci, čímž by mělo být zajištěno, že legislativní úprava bude dostatečně flexibilně reagovat na technologický vývoj. Komisi je také svěřena pravomoc přijetím aktu v přenesené pravomoci upřesnit definice kategorií kritických produktů.

Vysoce kritické produkty s digitálními prvky jsou produkty s digitálními prvky, které představující kybernetické riziko s ohledem na speciální kritéria, kterými jsou (i) používání nebo spoléhání se základními subjekty podle přílohy I směrnice NIS2 na takový produkt nebo (ii) relevance pro odolnost celého dodavatelského řetězce produktů s digitálními prvky vůči událostem způsobujícím narušení. Vysoce kritické produkty s digitálními prvky akt o kybernetické odolnosti neurčuje, ale svěřuje tuto pravomoc Komisi[33]. Důsledkem rozdělení produktů s digitálními prvky na vysoce kritické, kritické a „nekritické“ je různá míra náročnosti procesu posuzování shody, kterému podléhají, s ohledem na možná rizika spojená s jejich použitím.

[32] Pro kompletní výčet viz Příloha III aktu o kybernetické odolnosti.

[33] Viz čl. 6 odst. 5 Aktu o kybernetické odolnosti.

5. UVÁDĚNÍ A DODÁVÁNÍ PRODUKTŮ S DIGITÁLNÍMI PRVKY NA TRH

Obdobně jako u ostatních právních předpisů nového legislativního rámce je i v aktu o kybernetické odolnosti důležitým pojmem uvedení produktu s digitálními prvky na trh. Uvedením produktu s digitálními prvky na trh se rozumí „*první dodání produktu s digitálními prvky na trh Unie*“[34]. Dodáním na trh je pak „*jakékoli dodání produktu s digitálními prvky k distribuci nebo použití na trhu Unie v rámci obchodní činnosti, ať už za úplatu, nebo bezplatně*“[35]. Přitom pojmy *dodání* i *uvedení* se vztahují na každý jednotlivý produkt, nikoli na typ produktu, ať už byl vyroben nebo vyvinut individuálně nebo sériově[36]. To mj. znamená, že pravidla aktu o kybernetické odolnosti se budou vztahovat i na produkty s digitálními prvky (jako individuální jednotky), jejichž typ nebo model byl na unijní trh dodáván již přede dnem použitelnosti aktu o kybernetické odolnosti, pokud tyto jednotlivé produkty jako samostatné jednotky byly dodány až poté. K tomu je třeba doplnit, že na základě přechodných ustanovení se povinnosti výrobců informovat o zranitelnostech nebo incidentech podle čl. 11 mají vztahovat i na produkty s digitálními prvky uvedené na trh Unie přede dnem použitelnosti aktu o kybernetické odolnosti.

Dodání i uvedení produktu s digitálními prvky předpokládá nabídku nebo dohodu (písemnou či ústní) mezi dvěma či více právnickými nebo fyzickými osobami za účelem převodu vlastnictví, držby či jakéhokoli jiného práva týkajícího se dotčeného produktu. Může se přitom jednat nejen o převod vlastnického práva, ale např. i výpůjčku, nájem nebo leasing[37].

Povinnosti hospodářských subjektů návrh vztahuje k uvedení produktů s digitálními prvky na trh, nikoli k jejich prostému vyrobení, vývoji

[34] Čl. 3 odst. 22 aktu o kybernetické odolnosti.

[35] Čl. 3 odst. 23 aktu o kybernetické odolnosti.

[36] Viz sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 19-20. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC

[37] Viz sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 19-20. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC

nebo užívání. Na produkty s digitálními prvky, které nejsou výrobcem uváděny na trh, typicky na výsledky interního vývoje software, který je užíván výhradně subjektem, který jej vyvinul pro své vlastní účely, by se povinnosti hospodářských subjektů podle aktu o kybernetické odolnosti vztahoval neměly[38], na rozdíl však od produktů vyrobených výrobcem pro zákazníka na zakázku, u kterých k uvedení a dodání na trh dochází.

Produkty s digitálními prvky bude podle aktu o kybernetické odolnosti možné dodávat na trh pouze v případě, že

- splňují základní požadavky stanovené v oddíle 1 přílohy I aktu o kybernetické odolnosti za podmínky, že jsou řádně instalovány, udržovány a používány k určenému účelu či za podmínek, které lze rozumně předvídat a, je-li to relevantní, aktualizovány a
- výrobcem zavedené postupy jsou v souladu se základními požadavky stanovenými v oddíle 2 přílohy I aktu o kybernetické odolnosti[39].

Oddíl 1 přílohy I aktu o kybernetické odolnosti obsahuje seznam bezpečnostních požadavků týkající se vlastností produktů s digitálními prvky na základě posouzení rizik těchto produktů provedeného výrobcem.

Oddíl 2 přílohy I aktu o kybernetické odolnosti stanoví požadavky na řešení zranitelností, které musí výrobci zavést do svých postupů nejen při designu a výrobě produktu, ale také v poprodejní fázi, kdy jsou zejména povinni sdílet informace o možných zranitelnostech a zajišťovat bezpečnostní opravy nebo aktualizace včetně jejich bezplatného šíření po očekávanou dobu životnosti produktu nebo po dobu pěti let od jeho uvedení na trh (podle toho, která doba je kratší). Zranitelnost je definována shodně jako ve směrnici NIS2, tedy jako slabá stránka, snížená odolnost nebo chyba prostředku, systému, procesu nebo kontroly, která může být využita kybernetickou hrozbou[40].

[38] Viz vysvětlení obsažené ve sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 19-20. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC

[39] Čl. 5 aktu o kybernetické odolnosti.

Soulad produktu s digitálními prvky s požadavky stanovenými v oddíle 1 přílohy I aktu o kybernetické odolnosti a soulad výrobcem zavedených postupů se základními požadavky stanovenými v oddíle 2 přílohy I aktu o kybernetické odolnosti se dokládá prohlášením o shodě a umístěním CE označení[41]. Prohlášení o shodě lze vydat až po provedení posouzení shody v souladu s čl. 24 aktu o kybernetické odolnosti. Výrobce má na výběr ze tří variant postupů posuzování shody s využitím čtyř různých modulů[42]:

1. postup vnitřní kontroly (na základě modulu A)[43], tedy zjednodušeně vlastní posouzení shody výrobcem;
2. EU přezkoušení typu (na základě modulu B), po kterém musí následovat shoda s EU typem založená na interním řízení výroby (na základě modulu C)[44]; tzn. nechat provést posouzení shody typu produktu třetí oprávněnou osobou a zavést kontrolní mechanismy zaručující řízení výroby tak, aby byla zajištěna shoda s typem, který byl předmětem posouzení; nebo
3. posuzování shody založené na komplexním zabezpečení kvality (na základě modulu H)[45]; tj. přezkoumání a posouzení komplexního systému zabezpečení kvality třetí oprávněnou osobou.

---

[40] Čl. 3 bod 38) aktu o kybernetické odolnosti ve spojení s čl. 4 bod 8 návrhu SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148. COM/2020/823 final. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52020PC0823.

[41] Podrobněji viz čl. 10 odst. 7 a čl. 21 aktu o kybernetické odolnosti, a dále čl. 30 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

[42] Jedná se o moduly ve smyslu přílohy II 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.

[43] Blíže viz příloha VI aktu kybernetické odolnosti ve spojení s přílohou II Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES..

[44] Blíže viz příloha VI aktu kybernetické odolnosti ve spojení s přílohou II Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES.

[45] Blíže viz příloha VI aktu kybernetické odolnosti ve spojení s přílohou II Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES.

Jedná-li se o kritický produkt s digitálními prvky třídy II, musí být shoda se základními požadavky prokázána jedním z postupů uvedených shora pod body 2 nebo 3, vždy tedy s provedením posouzení shody třetí stanou, ledaže Komise určila, že povinnost posouzení třetí stranou lze nahradit certifikátem kybernetické bezpečnosti vydaným v rámci systému certifikace kybernetické bezpečnosti.

Pro kritický produkt s digitálními prvky třídy I je požadováno prokázání shody se základními požadavky rovněž jedním z postupů uvedených shora sub 2 nebo 3, pouze však v případě, kdy výrobce pro posouzení souladu nepoužil harmonizované normy[46], obecné specifikace[47] nebo evropský systém certifikace kybernetické bezpečnosti[48] určený Komisí[49] nebo jestliže použitelné harmonizované normy, obecné specifikace nebo evropský systém certifikace kybernetické bezpečnosti neexistují.

V případě „nekritických" produktů s digitálními prvky je možné využít bez dalších omezení i posouzení shody uvedené výše sub 1, které provádí výrobcem sám bez zapojení třetí osoby. Zároveň jsou-li „nekritické" produkty s digitálními prvky a postupy výrobce ve shodě s harmonizovanými normami nebo obecnými specifikacemi, nebo bylo-li pro ně vydáno prohlášení o shodě nebo certifikát podle evropského systému certifikace kybernetické bezpečnosti určeného Komisí, má se za to, že jsou tyto produkty ve shodě i se základními požadavky uvedenými v příloze I aktu o kybernetické odolnosti.

Pro kategorii vysoce kritických produktů s digitálními prvky, pokud je Komise stanoví, budou výrobci povinni k prokázání shody získat evropský certifikát kybernetické bezpečnosti podle certifikačního schématu na základě aktu o kybernetické bezpečnosti.

---

[46] Harmonizované normy, na něž byl zveřejněn odkaz v Úředním věstníku EU, ve smyslu čl. 2 odst. 1) psím. c) Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci.

[47] Obecné specifikace ve formě prováděcích aktů je při naplnění podmínek stanovených čl. 19 aktu o kybernetické odolnosti oprávněna vydávat Komise.

[48] Evropský systém certifikace kybernetické bezpečnosti podle aktu o kybernetické bezpečnosti.

[49] Viz čl. 18 odst. 4 aktu o kybernetické odolnosti.

Je-li v rámci posuzování shody požadováno zapojení třetí osoby, bude se jednat o subjekty posuzování shody. Subjekt posuzování shody musí splňovat podmínky stanovené aktem o kybernetické odolnosti, zejména týkající se odbornosti, nezávislosti a nestrannosti, a musí být oznámen Komisi a ostatním členským státům příslušným oznamujícím orgánem členského státu.[50] Subjekty posuzování shody zároveň mohou splnění způsobilosti prokázat osvědčením o akreditaci vydaným na základě nařízení (ES) č. 765/2008[51].

Pokud je produkt s digitálními prvky v souladu s aktem o kybernetické odolnosti, nesmí členské státy bránit jeho dodávání na trh, pouze však pro hlediska, na něž se akt o kybernetické odolnosti vztahuje. Pro jiná hlediska mohou členské státy dodávání konkrétního produktu s digitálními prvky bránit, pouze však v případě, že se tím nedostanou do rozporu s jinou unijní legislativou či judikaturou[52].

6. HLAVNÍ POVINNOSTI HOSPODÁŘSKÝCH SUBJEKTŮ

Akt o kybernetické odolnosti by měl ukládat povinnosti širokému spektru hospodářských subjektů od výrobců a jejich zmocněných zástupců přes dovozce a distributory až po jakékoli osoby, které provedou podstatnou změnu produktu s digitálními prvky.

Největší porce povinností by se měla vztahovat na výrobce, kterým se rozumí „*jakákoli 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*“[53]. Pokud však dovozce nebo distributor uvede na trh produkt s digitálními prvky pod svým jménem nebo

[50] Podrobněji viz čl. 29 a násl. aktu o kybernetické odolnosti.

[51] Nařízení Evropského parlamentu a Rady (ES) 765/2008 kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

[52] Srov. zejména rozhodnutí Soudního dvora ve věci 120/78 „Cassis de Dijon“ a nařízení (EU) 2019/515 o vzájemném uznávání zboží uvedeného v souladu s právními předpisy na trh v jiném členském státě.

[53] Čl. 3 odst. 18 aktu o kybernetické odolnosti.

ochrannou známkou, vztahují se na něj povinnosti výrobce a je považován pro účely aktu o kybernetické odolnosti za výrobce. Stejný důsledek má i provedení podstatné změny produktu s digitálními prvky již uvedeného na trh dovozcem či distributorem. Podobné důsledky nastávají i pro jakoukoli třetí osobu, která provede podstatnou změnu produktu s digitálními prvky. Taková osoba se považuje za výrobce a vztahují se na ní relevantní povinnosti, pokud jde o část produktu, která je podstatnou změnou ovlivněna, případně dokonce ve vztahu k celému produktu, jestliže byla podstatnou změnou ovlivněna kybernetická bezpečnost produktu s digitálními prvky jako celku[54]. Podstatnou změnou produktu se přitom rozumí „*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*“[55].

Případná změna produktu s digitálními prvky má významný dopad i pokud je provedena přímo výrobcem po uvedení produktu na trh. Výrobce by měl nejprve vyhodnotit, zda taková změna naplňuje definici podstatné změny a v případě kladného výsledku provést ověření shody s požadavky nařízení, případně nové posouzení shody. 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*“[56], měl by být software považován za podstatně změněný. V případě software je provádění změn ve formě aktualizací časté a obvyklé, řada aktualizací směřuje ke zvýšení výkonu, optimalizaci chodu, rozšíření funkcionalit nebo ke zvýšení bezpečnosti produktu. Jestliže každá aktualizace bude na straně výrobců vyvolávat nutnost interního posouzení, zda je podstatnou změnou a případně nutnost nového posouzení shody, může to vést paradoxně ke zhoršení bezpečnosti software nebo nežádoucímu zpomalení jeho vývoje[57].

[54] Čl. 15 a čl. 16 aktu o kybernetické odolnosti.

[55] Čl. 3 bod 31 aktu o kybernetické odolnosti.

[56] Recitál 22 aktu o kybernetické odolnosti.

Kromě již zmíněné povinnosti provést odpovídající postupy posuzování shody jsou výrobci zejména povinni při uvádění produktu s digitálními prvky na trh zajistit návrh, vývoj a výrobu produktu v souladu se základními požadavky stanovenými v oddíle 1 přílohy I včetně provedení posouzení kybernetických bezpečnostní rizik spojených s produktem. Toto posouzení musí být součástí povinně pořizované technické dokumentace produktu s digitálními prvky, jejíž náležitosti stanoví příloha V návrhu. Technickou dokumentaci musí výrobce průběžně aktualizovat po dobu očekávané životnosti produktu nebo po dobu pěti let od uvedení produktu na trh, podle toho, která doba je kratší, a uchovat jí pro potřeby dozorových orgánů po dobu deseti let od uvedení produktu s digitálními prvky na trh. Pro sériově vyráběné produkty (což bude většina) musí výrobci zajistit, že zůstanou ve shodě po celou dobu výroby.

Důležitou skupinu povinností lze zkráceně označit jako due diligence ve vztahu k dodavatelům. Výrobci musí při začleňování součástí od třetích stran do svého produktu s digitálními prvky postupovat s náležitou péčí a zajistit, aby tyto součásti neohrožovaly bezpečnost produktu. Součástí této povinnosti je i pořízení softwarového kusovníku, což je „*formální záznam obsahující podrobnosti o dodavatelském řetězci a vztazích v něm u součástí začleněných do softwarových prvků produktu s digitálními prvky*“[58]. I po uvedení produktu s digitálními prvky na trh musí výrobce systematicky dokumentovat relevantní aspekty kybernetické bezpečnosti vztahující se k produktu, a zejména zajistit odhalování a řešení zranitelností.

Další skupinu tvoří informační povinnosti výrobce vůči uživatelům. Výrobce je jednak povinen k produktu s digitálními prvky umístit označení CE[59], vydat a k produktu přiložit prohlášení o shodě. Tím však jeho informační povinnost nekončí. Výrobce je povinen zajistit, aby k produktům

[57] Srov např. Digitaleurope. Cybersecurity everywhere: deciphering the Cyber Resilience Act. [online]. 23. 1. 2023. [cit. 16. 4. 2023]. Dostupné z: https://www.digitaleurope.org/policies/cybersecurity/ nebo BSA Recommendations on the EU Cyber Resilience Act. [online]. 2022. [cit. 30. 11. 2022]. Dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Akt-o-kyberneticke-odolnosti-nova-pravidla-kyberneticke-bezpecnosti-pro-digitalni-produkty-a-podpurne-sluzby_cs.

[58] Čl. 3 bod 37 aktu o kybernetické odolnosti.

byly elektronicky nebo ve fyzické podobě připojeny informace a pokyny, které musí být jasné, srozumitelné, snadno pochopitelné, čitelné a v jazyce snadno srozumitelném uživatelům a jejichž minimální náležitosti stanoví příloha II nařízení. Výrobce je rovněž povinen informovat uživatele o incidentech a souvisejících nápravných opatřeních nebo o ukončení své činnosti.

Poslední skupinou povinností výrobců jsou povinnosti týkající se spolupráce s orgány dozoru. Výrobci jsou povinni poskytnout kterémukoli orgánu dozoru nad trhem na jeho žádost všechny informace nezbytné k prokázání shody produktu s digitálními prvky a výrobcem zavedených postupů se základními požadavky podle přílohy I, a dále s orgánem dozoru spolupracovat na odstranění kybernetických bezpečnostních rizik produktů s digitálními prvky, které uvedli na trh. Pokud výrobce ukončí činnost a není tak schopen plnit své povinnosti, je o tom rovněž povinen předem informovat orgány dozoru nad trhem.

Z hlediska ochrany před kybernetickým nebezpečím je obzvlášť důležitá povinnost výrobce informovat agenturu ENISA o každé aktivně zneužívané zranitelnosti produktu s digitálními prvky a o jakémkoli incidentu s dopadem na bezpečnost produktu, a to bez zbytečného odkladu nejpozději však do 24 hodin poté, co se o těchto skutečnostech dozví.

Povinnosti dovozců a distributorů se pak vztahují zejména k zajištění nebo ověření splnění povinností výrobce, informačních povinností a spolupráce s orgány dozoru nad trhem[60].

7. DOZOR A VYMÁHÁNÍ

Pro dozor nad trhem a kontrolu se použije nařízení Evropského parlamentu a Rady (EU) 2019/1020[61]. Každý členský stát je povinen určit jeden nebo

[59] Podrobnosti ke způsobu připojení CE označení stanoví čl. 22 aktu o kybernetické odolnosti, který zohledňuje i specifika jednotlivých typů produktů s digitálními prvky, kdy v případě softwaru postačuje např. uvedení označení na internetových stránkách.

[60] K povinnostem dovozců a distributorů podrobněji viz čl. 13 a čl. 14 aktu o kybernetické odolnosti.

[61] 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 204/42/ES a nařízení (ES) č. 765/2008 a (EU) č. 305/2011.

více orgánů dozoru nad trhem pro účely zajištění provádění aktu o kybernetické odolnosti. Může se jednat o orgány nové nebo stávající. Orgány dozoru nad trhem mají povinnost vzájemné spolupráce za účelem jednotného uplatňování nařízení včetně vytvoření specializované skupiny pro správní spolupráci[62] nebo organizování společných kontrolních akcí (tzv. „sweepy")[63]. V případě vzniku podezření, že produkt s digitálními prvky včetně řešení jeho zranitelností představuje významné bezpečnostní riziko, je orgán dozoru povinen provést jeho hodnocení z hlediska souladu se všemi požadavky stanovenými aktem o kybernetické odolnosti. Důsledkem zjištěného nesouladu může být uložení povinnosti přijmout vhodná opatření příslušnému hospodářskému subjektu, v krajním případě až zákaz dodávání produktu na trh příslušného státu nebo povinnost jeho stažení z trhu či oběhu. V případě odůvodněných opatření jsou ostatní členské státy povinny přijmout nezbytná opatření k zajištění stažení nevyhovujícího produktu s digitálními prvky i z jejich trhů.

Zajímavým nástrojem je možnost vyžadovat přijetí dalších dodatečných opatření u produktů s digitálními prvky, které jsou v souladu s aktem o kybernetické odolnosti, přesto však představují významné kybernetické bezpečnostní riziko, a navíc 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 základními subjekty podle směrnice NIS2 nebo pro jiné aspekty ochrany veřejného zájmu. Takto může postupovat dozorový orgán členského státu na základě vlastního provedeného hodnocení nebo z podnětu Komise. Komise má také rozhodující slovo při posouzení důvodnosti přijatých opatření[64].

Stanovení pravidel ukládání a prosazování sankcí za porušení nařízení má být svěřeno členským státům. Sankce musí být přiměřené, účinné a odrazující, návrh nařízení stanoví pouze horní hranici správních pokut a zá-

[62] Čl. 41 odst. 11 aktu o kybernetické odolnosti.

[63] Čl. 49 aktu o kybernetické odolnosti.

[64] Podrobněji viz čl. 46 aktu o kybernetické odolnosti.

kladní pravidla jejich vyměřování stanovením okolností, které musí brát orgán dohledu v úvahu[65].

V návrhu jsou určité činnosti svěřeny rovněž agentuře ENISA, a to zejména v oblasti koordinace a předávání informací o zranitelnostech CSIRT týmům členských států a Evropské síti styčných organizací pro řešení kybernetických krizí (EU-CyCLONe), zpracování zpráv o nových trendech v oblasti kybernetických bezpečnostních rizik produktů s digitálními prvky a spolupráce s Komisí v případě produktů s digitálními prvky představujících významné kybernetické bezpečnostní riziko.

8. POTENCIÁLNĚ PROBLEMATICKÉ SOUVISLOSTI

Tato část článku je věnována některým potenciálně problematickým důsledkům přijetí navrhované úpravy. Nečiní si nárok na úplnost, zajisté lze najít i další problematické konsekvence, ani na nevyvratitelnou správnost. Účelem je spíše podnítit čtenáře k dalšímu přemýšlení nad návrhem a vyvolat diskuzi.

Posuzování shody produktů s digitálními prvky je podle aktu o kybernetické odolnosti vztaženo objektově, tedy k produktu s digitálními prvky. Bezpečnostní požadavky uvedené v oddíle 1 přílohy I aktu o kybernetické odolnosti se týkají vlastností samotného produktu s digitálními prvky. Požadavky na řešení zranitelností v oddíle 2 přílohy I aktu o kybernetické odolnosti se vztahují k procesu řešení zranitelností, ale pouze příslušného produktu s digitálními prvky, nevztahují se k výrobním ani jiným procesům výrobce jako subjektu, nezohledňují další rizikové faktory jako např. ovládání výrobce. Přitom v dnešní době spočívá kybernetické bezpečnostní riziko často nikoli pouze v technickém řešení produktu, jako spíše v jeho výrobci a geopolitických souvislostech zázemí výrobce. Příkladem jsou např. významná varování NÚKIB z roku 2018 před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation[66]

[65] Podrobněji k sankcím viz čl. 53 aktu o kybernetické odolnosti.

[66] Varování NÚKIB ze dne 17. 12. 2018 před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation. [online]. 2018. [cit. 15. 11. 2022]. Dostupné z: https://nukib.cz/cs/uredni-deska/.

a z roku 2022 před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím, kde NÚKIB uvádí: „*Kybernetická bezpečnost nespočívá pouze na posuzování technických aspektů používaných technologií, ale například při výběru dodavatelů je nutné zvážit i netechnické aspekty bezpečnosti daných technologií, tedy posoudit důvěryhodnost dodavatelů a poddodavatelů (výrobců) dané technologie*“[67]. V současnosti v České republice vzniká návrh zákona, který by měl zavést mechanismus prověřování dodavatelů technologických prvků nejvýznamnější (strategické) infrastruktury a v případě jejich vysoké rizikovosti omezit využití takových dodavatelů pro tyto nejkritičtější infrastruktury[68]. Návrh aktu o kybernetické odolnosti takovéto aspekty nereflektuje. Výslovně však zmiňuje možnost členských států zohlednit i netechnické aspekty kybernetické bezpečnosti včetně nežádoucího vlivu třetí země na dodavatele v souvislosti s potřebou zajištění vysoké úrovně odolnosti a koordinovaným posouzením rizik kritických dodavatelských řetězců ve smyslu směrnice NIS2[69]. Dále může členský stát, resp. jeho orgán dozoru nad trhem, postupovat podle čl. 46 aktu o kybernetické odolnosti upravujícího postup v případě vyhovujících produktů představujících významné kybernetické bezpečnostní riziko. Podle čl. 46 však nestačí k tomuto postupu pouhá skutečnost, že produkt představuje významné kybernetické riziko, ale musí vyvolat i další riziko ve vyjmenovaných oblastech jako je např. zdraví nebo bezpečnost osob.

Problematické je vymezení působnosti aktu o kybernetické odolnosti ve vztahu k software poskytovanému formou služby (SaaS) s ohledem na formulaci výjimky pro zpracování dat na dálku. Na problematičnost a nejasnost tohoto vymezení poukazují četní zástupci veřejnosti v rámci veřejné

[67] Varování NÚKIB ze dne 30. 5. 2022 před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím. [online]. 2022. [cit. 15. 11. 2022]. Dostupné z: https://nukib.cz/cs/uredni-deska/.

[68] Viz NÚKIB. Stát vstupuje do závěrečné fáze přípravy návrhu zákona o snižování rizik spojených s dodavateli informačních a komunikačních technologií. [online]. 2022. [cit. 25. 11. 2022]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1911-stat-vstupuje-do-zaverecne-faze-pripravy-navrhu-zakona-o-snizovani-rizik-spojenych-s-dodavateli-informacnich-a-komunikacnich-technologii/

[69] Viz recitál 33 aktu o kybernetické odolnosti.

diskuze k návrhu[70] a organizace expertů nebo výrobců[71]. Samotná skutečnost, že v podstatě všichni komentující považují vymezení dopadu aktu o kybernetické odolnosti na poskytování software nebo platforem formou služby za nejasné, je známkou toho, že by příslušná ustanovení měla být přepracována. Nesrozumitelnost nebo nejasnost právní normy pro její adresáty je třeba považovat za nedostatek významně snižující právní jistotu, která je jedním z účelů práva, proto je žádoucí takový nedostatek v legislativním procesu odstranit. Nařízení se řadí k předpisům produktové bezpečnosti NLF, je logické nevztahovat je na služby, nicméně to neznamená, že by nutně měly být vyňaty produkty s digitálními prvky používané k poskytování těchto služeb. Výklad působnosti norem NLF zahrnuje pod pojem *dodání na trh* rovněž poskytování výrobků formou výpůjčky, leasingu, nájmu[72], obecněji tedy jakékoli dodání za účelem použití v rámci obchodní činnosti. Poskytování software formou služby se s ohledem na jeho nehmotnou podstatu, kdy zákazník software jako takový neužívá, ale čerpá pouze výsledky služby, samozřejmě liší od nájmu nebo výpůjčky hmotného produktu. Pro samotný software užívaný k poskytování služby, nikoli však pro službu jako takovou, by podle mého názoru mělo být splnění požadavků nařízení požadováno. Text nařízení by měl v této otázce být jasný a srozumitelný.

---

[70] Viz např. Evropská komise. Podělte se o svůj názor. Akt o kybernetické odolnosti – nová pravidla kybernetické bezpečnosti pro digitální produkty a podpůrné služby. The Federation of Finnish Enterprises. nebo BSA Recommendations on the EU Cyber Resilience Act. [online]. 2022. [cit. 30. 11. 2022]. Obojí dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Akt-o-kyberneticke-odolnosti-nova-pravidla-kyberneticke-bezpecnosti-pro-digitalni-produkty-a-podpurne-sluzby_cs.

[71] Srov. např. Center for Data Innovation. Feedback to the European Commission on the Draft Cyber Resilience Act. [online]. 15. 12. 2022. [cit. 16. 4. 2023]. Dostupné z: https://datainnovation.org/2022/12/feedback-to-the-european-commission-on-the-draft-cyber-resilience-act/ nebo Digitaleurope. Cybersecurity everywhere: deciphering the Cyber Resilience Act. [online]. 23. 1. 2023. [cit. 16. 4. 2023]. Dostupné z: https://www.digitaleurope.org/policies/cybersecurity/

[72] Viz „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 19 [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC.

K nejasným a veřejností hojně kritizovaným ustanovením patří dále vymezení výjimky pro software s otevřeným zdrojovým kódem[73]. V důsledku požadavku na dodávání mimo rámec obchodní činnosti a zároveň široce pojatý rozsah toho, co vše je uvedením produktu na trh, vznikají otázky, jaké všechny aktivity poskytnutí open source software lze ještě vnímat jako nekomerční a jaké již nikoli. Vzhledem k (nejen) ekonomickému významu, který má open source software celosvětově pro rozvoj celého IT odvětví, je zároveň na místě vymezit vztah aktu o kybernetické odolnosti k regulaci tohoto typu software přímo v normativním textu.

Dalším potenciálně problematickým místem je stanovení povinnosti výrobcům produktů s digitálními prvky po očekávanou dobu životnosti produktu nebo po dobu pěti let od jeho uvedení na trh – podle toho, která doba je kratší – zajistit, že je se zranitelnostmi tohoto produktu nakládáno účinně a v souladu se základními požadavky stanovenými v oddíle 2 přílohy I[74], což mj. zahrnuje poskytování bezpečnostních aktualizací. Návrh ale neobsahuje žádnou definici ani pravidla pro určení *očekávané doby životnosti*. Zejména v případě software je stanovení očekávané doby životnosti problematické. Lze jí chápat tak, že očekávaná doba životnosti končí vydáním nové verze téhož software? To by dávalo logický smysl z pohledu výrobců, kteří by nemuseli podporovat řešení zranitelností u více verzí téhož software najednou. Ovšem z pohledu uživatelů jde, zejména v případě placeného software, o situaci významně nežádoucí, která by je nutila k pořizování dalších verzí. Očekávanou dobu životnosti by mohl uvádět přímo výrobce, nicméně to by si pak výrobce sám stanovil dobu, po kterou je povinen zranitelnosti produktu řešit a regulace této doby v právním aktu by ztrácela význam.

Zavedení nové regulace bude pro výrobce produktů s digitálními prvky představovat nové náklady zejména na zajištění compliance, due diligence dodavatelského řetězce nebo nutné administrativy, ať již v podobě interních (např. nutnost najmout nové zaměstnance) nebo externích (zejm. na posouzení shody subjektem posuzování shody) nákladů. Logika fungování

[73] Viz recitál 10 aktu o kybernetické odolnosti.

[74] Viz čl. 10 odst. 6 aktu o kybernetické odolnosti.

trhu vede k závěru, že tyto náklady se pravděpodobně promítnou do ceny produktů s digitálními prvky jejím navýšením[75]. To by v případě významnějšího navýšení ceny mohlo vést zejména u spotřebitelů k nákupu alternativních produktů s digitálními prvky ze třetích zemí, které podobné regulaci nepodléhají a jsou proto levnější. V takovém případě by se částečně ztrácel Komisí očekávaný efekt jak celkového zvýšení kybernetické bezpečnosti navzájem propojených zařízení, tak ekonomické stimulace výroby produktů s digitálními prvky v Unii a zvýšení poptávky po nich i mimo EU[76]. Publikované výzkumy svědčí spíše o opaku, kdy většina spotřebitelů uvádí ochotu zaplatit vyšší cenu za bezpečnější produkt s digitálními prvky[77], je však namístě zmínit, že tyto výzkumy vycházejí z dotazníkových šetření, nikoli reálného tržního chování, a byly provedeny v ekonomicky silných státech. Jejich závěry tak nemusí platit pro trhy slabších ekonomik východní nebo jižní Evropy. Podíl spotřebitelů na poptávkové straně trhu produktů s digitálními prvky je, přinejmenším v případě softwaru, pravděpodobně významně menší[78] než podíl hospodářských subjektů, toto spotřebitelské chování (pokud k němu dojde) tak zřejmě nebude mít významnější dopad.

Navýšení nákladů přitom nejcitelněji dopadne zejména na malé a střední podniky („SMEs“) včetně start-upů a technologických inovátorů. SMEs tvoří většinu výrobců produktů s digitálními prvky v Unii, ačkoli jejich tržní podíl tomu neodpovídá. Např. na trhu softwarových produktů SMEs představují více než 99 % hospodářských subjektů, většinu (59 %)

[75] Srov. Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 1/3. s. 62. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

[76] Viz důvodová zpráva aktu o kybernetické odolnosti.

[77] Srov. Blythe, J.M., Johnson, S.D. & Manning, M. What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Science. 9, 1 (2020). https://doi.org/10.1186/s40163-019-0110-3.

[78] Srov. Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 1/3. s. 25. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

obratu ale vytváří několik „velkých hráčů“[79]. Navýšení nákladů přitom bude mít jasně závažnější dopad na SMEs než na kapitálově silné velké korporace[80], což může vést v některých případech k další redukci jejich podílu na trhu. Obava ze zatížení dopadajícího na SMEs z řad výrobců se opakovaně objevuje i v rámci veřejné diskuze ze strany jednotlivých podniků i jejich asociací.[81]

Do kategorie SMEs spadají i mikropodniky[82], které tvoří dokonce 94 % SMEs působících na softwarovém trhu Unie[83]. Realita přinejmenším v České republice je taková, že významnou část těchto „mikropodniků“ představují ve skutečnosti vývojáři – jednotlivci zcela bez zaměstnanců působící jako tzv. „freelanceři“, tedy samostatní podnikatelé (v ČR v režimu živnostenského podnikání) pracující na různých softwarových projektech, jak pro zákazníky z řad korporací, tak nezávisle z vlastní iniciativy . Tito vývojáři se budou ocitat v různém právním postavení podle toho, zda software samostatně vyvíjejí a dodávají pod svým jménem, nebo působí pouze jako členové většího vývojářského týmu pro projekt řízený jinou (zpravidla právnickou) osobou, která software uvádí na trh pod svým jménem nebo

---

[79] Viz Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 1/3. s. 24. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

[80] Podrobněji viz Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 1/3, s. 55-56 [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

[81] Podrobněji srov. Evropská komise. Podělte se o svůj názor. Akt o kybernetické odolnosti – nová pravidla kybernetické bezpečnosti pro digitální produkty a podpůrné služby. The Federation of Finnish Enterprises. [online]. 2022. [cit. 15. 11. 2022]. Dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410 Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/feedback_en?p_id=31490443

[82] Mikropodnikem je podnik s 0-9 zaměstnanci.

[83] Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 2/3, s. 29. [online] 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy-.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

ochrannou známkou. V případě samostatně vyvíjeného software, který vývojář nabízí nebo dodává svým jménem, se bude dostávat do postavení výrobce a bude muset plnit povinnosti stanovené aktem o kybernetické odolnosti, což bude pro jednotlivce znamenat velkou administrativní zátěž.

Povinnost zaobírat se kybernetickou bezpečností, podstoupit proces posuzování shody a vytvářet povinnou dokumentaci může vést rovněž k prodloužení doby vývoje a výroby produktu s digitálními prvky oproti konkurenci, což může mít za následek ztrátu konkurenční výhody prvního uvedení určitého typu produktu nebo jeho nové verze na globální trh oproti výrobcům ze třetích zemí[84]. Mimoevropští výrobci mohou dát přednost prvotnímu uvedení nového produktu s digitálními prvky nejprve na trzích s méně náročnými legislativními požadavky, a až posléze uvést produkt na trh také v Unii, což by mohlo mít za následek technologické zaostávání unijního trhu za zbytkem světa, zejména asijskými trhy.

Uplatňování aktu o kybernetické odolnosti podstatně zatíží nejen výrobce, ale i subjekty posuzování shody a vnitrostátní orgány dozoru nad trhem. S ohledem na množství běžně používaných produktů s digitálními prvky, které narůstá doslova na denní bázi, a jejich rozdílnost a složitost je jen obtížně představitelné, že orgány dozoru nad trhem budou skutečně schopny provádět efektivní dozor a kontrolu dodržování nové regulace.

9. ZÁVĚR

Akt o kybernetické odolnosti by měl navázat na stávající unijní právní úpravu a doplnit chybějící část v podobě regulace produktové kybernetické bezpečnosti. Legislativně technicky odpovídá ostatním předpisům nového legislativního rámce (NLF), atypický je ale svou horizontální působností, která má zahrnovat širokou škálu navzájem odlišných produktů. Potřebnost přijetí aktu o kybernetické odolnosti lze mít za dostatečně odůvodněnou jednak nutností ochrany práv jednotlivců, která mohou být v době digitálně propojeného internetu věcí (IoT) zranitelností produktů s digitálními prvky

[84] K otázce výhody prvního uvedení na trh srov. Evropská Komise. Commission staff working document. Impact Assessment Report. Part 1/3. SWD (2022) 282 final. s. 11. s. 64. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

ohrožena, a zároveň zjevným selháváním trhu v této oblasti. Ze stávající zkušenosti je zřejmé, že motivace výrobců zavést opatření posilující kybernetickou bezpečnost jejich produktů bez existence regulatorního tlaku, je nedostatečná[85].

Nové nařízení bude přínosem pro koncové uživatele produktů s digitálními prvky, ať již z řad spotřebitelů, podnikatelů nebo správců kritických informačních infrastruktur, kteří se budou moci spolehnout na minimální standard kybernetické bezpečnosti všech produktů s digitálními prvky dodávaných na trh v Unii bez nutnosti složitě získávat dnes často nedostupné informace. Skutečnost, že se jedná o jednotnou regulaci pro celý společný trh, by měla být přínosem i pro výrobce, dovozce a distributory produktů s digitálními prvky, kteří se tak budou moci spoléhat na stejná pravidla platná pro celý trh Unie bez nutnosti zajišťovat soulad se standardy stanovenými jednotlivými státy. Uživatelé z řad povinných subjektů podle směrnice NIS2 ale budou muset stejně zvažovat i u produktů uvedených na trh v souladu s tímto nařízením, zda neexistují i jiná (netechnická) rizika kybernetické bezpečnosti spojená s užíváním těchto produktů. Otázkou je, zda by nebylo vhodnější přímo v aktu o kybernetické odolnosti upravit právě i zohlednění těchto typů rizik.

Z hlediska znění textu nařízení by bylo vhodné, aby akt o kybernetické odolnosti jasně definoval, zda nebo kdy se vztahuje na software nabízený formou služby a kdy nikoli. Stejně tak by bylo vhodné doplnit pravidla nebo alespoň výkladová vodítka pro určení očekávané doby životnosti. Rovněž částečné vynětí open source softwaru z působnosti nařízení by bylo vhodné zakotvit přímo v normativním textu nikoli pouze v recitálu a učinit je jasnějším.

Z hlediska faktických dopadů nové regulace lze očekávat u výrobců software a hardware, přinejmenším v počátečním období, navýšení nákladů na

[85] Srov. TOMLINSON, Andrew; PARKIN, Simon; SHAIKH, Siraj Ahmed. Drivers and barriers for secure hardware adoption across ecosystem stakeholders. Journal of Cybersecurity, 2022, roč 8., č. 1, s. 7. nebo Evropská Komise. Commission staff working document. Impact Assessment Report. Part 1/3. SWD (2022) 282 final. s. 17. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

vývoj a výrobu produktů s digitálními prvky, které může být pro výrobce z řad SMEs problematické a může vést k posílení tržního postavení kapitálově silných „velkých hráčů“ na úkor inovativních start-upů a jiných menších podniků nebo nezávislých vývojářů. Z pracovních dokumentů Komise je zřejmé, že si je tohoto nebezpečí vědoma. Pro snížení zátěže spojené s adaptací na novou právní úpravu by proto bylo vhodné zavést opatření, například ve formě bezplatného přístupu k odpovídajícím metodickým nástrojům, postupům, šablonám a dalším informacím, která zejména malým a středním podnikům tento proces usnadní.

10. SEZNAM ZDROJŮ

[1] Blythe, J.M., Johnson, S.D. & Manning, M. What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Science. 2022, č. 9. https://doi.org/10.1186/s40163-019-0110-3.

[2] Chiarra, P. G. The Cyber Resilience Act: the EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements. Int. Cybersecur. Law Rev. 2022, č. 3, s. 255–272. https://doi.org/10.1365/s43439-022-00067-6.

[3] Tomlinson, A. Parkin, S. Shaikh, S.A. Drivers and barriers for secure hardware adoption across ecosystem stakeholders. Journal of Cybersecurity, 2022, roč 8., č. 1, s. 1-14. https://academic.oup.com/cybersecurity/article/8/1/tyac009/6656148?searchresult=1

[4] Evropská Komise. Společné sdělení Evropskému parlamentu a Radě Strategie kybernetické bezpečnosti EU pro digitální dekádu. JOIN (2020) 18 final. [online]. 202. [cit. 1. 11. 2022] Dostupné z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.

[5] Evropská Komise. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Digitální kompas 2030: Evropské pojetí digitální dekády. COM (2021) 118 final, [online]. 2020. [cit. 1. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

[6] Projev předsedkyně Komise von der Leyenové o stavu Unie v roce 2021. [online]. 2021. [cit. 1. 11. 2022]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701.

[7] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020, COM/2022/454 final. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52022PC0454&qid=1667332176493.

[8] Evropská Komise. Sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 9-10. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC.

[9] Evropská Komise. Commission staff working document. Impact Assessment Report. Part 1/3. SWD (2022) 282 final. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

[10] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o obecné bezpečnosti výrobků, o změně nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 a o zrušení směrnice Rady 87/357/EHS a směrnice Evropského parlamentu a Rady 2001/95/ES. COM/2021/346 final. [online]. 2022. [cit. 6. 11. 2022] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A52021PC0346

[11] Rozsudek Soudního dvora ze dne 20. února 1979 ve věci 120/78 „Cassis de Dijon". ECLI:EU:C:1979:42. Dostupné z : https://curia.europa.eu/jcms/jcms/Jo1_6308/

[12] Varování NÚKIB ze dne 17. 12. 2018 před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation. [online]. 2018. [cit. 15. 11. 2022]. Dostupné z: https://nukib.cz/cs/uredni-deska/

[13] Varování NÚKIB ze dne 30. 5. 2022 před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím. [online]. 2022. [cit. 15. 11. 2022]. Dostupné z: https://nukib.cz/cs/uredni-deska/.

[14] Podělte se o svůj názor. Akt o kybernetické odolnosti – nová pravidla kybernetické bezpečnosti pro digitální produkty a podpůrné služby. [online]. 2022. [cit. 15. 11. 2022]. Dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Akt-o-kyberneticke-odolnosti-nova-pravidla-kyberneticke-bezpecnosti-pro-digitalni-produkty-a-podpurne-sluzby_cs.

[15] NÚKIB. Stát vstupuje do závěrečné fáze přípravy návrhu zákona o snižování rizik spojených s dodavateli informačních a komunikačních technologií. [online]. 2022. [cit. 25. 11. 2022]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1911-stat-vstupuje-do-zaverecne-faze-pripravy-navrhu-zakona-o-snizovani-rizik-spojenych-s-dodavateli-informacnich-a-komunikacnich-technologii/

[16] Digitaleurope. Cybersecurity everywhere: deciphering the Cyber Resilience Act. [online] 2023. [cit. 16. 4. 2023]. Dostupné z: https://www.digitaleurope.org/policies/cybersecurity/

[17] Center for Data Innovation. Feedback to the European Commission on the Draft Cyber Resilience Act. [online] 2022. [cit. 16. 4. 2023]. Dostupné z: https://datainnovation.org/2022/12/feedback-to-the-european-commission-on-the-draft-cyber-resilience-act/

Toto dílo lze užít v souladu s licenčními podmínkami Creative Commons BY-SA 4.0 International (http://creativecommons.org/licenses/by-sa/4.0/legalcode).