Hodnocení dopadů regulace (RIA)

Závěrečná zpráva z hodnocení dopadů regulace

SHRNUTÍ ZÁVĚREČNÉ ZPRÁVY RIA

1. Základní identifikační údaje	
Návrh zákona o kybernetické bezpečnosti a návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti	
Zpracovatel / zástupce předkladatele: Národní úřad pro kybernetickou a informační bezpečnost	Předpokládaný termín nabytí účinnosti: 18. říjen 2024
Implementace práva EU: Ano (Lhůta pro implementaci 17. 10. 2024)	

2. Cíl návrhu zákona

Návrh nového zákona o kybernetické bezpečnosti (dále jen „návrh zákona“) a jeho prováděcích právních předpisů změní způsob stanovení okruhu povinných osob a způsob jejich identifikace, rozdělí povinné osoby do režimů stanovujících jejich práva a povinnosti, zavede nové požadavky na povinné osoby (aktualizuje stávající bezpečnostní opatření a spolu s tím stanoví novou množinu bezpečnostních opatření pro část nových povinných osob), upraví povinnost hlášení kybernetických bezpečnostních incidentů, aktualizuje stávající povinnosti spojené se zaváděním opatření a hlášením kontaktních údajů, změní požadavky spojené s institutem provozovatelů systému, zavede mechanismus prověřování bezpečnosti dodavatelského řetězce (viz níže v této části) a novou úpravu výkonu kontroly plnění povinností vyplývajících ze zákona, v souladu s evropským právním předpisem změní výši pokut a opraví další identifikované nedostatky stávající právní úpravy.

Smyslem zavedení mechanismu bezpečnosti dodavatelského řetězce je přispět k zajištění dlouhodobě udržitelné bezpečnosti České republiky (dále jen „ČR“) prostřednictvím zabezpečení a zvýšení odolnosti osob a institucí, jež jsou nezbytné pro naplňování základních funkcí státu. Tohoto cíle bude dosaženo prostřednictvím omezení závislosti vybraných povinných osob (dále také „poskytovatel strategicky významné služby“) na dodavatelích představujících strategickou hrozbu v oblasti informačních a komunikačních technologiích strategicky významné infrastruktury.

Vybrané povinné osoby, od kterých se odvíjí obsah pojmu „strategicky významná infrastruktura“, byly identifikovány na základě významnosti jimi poskytované služby pro chod státu ve vybraných regulovaných odvětvích a jejich přesné vymezení je představeno v kapitole 1.4 Identifikace dotčených subjektů.

Návrh zákona zmocní Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) k identifikaci a vyhodnocení hrozeb plynoucích z dodavatelských řetězců pro národní bezpečnost nebo vnitřní pořádek. Zda jsou tyto hodnoty v ohrožení, bude

vyhodnoceno na základě konkrétních podmínek stanovených prováděcím právním předpisem. Mechanismus prověřování bezpečnosti dodavatelského řetězce umožní Úřadu na základě zákonného zmocnění omezit či vyloučit z vymezených dodávek povinných osob mechanismu takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií. Ostatní státní orgány zapojené do procesu prověřování budou Úřadu poskytovat součinnost a informace z jejich zákonné působnosti. Bezpečnostní rada státu bude o omezení či vyloučení plnění ze strategicky významné infrastruktury informována a bude moci zvážit a projednat dopady a přínosy takového kroku. Návrh opatření obecné povahy bude rovněž projednán s Ministerstvem financí a dalšími zapojenými orgány, a v případě, že se návrh opatření obecné povahy bude dotýkat jejich působnosti, s Českým telekomunikačním úřadem a Energetickým regulačním úřadem. V závaznějších případech, kdy nebudou v opatření obecné povahy dodrženy odpisové doby, bude nutné také schválení formou závazného stanoviska Ministerstvem průmyslu a obchodu, Ministerstvem zahraničních věcí a Ministerstvem vnitra.

Návrh zákona doplňuje stávající systém zajišťování kybernetické bezpečnosti založený na aktivitě a odpovědnosti správce regulovaného informačního systému. Návrh zákona má státu umožnit zjišťovat strategická rizika spojená s dodavateli a omezovat vliv rizikových dodavatelů na nejkritičtějších částech nejvýznamnější infrastruktury. Měl by tak vzniknout komplexní a účinný systém omezování nejvýznamnějších strategických rizik spojených s dodavatelskými řetězci, který přenáší související komplikovaný bezpečnostní proces na stát, a přitom nemění osvědčené principy současné regulace kybernetické bezpečnosti.

Návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti (dále jen „návrh změnového zákona“) je předkládán současně s návrhem nového zákona, který má za cíl nahradit dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“ nebo „ZKB“) a jeho prováděcí právní předpisy. Návrh zákona je zároveň transpozičním předpisem 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). Právě v souvislosti s obsahem směrnice NIS 2 a dalšími změnami, které nastanou s účinností návrhu zákona, je nutné změnit ustanovení některých účinných právních předpisů v ČR.

Cílem návrhu změnového zákona je tedy změnit všechny níže uvedené právní předpisy, a docílit tak stavu, v němž bude český právní řád v souladu se změnami, ke kterým dojde díky přijetí návrhu zákona:

- zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů (dále jen „ZoB“)
- zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů (dále jen „zákon o poštovních službách“),
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen „ZoISVS“),
- zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále jen „ZEK“),
- zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů (dále jen „ZPMS“),

- zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (dále jen „AML“, odvozeno z „*anti money laundering*“),
- zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů (dále jen „daňový řád“),
- zákon č. 17/2012 Sb., o Celní správě České republiky, ve znění pozdějších předpisů (dále jen „ZCS“),
- zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic) (dále jen „ZoPZI“).

3. Agregované dopady návrhu zákona

3.1 Dopady na státní rozpočet a ostatní veřejné rozpočty: Ano

Dopady na státní rozpočet mohou být dány jak požadavky na plnění povinností plynoucích z návrhu zákona od subjektů veřejné správy, tak požadavky na zajištění kapacit nutných k zajištění fungování Úřadu. Subjekty veřejné správy jsou již za současného znění zákona o kybernetické bezpečnosti z velké části povinny zabezpečovat své systémy v souladu se zákonnými požadavky. V tomto případě lze tedy očekávat požadavky na poskytnutí prostředků k plnění zákona. Nad rámec implementačních a průběžných nákladů, které vynakládají povinné subjekty veřejné správy již v současné době podle současného znění zákona o kybernetické bezpečnosti, a které jsou z části započitatelné také do nákladů spojených s tímto návrhem zákona. Podstatná část subjektů veřejné správy je již nyní povinným subjektem podle současného zákona o kybernetické bezpečnosti a jsou jim uloženy téměř totožné povinnosti jaké vyplývají z tohoto návrhu. Podstatným rozdílem je však šíře navrhované regulace, která v souladu s přístupem zvoleným směrnicí NIS 2 rozšiřuje rozsah zajišťovaných systémů z jednotlivých ohraničených informačních systémů na služby v rozsahu výkonu činnosti daného subjektu veřejné správy, což náklady navyšuje. Přestože tedy subjekty veřejné správy budou moci v části nákladů na zajištění kybernetické bezpečnosti pokračovat podle dosavadního rozpočtování, bude stejně tak potřeba promítnout ostatní nově navýšené náklady do budoucích rozpočtů těchto subjektů.

Primárně budou veškeré výdaje a zvýšená potřeba v personální a platové oblasti, jež jsou spojeny s implementací návrhu zákona o kybernetické bezpečnosti včetně prováděcích předpisů ve všech dotčených rozpočtových kapitolách, pokryty v rámci schválených rozpočtových limitů a stanovených limitů počtu míst a objemu prostředků na platy.

Pokud správci jednotlivých dotčených kapitol identifikují potřebu navýšení své kapitoly rozpočtu nad rámec schválených rozpočtových limitů nebo stanovených limitů počtu míst a objemu prostředků na platy, bude taková potřeba předmětem standardního vyjednávání o podobě relevantní kapitoly státního rozpočtu.

Nad rámec výše uvedeného je pro financování nákladů také možné využívat k tomu vzniklé nebo do budoucna vznikající dotační programy na úrovni Evropské unie, případně dotační programy původně na financování kybernetické bezpečnosti nezaměřené, ale dílčím způsobem k tomu využitelné (např. the Digital Europe Programme apod.).

Nevýhodou otázky analýzy finančních dopadů na regulované subjekty je skutečnost, že distribuce nákladů na kybernetickou bezpečnost není plošná a existuje informační asymetrie ve směru od subjektů samotných k regulačnímu orgánu (tj. jen regulovaná organizace samotná

by měla být schopná identifikovat své vlastní náklady na zavedení a udržování přiměřené úrovně kybernetické bezpečnosti).

Výši finančních dopadů není možné předem stanovit a veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídající hodnotou.

Distribuce nákladů na kybernetickou bezpečnost není plošná z důvodu velkého počtu neznámých a proměnlivých indikátorů:

- aktuální stav zabezpečení každé jedné organizace,
- různý cílový stav každé organizace související s významností její činnosti a potřebou zajistit její fungování,
- široká variabilita rozsahu opatření na zajištění kybernetické bezpečnosti, která může být naprosto odlišná u jednotlivých organizací,
- identifikace toho, co je nákladem na zajištění kybernetické bezpečnosti a co je nákladem na běžný provoz informačních a komunikačních technologií (dále jen „ICT“) u daného subjektu (tyto množiny se velmi prolínají),
- soulad se zněním zákona o kybernetické bezpečnosti,
- neznámý přesný počet výsledných regulovaných subjektů,
- proměnlivost nákladů v čase související jak s makroekonomickými otázkami, tak s vývojem technologií a mnoho dalších indikátorů.

Tyto indikátory jsou bohužel spjaty se systémem zajištění kybernetické bezpečnosti, ať už podle současného znění zákona o kybernetické bezpečnosti, tak i z obecně přijímaných norem upravujících kybernetickou bezpečnost.

Při zpracovávání RIA k návrhu zákona došlo k orientačnímu zohlednění výpočtů nákladů provedených podle:

- návrhu novelizace zákona o kybernetické bezpečnosti (2017),
- návrhu novelizace vyhlášky o významných informačních systémech (2019),
- Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2021),
- Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2022),
- průzkum u vybraných subjektů v rámci přípravy metodického materiálu pro zjištění interních nákladů organizace v souvislosti s přípravou této novely (2023).

Tím došlo k orientačnímu výpočtu nákladů na zavedení a následné provádění především bezpečnostních opatření ve formě velmi hrubých odhadů, pohybujících se přibližně mezi 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému. Změny v přístupu k regulaci zavedené směrnicí, výše uvedené proměnné (především různý stav současného zabezpečení u regulovaných organizací), rozdělení povinností uložených těmto subjektům, stejně tak jako agregace řady bezpečnostních opatření u více systémů v rámci organizace pak mohou tyto hodnoty ovlivnit, nicméně s ohledem na výše uvedené je možné očekávat požadavky na veřejné rozpočty v této přibližné míře. Podstatnou proměnnou tak bude především to, jaký je daný počet jednotlivých systémů u každé konkrétní organizace, a takový násobek výše uvedené částky bude potřeba daným organizacím alokovat v rámci veřejných rozpočtů.

Naprostá většina nově regulovaných povinných osob vzejde v souladu s obsahem transponované směrnice ze soukromého sektoru.

I výše zmíněný průzkum související s touto novelou, který byl zejména prostředkem ověření funkčnosti metodiky k vyčíslení nákladů uvnitř organizace pro vnitřní potřebu adresátů zákona o kybernetické bezpečnosti, dokumentuje vliv výše popsaných indikátorů a dokládá, že není z pohledu regulátora možné vyčíslit dopady na rozpočty v podobě absolutního čísla, které by bylo dostatečně přesné. Z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů.

I mezi typově a velikostně shodnými subjekty, které poskytují veřejnosti druhově srovnatelné služby, byl rozptyl vyčíslených nákladů jednotky milionů, přičemž tyto subjekty vyčíslovaly své náklady rovněž v jednotkách milionů za organizaci. V tomto případě se jednalo o 5 srovnatelných organizací, u kterých se rozptyl pohyboval od 6 milionů za organizaci do 11 milionů za organizaci. Co se týče rozptylu mezi velkou koncernovou organizací s mnoha aktivy, která však má s řízením bezpečnosti zkušenosti, a malou začínající organizací, lze mluvit o rozptylu jednotek miliard do nízkých jednotek milionů.

I zde je však třeba poznamenat, že se nejedná o výdaje, které by bylo nutné vynaložit v rámci jednoho roku nutného pro implementaci povinností zákona o kybernetické bezpečnosti. Vždy je tu možnost tyto náklady rozložit do jednotlivých let v závislosti na prioritizaci daných aktiv a finančních možností organizací.

V souhrnu je nárůst povinných osob minimálně 15násobný oproti současnému stavu, což bude muset být reflektováno v zajištění fungování gestora této problematiky. Náklady na straně Úřadu budou v personálních otázkách vyšší desítky tabulkových míst oproti aktuální Koncepci rozvoje Úřadu[1]. Takto velký nárůst je dán skutečností, že na rozdíl od evropské úpravy byl Úřad od svého počátku stavěn jako Úřad poskytující služby omezené množině povinných osob (cca 500), čemuž odpovídaly veškeré dosavadní koncepce a požadavky. S přicházející změnou vznikne potřeba odchýlit se od dosavadního směřování a změnit jej tak, aby bylo možné služby poskytovat i novým povinným osobám. Personální náklady bude potřeba alokovat především do kapacitního posílení služeb vládního CERT (především v otázkách řešení kybernetických bezpečnostních incidentů a jejich analýzy, pentestů či skenů zranitelností), výkonu metodického řízení povinných osob (lze očekávat, že v souladu s obsahem směrnice NIS 2 budou pod zákonnou regulaci nově spadat také organizace s nižší úrovní kybernetické bezpečnosti) a výkonu kontroly (zde především v otázkách kontrol prováděných Úřadem). Násobný nárůst oproti aktuální Koncepci rozvoje Úřadu bude také ve finančních nákladech. Výsledné náklady se budou odvíjet od finálního znění schváleného návrhu. Kromě těchto personálních a finančních nákladů se předpokládá vznik informačního systému, který umožní řádné vykonávání pravomocí a povinností Úřadem v souvislosti s nárůstem počtu regulovaných subjektů a celkovému rozšíření souvisejících agend.

K zavedení mechanismu bezpečnosti dodavatelského řetězce je namístě podrobněji doplnit, že na poměry nových oblastí působnosti ústředního orgánu státní správy se očekává nízký dopad na státní rozpočet. Ve vztahu k návrhu zákona lze předpokládat především nutnost vyhrazení jednotek až nízkých desítek tabulkových míst u zapojených státních orgánů a rozšíření stávajících či připravovaných informačních systémů k technické obsluze procesu prověřování. V souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy či prověřování zahraničních investorů podle zákona

[1] Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost, 2020, dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/Koncepce_rozvoje_NUKIB.pdf

o prověřování zahraničních investic, a to včetně účelného využívání informačních systémů, které tyto agendy podporují.

Dopady na státní rozpočet pak může mít také zvýšení nákladů poskytovatelů strategicky významné služby z řad veřejné správy.

Z hlediska zásad pro tvorbu digitálně přívětivé legislativy jsou respektovány zásady budování přednostně digitálních služeb, maximální opakovatelnosti a znovupoužívání údajů a služeb, konsolidace a propojování informačních systémů veřejné správy, otevřenosti a transparentnosti včetně otevřených dat a služeb a technologické neutrality, což v konečném důsledku vede k minimalizaci vynaložených nákladů, resp. maximalizace jejichž využití. Veškeré náklady vynaložené ze státního či jiného veřejného rozpočtu navíc směřují ke zvyšování kybernetické bezpečnosti při respektování zákonných omezení co se týče možností zásahu do ochrany osobních práv a svobod.

Termín zohlednění relevantních požadavků je nutné vést v patrnost v souvislosti s očekávanou účinností návrhu zákona. Pokud bude účinnost zákona stanovena v souladu s transpoziční lhůtou, klade návrh zákona požadavky na zavedení nejnákladnějších procesů do 17. října 2025. Přestože náklady jsou také provozní a je proto potřeba je zohledňovat každoročně, v období mezi roky 2025 a 2026 lze očekávat ustálení požadavků na financování hlavních povinností podle tohoto návrhu zákona.

Z relevantních právních předpisů, které se navrhují změnit v souvislosti s přijetím návrhu zákona, má dopad na státní rozpočet a ostatní veřejné rozpočty jen změna ZoISVS. Tyto dopady však budou pouze minimální, protože cílem změny je zachovat kontinuitu dosavadní regulace. Dá se předpokládat, že obce s pověřeným obecním úřadem či obce I. stupně, kterým návrh změnového zákona ukládá povinnost přiměřeně zavádět bezpečnostní opatření pro jejich informační systémy podle návrhu zákona, již mají tato opatření zavedena z důvodu plnění původního požadavku ZoISVS.

Primárně budou veškeré výdaje a zvýšená potřeba v personální a platové oblasti, jež jsou spojeny s implementací návrhu změnového zákona včetně prováděcích předpisů ve všech dotčených rozpočtových kapitolách, pokryty v rámci schválených rozpočtových limitů a stanovených limitů počtu míst a objemu prostředků na platy.

Pokud správci jednotlivých dotčených kapitol identifikují potřebu navýšení své kapitoly rozpočtu nad rámec schválených rozpočtových limitů nebo stanovených limitů počtu míst a objemu prostředků na platy, bude taková potřeba předmětem standardního vyjednávání o podobě relevantní kapitoly státního rozpočtu.

Nad rámec výše uvedeného je pro financování nákladů také možné využívat k tomu vzniklé nebo do budoucna vznikající dotační programy na úrovni Evropské unie, případně dotační programy původně na financování kybernetické bezpečnosti nezaměřené, ale dílčím způsobem k tomu využitelné (např. the Digital Europe Programme apod.).

3.2 Dopady na mezinárodní konkurenceschopnost ČR: Ano

Kontinuálním zvyšováním kybernetické bezpečnosti nepodnikatelských, ale především podnikatelských subjektů v ČR dochází k respektování mezinárodněprávního principu due dilligence, tj. principu, na jehož základě je suverénní stát povinen v rámci své jurisdikce aktivně bránit škodám, které by mohly vzniknout ostatním státům nebo mezinárodnímu společenství. Stejným způsobem dochází také k tomu, že subjekty předchází škodám, které by měly potenciál poškozovat jejich reputaci nebo omezovat jimi poskytované služby.

V souvislosti se zavedením mechanismu bezpečnosti dodavatelského řetězce návrh zákona přispěje k posílení konkurenceschopnosti ČR, a to zejména posílením její reputace v rámci mezinárodního společenství. Přijetím a implementací Mechanismu prověřování bezpečnosti dodavatelského řetězce ČR značně vylepší svoji mezinárodní pozici z hlediska zabezpečení investičního prostředí prostřednictvím zvýšení úrovně bezpečnosti strategicky významné infrastruktury, čímž zvýší svoji atraktivitu pro investory. Mechanismus prověřování bezpečnosti dodavatelského řetězce mimo jiné umožní dosažení vyšší bezpečnosti dat, která, navzdory svému ekonomickému a strategickému významu, mnohdy nebývají pod plnou kontrolou subjektů, jimž patří. Namísto toho z povahy fungování kyberprostoru bývají data spravována či ukládána na infrastruktuře ovládané třetí stranou. Například pro společnosti vytvářející a vlastnící práva související s duševním vlastnictvím či know-how bude tedy přijetí navrhované úpravy znamenat lepší ochranu proti exfiltraci nebo kompromitaci těchto cenných aktiv. Je žádoucí zajistit, aby třetí strana nepředstavovala pro určitý subjekt, a tím pádem i pro stát, bezpečnostní riziko.

Zavedením takového mechanismu ČR rovněž splní některá z klíčových opatření zabezpečení 5G sítí podle Souboru opatření Evropské unie (dále jen „EU“) pro kybernetickou bezpečnost sítí 5G, a prokáže tak vůli navyšovat kromě bezpečnosti investic také bezpečnost své strategicky významné infrastruktury obecně; tímto krokem navíc půjde ČR v Evropě příkladem vzhledem k aplikaci doporučeného opatření i na jiné sektory strategicky významné infrastruktury, než je sektor elektronických komunikací. Naopak nelze vyloučit určitý negativní dopad na konkurenční postavení podnikatelských subjektů v ČR v podobě redukce nabídky některých dodávek v důsledku omezení rizikových dodavatelů (tedy zejména dodavatelů pocházejících ze zemí mimo vnitřní trh EU), a tedy i omezený negativní dopad na mezinárodní konkurenceschopnost.

Možné omezení okruhu subjektů na trhu může vést k nárůstu cen dodávaných technologií, a tedy i ke zvýšeným nákladům na straně regulovaných subjektů. Vzhledem k možnému snížení počtu dodavatelů technologií může dojít k dočasnému poklesu vzájemného konkurenčního tlaku, a tím pádem i ke snížení motivace k vytváření inovací.[2] Bude však zvýšena celková úroveň bezpečnosti služeb a produktů, čímž dojde ke snížení investičních rizik spojených s dodavatelským řetězcem pro potenciální investory, obzvláště ze zemí, které bezpečnost dodavatelského řetězce již právně regulují. Stejně tak povede zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce k větší důvěře spotřebitelů a koncových uživatelů v procesy, produkty a služby subjektů, které jsou s kritickou infrastrukturou spojené. V konečném důsledku bude mezinárodní konkurenceschopnost ČR ve srovnání se zeměmi bez adekvátní právní úpravy posílena.

Ekonomika ČR závisí na vývozu dodávek zboží do okolních zemí, a to zejména do Německa (kam směřuje přes 30 % vývozu), Slovenska, Polska a Rakouska (podíl na celkovém exportu přes 50 %).[3] Všechny zmíněné státy již do různé míry dodavatelský řetězec kritické infrastruktury nebo jejích sektorů regulují nebo regulaci připravují.[4]

Absence regulace bezpečnosti dodavatelského řetězce by tak v budoucnu mohla vést ke zhoršení pozice podnikatelských subjektů působících v ČR, neboť by nemohly nabídnout stejnou míru bezpečnosti svého produktu či služby jako subjekty působící ve státech, které obdobnou regulaci přijaly. Nepřijetí předmětné právní úpravy by tedy mohlo vyvolat nucené

[2] Podobné obavy měli např. v Dánsku (viz FOLKETINGET. L 190 Forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur. Dostupné z: https://www.ft.dk/samling/20201/lovforslag/l190/20201_l190_som_fremsat.htm

[3] ČSÚ. Zahraniční obchod ČR se zbožím – roční údaje – 2021, tab. 2.3., 2022. Dostupné z: https://www.czso.cz/csu/czso/zahranicni-obchod-cr-se-zbozim-rocni-udaje-498eu1tklj

[4] DE – Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (2021), AT – Telekommunikationsgesetz (2021), SK – Zákon o kybernetickej bezpečnosti (2021), PL – chystaná novela: Ustawa krajowym systemie cyberbezpieczeństwa

odmítání dodávek českých společností zahraničními odběrateli kvůli bezpečnostním a strategickým hrozbám plynoucím z dodávek subdodavatelů. České společnosti by se tím de facto staly nespolehlivými dodavateli pro zahraniční obchodní partnery, kteří by byli v takovém případě nuceni svým národním legislativním systémem upřednostnit dodavatele ze zemí, které rizika dodavatelského řetězce legislativně ošetřují.

Obecně lze na mezinárodní úrovni spatřovat rostoucí tendence zavádět mechanismy bezpečnosti dodavatelského řetězce. Na úrovni EU se jedná například o závěry Rady EU ohledně bezpečnosti dodavatelského řetězce v oblasti ICT ze dne 17. 10. 2022[5]. Dalším příkladem může být sektorově zaměřený dokument „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures“[6] skupiny pro spolupráci podle Směrnice (EU) 2016/1148, která klade důraz na přijetí opatření zajišťujících bezpečnost dodavatelského řetězce v 5G sítích. Trend lze pozorovat i v legislativě evropských států, které postupně zavádějí nebo již zavedly právní nástroje k zajištění bezpečnosti dodavatelského řetězce alespoň v některých kritických odvětvích. Kromě výše zmíněných sousedních zemí se také jedná např. o Francii, Dánsko či Spojené království.

Z hlediska mezinárodní konkurenceschopnosti je vysoká úroveň kybernetické bezpečnosti a odolnosti, ať už obecně nebo ve vztahu k dodavatelskému řetězci, bezesporu přínosem. Příkladem toho je jeden ze závěrů, který zazněl na akci 12th Annual National Conference on Cyber Security, ze kterého vyplývá, že se jedná o významný faktor při rozhodování investorů.[7] Investoři se zajímají o to, jakým způsobem společnosti ke kybernetickým rizikům přistupují.[8] Podle globálního investorského průzkumu společnosti PricewaterhouseCoopers (PwC)[9] se investoři kybernetických hrozeb obávají více než geopolitické nestability nebo nadměrné regulace.

Z hlediska zásad pro tvorbu digitálně přívětivé legislativy je dodržena zásada mezinárodní interoperability – budování služeb propojitelných a využitelných v evropském prostoru. Informační systémy využívané pro agendy vyplývající ze směrnice NIS 2, resp. návrhu zákona, mohou mimo jiné sloužit pro agregaci a bezpečné sdílení informací s partnery na mezinárodní a EU úrovni.

Co se týče nárůstu počtu zaměstnanců u regulovaných subjektů vyplývajícího z navrhované úpravy, lze uvést následující. Je třeba si uvědomit, že musíme přistupovat k regulovaným subjektům rozdílně s ohledem na režim povinností, do kterého budou spadat.

Regulované subjekty spadající do režimu nižších povinností musí splňovat zcela minimální požadavky z pohledu kybernetické bezpečnosti. Osobou zodpovědnou za kybernetickou bezpečnost regulovaného subjektu se může stát kdokoli, kdo má pro poskytovatele regulované služby dostatečnou odbornou způsobilost v oblasti kybernetické bezpečnosti. Odbornou způsobilostí tak disponuje již při pověření, případně musí absolvovat odborné školení v oblasti kybernetické bezpečnosti. Lze předpokládat, že nejvážnějším problémem regulovaného subjektu bude nalezení vhodného zařazení takové osoby v rámci organizační struktury

[5] COUNCIL OF THE EUROPEAN UNION. Council conclusions on ICT supply chain security. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf, str. 2, odst. 3

[6] NIS COOPERATION GROUP. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. Dostupné z:https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf, str. 18

[7] FT. Strengthening cyber security can boost FDI, say experts. Dostupné z: https://www.ft.lk/front-page/Strengthening-cyber-security-can-boost-FDI-say-experts/44-687887

[8] DELOITTE. Governance in focus. Cyber risk reporting in the UK. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-gif-cyber-risk-reporting-uk-march-2018.pdf, str. 1

[9] PWC. 2018 Global Investor Survey. Anxious optimism in a complex world. Dostupné z: https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf, str. 11

regulovaného subjektu tak, aby byla schopná plnit efektivně svou roli. Vzhledem k faktické neexistenci vážnějších omezení se takovou osobou může stát prakticky jakýkoli zaměstnanec povinné osoby schopný absolvovat odborné školení v oblasti kybernetické bezpečnosti. Poskytovatel regulované služby v režimu nižších povinností může výkon této role vyřešit také pomocí outsourcingu, tj. pověřením externí osoby. Také lze předpokládat, že některé regulované subjekty v režimu nižších povinností budou takové osoby sdílet. Malé množství reálných povinností a jejich možné celkové rozvrstvení v čase pak pro regulovaný subjekt znamená, že s vysokou pravděpodobností nebude muset vynakládat další prostředky na nové pracovníky, případně že půjde o marginální náklady na externího pracovníka, jehož pracovní náplň bude v případě režimu nižších povinností splnitelná v rámci dnů, maximálně týdnů kalendářního roku.

V režimu vyšších povinností, na rozdíl od režimu nižších povinností, jsou požadavky komplexnější a bezpečnostní opatření širší. Tím pádem je nutné, aby na efektivním prosazování kybernetické bezpečnosti spolupracoval větší počet osob. To nevyhnutelně vede k určitému nárůstu nákladů spojených s plněním těchto rolí. Přesto je důležité zdůraznit dvě klíčové skutečnosti.

Za prvé je důležité upozornit, že režim vyšších povinností se ve značné míře dotkne subjektů, které již podléhají stávající regulaci kybernetické bezpečnosti. Tento režim do regulace zahrne i subjekty, které sice dosud regulovány nebyly, ale lze u nich díky povaze jejich činnosti předpokládat, že se kybernetickou bezpečností své organizace zabývaly. Stávající právní úprava již nyní vyžaduje, aby regulované subjekty měly ve svých organizacích jasně definované bezpečnostní role (§ 7 vyhlášky o kybernetické bezpečnosti), a nová právní úprava nepřináší pro tyto subjekty zásadní změny. Nečekejme tedy výrazné zvýšení počtu potřebných zaměstnanců, protože tyto role musí být obsazeny kvalifikovanými osobami již nyní. Pro nově regulované subjekty to bude znamenat zejména přizpůsobení své organizační struktury tak, aby vyhověly novým požadavkům na kybernetickou bezpečnost z hlediska personálního zajištění.

Rovněž je zde na místě zdůraznit, že se jedná o role, nikoli o pracovní pozice jako takové. Je tedy možné jednotlivými rolemi pověřit osoby, které mají v rámci regulovaných subjektů na starosti i plnění jiných úkolů než jen těch týkajících se kybernetické bezpečnosti. Takovým přizpůsobením a jmenováním do některé z konkrétních rolí může povinná osoba eliminovat nutnost dalšího navyšování počtu zaměstnanců.

K výše zmíněnému dojde především díky přijetí návrhu zákona, nicméně návrh změnového zákona svým obsahem ke stanovenému cíli v celkovém důsledku napomáhá.

Z hlediska zásad pro tvorbu digitálně přívětivé legislativy je dodržena zásada mezinárodní interoperability – budování služeb propojitelných a využitelných v evropském prostoru. Informační systémy využívané pro agendy vyplývající ze směrnice NIS 2, resp. návrhu ZKB, mohou mimo jiné sloužit pro agregaci a bezpečné sdílení informací s partnery na mezinárodní úrovni a na úrovni Evropské unie.

3.3 Dopady na podnikatelské prostředí: Ano

Z důvodu rozsahu transponované směrnice dojde k přinejmenším patnáctinásobnému nárůstu regulovaných subjektů, což přinese značné ekonomické a finanční dopady na podnikatelské prostředí v ČR. Naprostá většina z nově regulovaných subjektů bude ze soukromého sektoru.

V případě ekonomických a finančních dopadů lze stejným způsobem odkázat na informace uvedené výše u dopadů na státní rozpočet a veřejné rozpočty. Nevýhodou otázky analýzy finančních dopadů na regulované subjekty je skutečnost, že distribuce nákladů na kybernetickou bezpečnost není plošná a existuje zde naprostá informační asymetrie ve směru od subjektů samotných k regulačnímu orgánu (tj. jen regulovaná organizace samotná

by měla být schopná identifikovat její vlastní náklady na zavedení a udržování přiměřené úrovně kybernetické bezpečnosti).

Výši finančních dopadů není možné předem stanovit a veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídající hodnotou.

Distribuce nákladů na kybernetickou bezpečnost není plošná z důvodu velkého počtu neznámých a proměnlivých indikátorů:

- aktuální stav zabezpečení každé jedné organizace,
- různý cílový stav každé organizace související s významností její činnosti a potřebou zajistit její fungování,
- široká variabilita rozsahu opatření na zajištění kybernetické bezpečnosti, která může být naprosto odlišná u jednotlivých organizací,
- identifikace toho, co je nákladem na zajištění kybernetické bezpečnosti a co je nákladem na běžný provoz ICT u daného subjektu (tyto množiny se velmi prolínají),
- soulad se zněním zákona o kybernetické bezpečnosti,
- neznámý přesný počet výsledných regulovaných subjektů,
- proměnlivost nákladů v čase související jak s makroekonomickými otázkami, tak s vývojem technologií a mnoho dalších indikátorů.

Tyto indikátory jsou bohužel spjaty se systémem zajištění kybernetické bezpečnosti, ať už podle zákona o kybernetické bezpečnosti, tak i z obecně přijímaných norem upravujících kybernetickou bezpečnost.

Stejně jako ve výše uvedeném případě lze i zde uvést, že se použije hrubě orientační výpočet nákladů zohledněný v rámci RIA k návrhu zákona, který vychází z výpočtů nákladů provedených podle:

- návrhu novelizace zákona o kybernetické bezpečnosti (2017),
- návrhu novelizace vyhlášky o významných informačních systémech (2019),
- Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2021),
- Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2022),

čímž došlo k orientačnímu výpočtu nákladů na zavedení a následné provádění především bezpečnostních opatření ve formě velmi hrubých odhadů, pohybujících se přibližně mezi 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému. Změny v přístupu k regulaci zavedené směrnicí, výše uvedené proměnné (především různý stav již současného zabezpečení u regulovaných organizací), rozdělení povinností uložených těmto subjektům, stejně tak jako agregace řady bezpečnostních opatření u více systémů v rámci organizace pak mohou tyto hodnoty ovlivnit. Podstatnou proměnnou tak bude především to, jaký je daný počet jednotlivých systémů u každé konkrétní organizace, a takový násobek výše uvedené částky bude potřeba u daných organizací zohlednit.

Návrh zákona o kybernetické bezpečnosti pracuje s pojmy mikropodnik a malý a střední podnik. Tyto definice jsou obsaženy v doporučení Komise 2003/361/ES. Podnikem se rozumí každý subjekt vykonávající hospodářskou činnost, včetně osob samostatně výdělečně činných (dále jen „OSVČ“). Regulace ovlivní tyto podniky dvěma způsoby: přímým dopadem, kdy část

mikropodniků, malých a středních podniků se stane poskytovatelem regulovaných služeb a bude muset plnit povinnosti podle zákona, a nepřímým dopadem, kdy obchodní partneři mohou požadovat zavedení bezpečnostních opatření do smluv.

V rámci dané skupiny se jedná zejména o střední podniky, zatímco počet mikropodniků a malých podniků, které se stanou povinnou osobou, by měl být minimální. Návrh zákona počítá se dvěma režimy poskytovatelů regulované služby – režim nižších a vyšších povinností. Od zařazení do těchto režimů se odvíjí množství a náročnost stanovených povinností. Mikropodniky, malé podniky a OSVČ budou většinou spadat do režimu nižších povinností, kde budou zavádět základní bezpečnostní opatření, což bude představovat hlavně administrativní zátěž. Pravděpodobně již některá opatření aplikují, takže náklady na novou regulaci nemusí být významné.

Druhým způsobem, kterým regulace ovlivní mikropodniky, malé a střední podniky, je nepřímý dopad. Podniky, které se nestanou povinnou osobou podle zákona, mohou přesto pocítit dopady regulace, pokud jejich obchodní partneři budou požadovat zavedení určitých bezpečnostních opatření do smluvních vztahů. To se týká například řízení dodavatelů, což je samostatné bezpečnostní opatření, které musí poskytovatelé regulovaných služeb v režimu vyšších povinností zavést a provádět.

Podle současných odhadů se navrhovaná úprava přímo dotkne přibližně 6000 subjektů, z čehož asi 5000 bude regulováno v režimu nižších povinností. Většina těchto subjektů budou střední podniky. Mikropodniky, malé podniky a OSVČ většinou do působnosti regulace spadat nebudou, s výjimkou subjektů poskytujících služby v odvětví digitální infrastruktury a služeb. V takovém případě se bude jednat primárně o poskytovatele regulovaných služeb v režimu nižších povinností. U některých služeb se pak mohou tyto podniky stát třeba i poskytovatelem regulované služby v režimu vyšších povinností díky naplnění jiných podmínek významnosti poskytovatele, než je podmínka jeho velikosti. Ačkoliv u některých dalších regulovaných služeb nejsou mikropodniky, malé podniky a OSVČ explicitně vyloučeny, z povahy věci na ně zde regulace spíše nedopadne, jelikož tyto služby (příkladně subjekt poskytující službu stavění vlakových cest na celostátní úrovni nebo ústřední správce zásob podle zákona o nouzových zásobách ropy) jsou zajišťovány subjekty spadajícími mimo tuto množinu.

Finanční zatížení poskytovatelů v režimu nižších povinností nebude zásadní, jelikož budou zavádět velmi základní povinnosti. Většina subjektů zvládne plnit povinnosti se stávajícími zaměstnanci přiřazením role nebo plnění této povinnosti zajistí externími subjekty.

Vedle negativních dopadů na podnikatelské prostředí, které mohou být vyvolány zvýšením nákladů daných společností, lze sekundárně očekávat posílení podnikatelského prostředí tím, že zvýšení zabezpečení přispěje k budování důvěry spotřebitelů a obchodních partnerů, případně i zahraničních investorů, které může přilákat právě vysoká míra bezpečnosti českého ICT prostředí.

Zároveň plnění povinností vyplývajících z navrhovaného zákona slouží jako prevence kyberbezpečnostních incidentů, které mají oproti zavedení daných bezpečnostních opatření násobně vyšší administrativní, ekonomické i reputační náklady, případně pomáhají díky požadavku na zajištění kontinuity a zvládání incidentů tyto negativní dopady minimalizovat.

Návrh zákona zvýší úroveň bezpečnosti spolupráce mezi regulovanými subjekty z podnikatelského prostředí a státem.

Co se týče zavedení mechanismu bezpečnosti dodavatelského řetězce, platí, že za pozitivní dopad na podnikatelské prostředí lze považovat také to, že díky omezení dodávek technologií rizikových dodavatelů pro výstavbu a provoz významné strategické infrastruktury zvýší mechanismus prověřování bezpečnosti dodavatelského řetězce pravděpodobnost řádného

poskytování regulovaných služeb prostřednictvím strategicky významné infrastruktury napříč jednotlivými sektory, jako jsou například služby elektronických komunikací či služby výroby a distribuce elektřiny, které návazně využívají jak spotřebitelé, tak podnikatelé.

Za negativní dopady zavedení uvedeného mechanismu na podnikatelské prostředí lze považovat zvýšení nákladů pro poskytovatele strategicky významné služby vyplývající z povinnosti hlásit dodavatele a reagovat na vydaná omezení, omezení nabídky a konkurenčního prostředí na relevantním trhu strategicky významné infrastruktury a reputační dopady na pověst dodavatelů, vůči nimž by případně bylo uplatňováno omezení. Ekonomický dopad na podnikatelské prostředí bude částečně mitigován nastavováním lhůty pro omezení či vyloučení bezpečnostně významné dodávky tak, aby v ideálním případě respektovala životní cyklus technologií. Tento princip je v návrhu zákona zapracován podle délky daňového odepisování zpracovaného v právním předpisu upravujícím zdanění příjmů[10], kdy je Úřad povinen vzít tyto doby odepisování v potaz při vydávání opatření obecné povahy.

Administrativní zátěž navrhovaného řešení by měla být pro podnikatelské subjekty minimální, jelikož všechny nově zaváděné procesy navazují na již existující administrativní povinnosti těchto subjektů, či jsou spojeny s jinými administrativními povinnostmi subjektů regulovaných v oblasti kybernetické bezpečnosti. Administrativní zátěž způsobená výhradně navrhovaným řešením by měla být za těchto předpokladů zanedbatelná, spočívající především v nově zavedené povinnosti nahlašovat Úřadu dodavatele specificky vymezených aktiv.

Z hlediska zásad pro tvorbu digitálně přívětivé legislativy je respektována technologická neutralita jakožto jedna ze stěžejních zásad zákona o kybernetické bezpečnosti i návrhu zákona. Návrh zákona tak zachovává volný trh a rovnou hospodářskou soutěž, je totiž na rozhodnutí samotných regulovaných subjektů, jaká konkrétní technická řešení, služby a produkty zvolí pro zajištění kybernetické bezpečnosti v rámci organizace. Rozšíření působnosti návrhu zákona popisované výše má potenciál nepřímo podpořit inovace v oblasti ICT, resp. konkrétně kybernetické bezpečnosti, jelikož se zvětšuje množina subjektů majících potenciálně zájem o inovativní řešení z této oblasti.

Z důvodu navrhované změny ZoISVS dochází stejně jako v případě dopadů na státní rozpočet a ostatní veřejné rozpočty a územní dopady na územní samosprávné celky pouze k minimálním dopadům.

Podobně dochází k minimálním dopadům na podnikatelské prostředí v případě navrhované změny ZoPZI. Návrh změny ZoPZI následuje analogicky původní rozvržení tzv. cílových osob, v případě dopadů na podnikatelské prostředí je tedy možné odkázat na řešení této otázky v důvodové zprávě k ZoPZI.

3.4 Územní dopady na územní samosprávné celky: Ano

Podle zákona o kybernetické bezpečnosti jsou vyšší územní samosprávné celky povinnými osobami zavádějícími bezpečnostní opatření k ochraně svých regulovaných systémů. V souladu s návrhem zákona zůstává tato regulace zachována, nicméně dojde k jejímu rozšíření na celou organizaci, nikoli pouze na jednotlivé konkrétní systémy. Vedle toho i v případě územních samosprávných celků platí, že mohou být touto novou regulací zasaženy tehdy, pokud naplňují definice a určující kritéria stanovená pro regulované subjekty. V takovém případě by musely i tyto ostatní územní samosprávné celky plnit povinnosti plynoucí z návrhu zákona.

[10] Zákon č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů.

Rozšíření oproti zákonu o kybernetické bezpečnosti však přináší návrh zákona v nové regulaci části základních územně samosprávných celků, tedy obcí, resp. obcí s rozšířenou působností, kterých je v ČR aktuálně 205. Obce s rozšířenou působností dlouhodobě pod regulací zákona o kybernetické bezpečnosti nespadaly z důvodu výslovné výjimky, nicméně současné trendy a zkušenosti z ČR a zahraničí ukazují, že nelze jejich postavení podceňovat – jak ukazují neblahé zkušenosti některých obcí s kybernetickými bezpečnostními incidenty, které se ani jim nevyhýbají. V případě obcí s rozšířenou působností počítá návrh zákona s jejich zařazením zpravidla do kategorie spojené s nižšími požadavky na zajištění kybernetické bezpečnosti, nicméně lze také očekávat jejich nižší vyspělost v kybernetické bezpečnosti obecně. Z toho se dá odhadnout, že náklady na jejich zabezpečení budou v zásadě srovnatelné s výpočtem uvedeným výše.

Z hlediska zásad pro tvorbu digitálně přívětivé legislativy návrh zákona každopádně směřuje ke zvýšení kybernetické bezpečnosti územních samosprávných celků, na něž příslušná regulace dopadá. Zavedením příslušných bezpečnostních opatření bude navíc posílena ochrana osobních údajů umožňující poskytování kvalitních a důvěryhodných služeb ze strany těchto územně samosprávných celků občanům.

V rámci návrhu změnového zákona nebude na územní samosprávné celky přenášena žádná další působnost. Finanční dopady na územní samosprávné celky mohou být způsobeny požadavkem na změnu ZoISVS, jelikož se ukládají povinnosti přiměřeně zavádět bezpečnostní opatření vyplývající z návrhu zákona správcům informačních systémů veřejné správy, kterými jsou obce s pověřeným obecním úřadem či obce I. stupně. Tyto dopady by nicméně byly stanoveny prostřednictvím samostatné legislativy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy), pokud by nebyly stanoveny změnou ZoISVS. Nebudou nicméně tak zásadní, jedná se totiž toliko o přiměřené zavádění požadavků na nižší režim.

3.5 Sociální dopady: Ne

3.6. Dopady na rodiny: Ne

3.7 Dopady na spotřebitele: Ano

Návrh zákona nepředpokládá žádné přímé dopady na spotřebitele, neboť nedochází k právní úpravě jejich postavení ani práv nebo povinností. Negativním nepřímým dopadem, který lze očekávat v případě jakékoli veřejnoprávní regulace, je tlak regulovaných orgánů a osob na promítání zavádění bezpečnostní opatření do ceny služeb pro jednotlivé spotřebitele. Je však nutno podotknout, že směrnice NIS 2 cílí na ochranu a podporu fungování vnitřního trhu EU. Povinnost podnikatelských a nepodnikatelských subjektů zavádět bezpečnostní opatření, a tím co nejvíce předcházet výskytu kybernetických bezpečnostních incidentů, na druhé straně může mít nejen pozitivní dopad na jeho fungování, ale přeneseně také na spotřebitele a odběratele jejich služeb, protože poskytování těchto služeb bude méně náchylné na narušení způsobené kybernetickým bezpečnostním incidentem, a zároveň může dojít ke zvýšení důvěryhodnosti a celkové odolnosti daného subjektu, což by mělo motivovat spotřebitele k využívání jeho služeb.

Přijetím mechanismu prověřování bezpečnosti dodavatelského řetězce dále dojde k navýšení úrovně bezpečnosti strategicky významné infrastruktury, což bude mít pozitivní efekt na zajištění vysoké úrovně stability a bezpečnosti služeb poskytovaných spotřebitelům napříč strategicky významnými sektory.

Navrhované řešení zároveň počítá s mechanismy minimalizujícími negativní dopady na spotřebitele prostřednictvím omezení využitelnosti dodávek bezpečnostně rizikových

dodavatelů správcem infrastruktury tak, aby nedocházelo např. k omezení všech nabízených technologických produktů v daném sektoru či k tzv. proprietárnímu uzamčení (vendor lock-in) správce regulované infrastruktury závislého na jednom dodavateli. Navrhované řešení má za cíl rovněž přispět k budování zdravého tržního prostředí, které staví na spravedlivé hospodářské soutěži soutěžitelů, motivovaných soubojem o zákazníka, a nikoli např. omezením funkčnosti infrastruktury k dosažení geopolitických cílů státu, jež má na dodavatele vliv.

Z hlediska zásad pro tvorbu digitálně přívětivé legislativy a dopadů na spotřebitele respektuje návrh zákona zásady ochrany osobních údajů umožňující kvalitní služby, uživatelskou přívětivost, budování přednostně digitálních služeb i maximální opakovatelnost a znovupoužitelnost údajů a služeb. Nicméně návrh zákona, jak bylo řečeno výše, na spotřebitele přímo nedopadá, a Úřadem poskytované digitální služby tak nebudou pro běžného spotřebitele (fyzickou osobu) úplně relevantní.

Návrh změnového zákona nepředpokládá žádné přímé dopady na spotřebitele. Povinnost podnikatelských a nepodnikatelských subjektů zavádět bezpečnostní opatření, a tím co nejvíce předcházet výskytu kybernetických bezpečnostních incidentů, může mít nejen pozitivní dopad na jeho fungování, ale přeneseně také na spotřebitele a odběratele jejich služeb, protože poskytování těchto služeb bude méně náchylné k narušení způsobenému kybernetickým bezpečnostním incidentem. Zároveň může dojít ke zvýšení důvěryhodnosti a celkové odolnosti daného subjektu, což by mělo motivovat spotřebitele k využívání jeho služeb.

3.8 Dopady na životní prostředí: Ne

3.9 Dopady ve vztahu k zákazu diskriminace a ve vztahu k rovnosti žen a mužů: Ne

3.10 Dopady na výkon státní statistické služby: Ne

3.11 Korupční rizika: Ano

Rozsah povinností a rozšíření působnosti zákona o kybernetické bezpečnosti jsou přiměřené, zejména s ohledem na rizika a dopady, které by vznikly netransponováním směrnice a neodstraněním současných legislativních nedostatků.

Rozsah úkolů orgánů státní správy zůstává z velké části nezměněn, významné je však rozšíření působnosti na nově regulované subjekty. S rozšířením působnosti je však pro praktickou realizaci výkonu činností nutno využít osvědčené postupy, stejně tak jako přistoupit k doposud neaplikovaným řešením.

V prvé řadě klade návrh zákona větší důraz na mechanismus samoidentifikace povinného subjektu, který byl doposud využíván jen u tzv. významných informačních systémů. Tento mechanismus je úzce spojen se zjednodušením tzv. kritérií pro identifikaci a ve výsledku dělá proces vyhodnocení naplnění kritérií poskytovatele regulované služby jednodušší a objektivnější, čímž dochází ke snižování potenciálního korupčního rizika spojeného s vyhodnocováním naplnění těchto kritérií, především dodatečně v případě přezkumu Úřadem. Návrh zákona dále využívá také tzv. kritéria pro určení poskytovatele regulované služby, nicméně i v jejich případě se jedná o zákonem stanovená kritéria. Ne jinak je tomu také v případě stanovení tzv. strategicky významné služby, tedy množiny v rámci poskytovatelů regulované služby ve vyšším režimu, pro které jsou stanovena také zákonná kritéria. Proces komunikace mezi Úřadem a poskytovateli regulované služby by měl navíc probíhat primárně prostřednictvím tzv. Portálu Úřadu, tj. informačního systému, který

veškerou komunikaci a obsah podání eviduje a uchovává. Také tento proces by měl vést ke snížení možného korupčního jednání.

V případě povinností uložených poskytovatelům regulované služby se jedná o povinnosti definované návrhem zákona a vycházející již z aktuální právní úpravy. V rámci těchto povinností nebyla identifikována nová korupční rizika. Naopak návrh zákona některé povinnosti blíže rozpracovává (např. v případě hlášení a řešení kybernetického bezpečnostního incidentu), čímž dochází ke zpřesnění povinností jak na straně poskytovatele regulované služby, tak na straně Úřadu, a snižuje se prostor pro potenciální korupční jednání.

V rámci nově stanovených povinností nevycházejících z dosavadní právní úpravy je vhodné uvést povinnost zajištění regulované služby z území ČR, což však ze své podstaty je pouze zpřesnění jednoho z bezpečnostních opatření - tzv. zajištění kontinuity činností, a tedy ani v tomto případě nedošlo k identifikaci korupčních rizik.

Zavedením mechanismu bezpečnosti dodavatelského řetězce může návrh zákona mít potenciálně zásadní dopady na poptávku po zboží a službách některých dodavatelů do strategicky významné infrastruktury ČR. Tato skutečnost může vyvolat korupční tlak na změnu způsobu prověřování kritérií nebo úpravu celkového hodnocení rizikovosti dodavatele. Obdobně mohou i někteří správci regulované infrastruktury usilovat o to, aby nebyl konkrétní poskytovatel v důsledku posouzení důvěryhodnosti omezen, jelikož by to pro ně znamenalo zvýšené náklady, či naopak mohou usilovat o omezení konkrétního dodavatele za účelem zhoršení postavení svého konkurenta, který takového dodavatele využívá ve své infrastruktuře.

Jelikož je tedy rozhodnutí o omezení dodavatele implicitně zatíženo korupčním rizikem, jako vhodné řešení se jeví právě existence veřejně stanovených a transparentních kritérií a rozhodování o možném významném ohrožení bezpečnosti ČR nebo vnitřního pořádku na základě vyhodnocení těchto kritérií. Příslušný ústřední správní orgán rozhodne o případném omezení dodavatele na základě vlastního šetření i sběru informací od ostatních zapojených státních orgánů. Případné omezení dodavatele je následně možné přezkoumat v přezkumném řízení nebo v soudním řízení správním podle obecné úpravy správního řádu a soudního řádu správního. Obdobný proces již v českém právním řádu existuje, jedná se např. o proces prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy, který je zaveden do české právní úpravy zákonem o informačních systémech veřejné správy. Dalším kontrolním prvkem sloužícím k omezení korupčního rizika je dohled, který nad Úřadem, potažmo procesem prověřování dodavatelského řetězce, provádí Bezpečnostní rada státu.

V neposlední době je vhodné uvést navrhovanou novou právní úpravu stavu kybernetického nebezpečí. Navrhovaná právní úprava umožňuje řediteli Úřadu uložit za výjimečné situace opatření fyzickým a právnickým osobám. S ohledem na možná korupční rizika je však proces jejich vydání stanoven stejným způsobem jako je tomu již nyní v případě krizových stavů, a navíc rozhodování ředitele Úřadu je podrobeno dohledu kontrolního orgánu Poslanecké sněmovny a ředitel Úřadu je odpovědný vládě ČR.

Z hlediska zásad pro tvorbu digitálně přívětivé legislativy lze pouze zmínit, že zásada technologické neutrality je jednou ze stěžejních zásad celého návrhu zákona, což znamená, že návrh zákona nezvyšuje korupční rizika v tom smyslu, že by preferoval výrobky či služby určitých výrobců či poskytovatelů. Naopak je maximálně respektována volnost trhu, rovná hospodářská soutěž a nedochází k vytváření podmínek pro nedovolenou veřejnou podporu.

3.12 Dopady na bezpečnost nebo obranu státu: Ano

Návrh zákona má pozitivní dopady na bezpečnost a obranu státu, zejména přispěje k dalšímu posílení zabezpečení klíčových služeb v ČR, čímž dojde k posílení zabezpečení českého kyberprostoru jako celku, a rovněž ke snížení míry rizika realizace incidentů, které by mohly ohrozit bezpečnost ČR jako celku.

Na národní bezpečnost a obranu bude mít pozitivní vliv také zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, neboť odolná strategicky významná infrastruktura bez rizikových dodavatelů je klíčovým předpokladem pro zajištění národní bezpečnosti a obrany, s nímž pracuje jak aktuálně platná Bezpečnostní strategie ČR, tak i Národní strategie pro čelení hybridnímu působení a Národní strategie kybernetické bezpečnosti ČR. Vazbu na odolnou a bezpečnou infrastrukturu jako integrální součást národní bezpečnosti rovněž zdůrazňují strategické dokumenty NATO. Zavedením mechanismu prověřování bezpečnosti dodavatelského řetězce se navíc podstatně sníží riziko vzniku závislosti strategické infrastruktury na jednotlivých rizikových dodavatelích.

Z hlediska zásad pro tvorbu digitálně přívětivé legislativy lze pouze zopakovat výše zmíněné, tedy že návrh zákona zásadním způsobem přispívá k celkovému zvýšení úrovně kybernetické bezpečnosti u poskytovatelů regulovaných služeb, z nichž někteří mohou být strategicky významní pro bezpečnost nebo obranu státu.

Návrh změnového zákona má pozitivní dopady na bezpečnost a obranu státu, zejména přispěje k dalšímu posílení zabezpečení klíčových služeb v ČR, čímž dojde k posílení zabezpečení českého kyberprostoru jako celku a rovněž ke snížení míry rizika realizace incidentů, které by mohly ohrozit bezpečnost ČR jako celku.

1. Důvod předložení a cíle

1.1.1. Návrh zákona

Dne 27. prosince 2022 byla přijata 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 (dále jen „směrnice“ nebo „směrnice NIS 2“). Podle směrnice musí každý členský stát EU transponovat obsah této směrnice do svého právního řádu do 21 měsíců od nabytí platnosti této směrnice.

V Plánu legislativních prací vlády na rok 2023 je pro Úřad zařazen legislativní úkol zpracovat a předložit vládě návrh zákona, zpracovaný na základě Bezpečnostní radou státu zvoleného přístupu A – Prověřování dodavatelů podle aktuální bezpečnostní situace, uvedeného v materiálu „Bezpečnost dodavatelských řetězců strategické infrastruktury státu“, č. j. 28261/2022-UVCR“ (dále také jako „mechanismus prověřování bezpečnosti dodavatelského řetězce“).

Návrh zákona reflektuje také připomínky z praktické aplikace zákona o kybernetické bezpečnosti.

Cílem návrhu zákona je na základě požadavků všech tří výše uvedených skutečností vytvořit ucelený právní předpis reagující na tyto nové požadavky a prostřednictvím něj dosáhnout vysoké společné úrovně (kybernetické) bezpečnosti služeb v ČR, což v praxi znamená zvýšení bezpečnosti sítí a informačních systémů, na nichž je do značné míry postaveno fungování naší společnosti a hospodářství.

1.1.2. Návrh změnového zákona

Povinnosti upravené v návrhu zákona se vztahují mimo jiné i na podnikatele zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, kteří mají povinnost hlásit kybernetické bezpečnostní incidenty Úřadu a spolupracovat s ním při jejich řešení a předcházení jim. Tito podnikatelé jsou ve vztahu k zajišťování bezpečnosti a integrity uvedené sítě a k zajišťování bezpečnosti uvedené služby, vázáni také ZEK, v rámci něhož mají povinnost hlásit (obecné) bezpečnostní incidenty Českému telekomunikačnímu úřadu (dále také jen „ČTÚ“) a spolupracovat s ČTÚ při jejich řešení a předcházení jim. Vyvstává proto potřeba upravit vzájemný vztah návrhu zákona a ZEK, a to změnou posledně zmíněného právního předpisu. Obdobně je tomu také v případě provozovatelů poštovních služeb podle zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů.

Dále platí, že návrh zákona na rozdíl od ZKB stanovuje jedinou povinnou osobu (poskytovatele regulované služby) a nestanovuje orgánům veřejné moci povinnost zajistit dodržování bezpečnostních pravidel v souvislosti s využíváním služby cloud computingu, stejně tak ani povinnost zařadit poptávaný cloud computing do bezpečnostní úrovně před uzavřením smlouvy s poskytovatelem cloud computingu. Návrh zákona dále ruší vyhlášku č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, ve znění pozdějšího předpisu. Z těchto skutečností vyplývá nutnost upravit znění ZoISVS. Společně s touto změnou se nabízí možnost využít v návrhu zákona zakotvenou úroveň bezpečnostních opatření stanovených pro poskytovatele regulované služby v režimu nižších povinností tak, aby došlo ke sjednocenému stanovení standardu kybernetické bezpečnosti pro téměř celou veřejnou správu v ČR. Tento návrh má ambici dosáhnout nápravy doposud neutěšeného stavu, který byl popsán již v původní důvodové zprávě k ZKB, v níž je uvedeno že, *„[v] oblasti veřejné správy neexistuje jednotný způsob stanovení bezpečnostních standardů, které by minimalizovaly potencionální škody vzniklé z kybernetických útoků“*.

Výše uvedenou změnu, obsaženou v návrhu zákona, spočívající ve stanovení jediné povinné osoby, je nutné promítnout rovněž do znění ZoPZI, neboť také tento právní předpis obsahově vychází z vymezení více povinných osob ZKB.

V neposlední řadě platí, že ZoB, ve vztahu k bankám, ZPMS a AML ve vztahu k Finančnímu analytickému úřadu, daňový řád ve vztahu ke správci daně, ZCS ve vztahu k Celní správě ČR a ZoPZI ve vztahu k Ministerstvu průmyslu a obchodu vždy výslovně upravují situace, v nichž se poskytnutí informací uvedenými orgány nepovažuje za prolomení povinnosti mlčenlivosti, případně bankovního tajemství. S ohledem na skutečnost, že návrh zákona zavádí mj. mechanismus prověřování rizik spojených s dodavatelem, a za účelem zajištění jeho řádného fungování v § 28 stanoví, že některé subjekty jsou povinny poskytovat Úřadu informace, které získaly při své činnosti, případně poskytovat nezbytnou součinnost při zjišťování nezbytných informací potřebných pro činnost Úřadu v rámci mechanismu prověřování rizik spojených s dodavatelem. Z tohoto důvodu je nutné u výše zmíněných subjektů novelizovat uvedené předpisy tak, aby poskytnutí těchto informací, případně poskytnutí součinnosti neznamenalo porušení povinnosti mlčenlivosti, resp. bankovního tajemství.

1.2. Název

Návrh zákona o kybernetické bezpečnosti a návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

1.3. Definice problému

1.3.1. Návrh zákona

Výrazný nárůst používání informačních technologií v současném světě vede na jedné straně k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb (a tím celé společnosti). Závislost společnosti a jejího fungování na informačních technologiích rapidně narůstá, a to ve všech oblastech (nejedná se tedy pouze o služby informační společnosti, jako je internetový obchod, ale i o fungování informačních systémů, na jejichž správné funkci je závislá celá řada základních služeb jako například řízení dopravy, přenos energií, výkon veřejné moci apod.). Do kybernetického prostoru se však nepřesouvají jenom ekonomické aktivity. Vznikem sociálních, herních a zájmových sítí se z nejznámější části kybernetického prostoru, z internetu, stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat.

V ČR je problematika kybernetické bezpečnosti komplexně řešena již od roku 2015, kdy nabylo účinnosti první znění zákona o kybernetické bezpečnosti. Forma zvláštního zákona upravujícího otázku veřejnoprávní regulace kybernetické bezpečnosti byla zvolena z důvodu specifické věcné působnosti regulace. S ohledem na smysl a účel této regulace nebylo racionální kybernetickou bezpečnost podřadit pod jiný právní předpis. Povinnosti se v zákoně o kybernetické bezpečnosti vztahovaly k osobám soukromého práva i orgánům veřejné moci, přičemž jejich základní rozlišení bylo podle typu informačního a komunikačního systému, kterou příslušný subjekt spravuje či zajišťuje – jednalo se o poskytovatele služeb elektronických komunikací, subjekty zajišťující významné sítě, správce informačních a komunikačních systémů kritické informační infrastruktury a správce významných informačních systémů. Povinnosti, které byly adresátům normy uloženy, byly jak preventivního, tak reaktivního charakteru, přičemž ústředními povinnostmi bylo zavádět preventivní bezpečnostní opatření, hlásit kybernetické bezpečnostní incidenty a provádět opatření Úřadu. Zákon o kybernetické bezpečnosti dále upravoval specifické instituty, jakým je např. stav kybernetického nebezpečí, stejně jako upravoval postavení a pravomoci příslušných orgánů veřejné moci – v původním znění zákona především Národního bezpečnostního úřadu.

O dva roky později, v roce 2017, se zákon o kybernetické bezpečnosti dočkal hned dvou stěžejních novelizací. Ta první přinesla nový institut tzn. provozovatele systému, tou druhou byla komplexní novela transponující do zákona obsah unijní směrnice zabývající se kybernetickou bezpečností – 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 (tzv. směrnice NIS). Kromě celé řady doplňujících ustanovení, které tato komplexní novelizace do zákona přinesla, dala vzniknout dalším typům povinných osob – provozovateli základní služby, správci a provozovateli informačního systému základní služby a poskytovateli digitální služby. Tato novelizace také umožnila vznik Úřadu.

Přestože po komplexní novelizaci bylo pod zákonem o kybernetické bezpečnosti regulováno celkem 13 druhů povinných osob rozdělených v § 3 do osmi kategorií, povinnosti, které jim byly zákonem uloženy, vycházely z původního znění zákona. Prakticky bylo v ČR po komplexní novele regulováno přibližně 400 orgánů a osob ve čtyřech nejdůležitějších kategoriích – správce a provozovatel informačního systému kritické informační infrastruktury, správce a provozovatel komunikačního systému kritické informační infrastruktury, správce a provozovatel významného informačního systému a správce a provozovatel informačního systému základní služby.

Na konci roku 2020 představila Evropská komise návrh revize směrnice NIS, tzv. směrnici NIS 2. Tato směrnice přináší zásadní změny v dosavadním přístupu k veřejnoprávní regulaci kybernetické bezpečnost, především v otázce stanovení jejího rozsahu. Primárním způsobem stanovení, jestli organizace spadá pod regulaci směrnice, je současné naplnění dvou pravidel – organizace poskytuje alespoň jednu službu uvedenou v přílohách směrnice a zároveň je středním nebo velkým podnikem podle Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků. Už jen tato jediná změna znamená v kontextu ČR enormní nárůst regulovaných subjektů, přičemž odhady hovoří o minimálně 6 000 povinných orgánech a osobách. Vedle změny rozsahu upravuje směrnice také další podmínky pro bezpečnostní opatření a hlášení kybernetických bezpečnostních incidentů, zavádí zcela nové povinnosti a ruší a do svého obsahu přesouvá některá ustanovení jiných právních předpisů. Všechny tyto změny přináší pro znění zákona o kybernetické bezpečnosti zcela zásadní výzvy.

K zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce je nutno uvést, že bezpečnost a odolnost organizačních složek státu a dalších orgánů a osob, jež poskytují služby důležité pro chod státu, jsou předpokladem pro zajištění bezpečnosti ČR. Hrozby, které pro ČR plynou z prostředí, v němž se tyto subjekty nachází, jsou definovány v Bezpečnostní strategii ČR z roku 2023.[11] Jedná se zejména o hrozby spočívající v:

a) kybernetických útocích, nebo

b) ohrožení funkčnosti a bezpečnosti komunikačních informačních systémů, dodavatelských řetězců a kritické infrastruktury, včetně dodávek kritických surovin, potravin a energetických komodit.

Počet kybernetických útoků na infrastrukturu regulovanou zákonem o kybernetické bezpečnosti v posledních letech výrazně narůstá, což dlouhodobě dokládají i Zprávy o stavu kybernetické bezpečnosti ČR (dále jen „ZSKB“), naposledy ZSKB za rok 2021.[12] V té se uvádí,

[11] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. Bezpečnostní strategie České republiky. 2023. Dostupná zde: https://mocr.army.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_Ceske_republiky_2023.pdf

[12] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2021. Dostupná zde: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

že rok 2021 se vyznačoval nárůstem škodlivých kybernetických aktivit, ke kterým docházelo plošně na celém území ČR.

Meziročně také vzrostl počet kybernetických incidentů evidovaných Úřadem. Například v roce 2021 zaznamenal Úřad celkem 157 kybernetických bezpečnostních incidentů oproti 99 incidentům v roce 2020. V tomto ohledu aktivity státem podporovaných aktérů v kybernetickém prostoru dlouhodobě patří mezi nejvážnější hrozby pro kybernetickou bezpečnost ČR.[13] Tito aktéři jsou zpravidla vysoce sofistikovaní a k dosažení svých cílů využívají širokou škálu taktik a technik, přičemž dochází k neustálému zdokonalování používaných nástrojů.

Podle Policie ČR došlo také k nárůstu kyberkriminálních aktivit. Podle Policie ČR se i v průběhu roku 2021 potvrzuje dlouhodobý trend postupného přesunu trestné činnosti do kyberprostoru. V roce 2021 se počet skutků spadajících do kategorie kybernetické kriminality a ostatní kriminality páchané v kyberprostoru meziročně zvýšil o 17,9 %.[14] Vyhodnocení Úřadu k roku 2022 vykazuje opětovný nárůst a statistky nasvědčují tomu, že se situace ani v budoucnosti nebude měnit.

Útoky státních aktérů na systémy kritické pro chod státu se stávají běžnou realitou, ovlivňující život a fungování mnoha obyvatel a institucí**.** Bezpečnost těchto systémů je ohrožena nejen kybernetickými útoky, ale i prostřednictvím dodavatelů a dodavatelských řetězců, spadajících do sféry vlivu aktérů, jejichž zájmy a mezinárodní působení jsou v konfliktu se zájmy ČR. Dodavatelé se tak mohou stát prostředkem k prosazování politických cílů**.**

Jelikož ČR v rámci plnění svých základních funkcí povětšinou spoléhá na infrastrukturu vlastněnou, dodávanou či spravovanou třetími osobami, vzniká státu na těchto dodavatelích závislost (dále také „strategická závislost“). Pokud vznikne závislost na rizikovém dodavateli, plynou z toho pro stát významná rizika. Možné dopady takových rizik ukázal např. vývoj související s Ruskou invazí na Ukrajinu, která byla zahájena 24. února 2022. Válka na Ukrajině měla a má kromě nezměrných lidských, humanitárních, bezpečnostních a geopolitických dopadů také značné dopady na evropskou ekonomiku, a to především a nejcitelněji v energetice. Razantní zvýšení cen energií, zejména plynu,[15] bylo způsobeno právě onou rizikovou závislostí, jež si ČR na dovozu plynu z Ruska vytvořila.[16]

Obdobná situace strategické závislosti státu na dodavatelích může nastat, a v mnoha sektorech již nastává, v oblasti ICT. V ICT je kromě již identifikovaných problémů strategické závislosti potřeba vyhodnocovat také rizika související s narušením důvěrnosti, integrity i dostupnosti dat a informací přenášených dodávanými technologiemi ze strany dodavatele.

Strategicky významná infrastruktura (viz část 1.4 Identifikace dotčených subjektů) je přitom na ICT značně závislá. S narůstající digitalizací a rozvojem této infrastruktury se rozšiřuje rozsah infrastruktury pro provádění potenciálních kybernetických útoků, a tím se i značně zvyšuje riziko kybernetických útoků. Společně se zvyšující se mírou přenosu

[13] Tamtéž.

[14] POLICIE ČR. Vývoj registrované kriminality v roce 2021. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx#:~:text=V%20roce%202021%20bylo%20na,tedy%20vzrostla%20meziro%C4%8Dn%C4%9B%20o%201%20%25.

[15] ČESKÁ NÁRODNÍ BANKA. Vývoj na evropském trhu se zemním plynem. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Vyvoj-na-evropskem-trhu-se-zemnim-plynem/

[16] Eurostat uvádí 75–100% závislost ČR na ruském plynu pro první pololetí roku 2021. (Viz EUROSTAT. File: Share of Russia in national extra EU imports of each Member State, first semester 2021.png. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Share_of_Russia_in_national_extra_EU_imports_of_each_Member_State,_first_semester_2021.png)

odpovědnosti za zajištění důvěrnosti, integrity a dostupnosti informací přenášených informačními systémy (dále jen „IS“) na dodavatele ICT a zvyšující se mírou složitosti jednotlivých prvků technologických systémů závislost strategicky významné infrastruktury na těchto dodavatelích dále narůstá.

Dodavatelé mají v ICT infrastruktuře výsadní postavení. Hardwarová a softwarová řešení informačních a komunikačních technologií jsou již natolik komplexní a v infrastrukturách poskytovatelů strategicky významné služby tak četně zastoupená, že je nelze technicky komplexně včas a efektivně prověřovat.

I s ohledem na časté aktualizace je technické testování ICT produktů ve velkém měřítku vysoce neefektivní. Problematika bezpečnostních záplat taktéž ztěžuje správcům infrastruktury technicky ověřit implementovaná softwarová řešení od svých dodavatelů, jelikož v případě odhalení (i zcela neúmyslných) slabin je potřeba co nejrychleji vydat softwarové aktualizace, než jich využijí útočníci (tzv. zranitelnosti nultého dne[17]). Takové aktualizace proto nemohou být podrobeny důkladné analýze, a nelze tak vyloučit riziko, že budou obsahovat například zadní vrátka nebo jiný škodlivý kód. Klíčovým faktorem zabezpečení ICT je proto důvěra v dodavatele, že nezneužije své výsadní postavení ve prospěch svůj, státu, který má na dodavatele vliv, či jiného aktéra.

Dodavatele ze zemí majících např. nestandardní legislativní prostředí, umožňující ingerenci státních aktérů do produktů, služeb či procesů dodavatelů, jejichž zájmy jsou v konfliktu se zájmy ČR a jejích spojenců, lze považovat za rizikové. Ačkoli výrobci či dodavatelé ICT produktů a služeb (dále jen „dodavatelé ICT“) mají s ohledem na generování zisku zájem o prodej kvalitních a bezpečných produktů, ne vždy se musí jednat o jejich jediný zájem.

Dodavatelé ICT mají sídla v různých zemích a podléhají rozličným právním řádům, mocenským strukturám a jiným neobchodním vlivům. Zvýšené riziko představují primárně dodavatelé ICT z autoritářských států, které mají silný vliv na své domácí společnosti, a neváhají jej využít pro prosazování svých geopolitických cílů, jež mohou být v rozporu se zájmy ČR či jejích spojenců. Dodavatel ICT může být natolik propojený a ovlivněný státním a politickým aparátem své domovské země, že bude nezřídka činit i ekonomicky kontraproduktivní rozhodnutí v souladu se zájmy režimu, který mu potenciální reputační škodu může kompenzovat, případně jej za jednání v rozporu se svými zájmy potrestat. Navíc, vzhledem k obtížnému odhalení, a ještě obtížnější přičitatelnosti kybernetických útoků,[18] mohou tyto aktivity představovat pro výrobce přijatelné riziko, které mu zajistí výhodné postavení v domovském státě a výrazněji neohrozí jeho zisk.

V řadě států mohou být společnosti také nuceny ke spolupráci se zpravodajskými službami státu prostřednictvím legislativy, jež na ně dopadá. V Čínské lidové republice (dále jen „ČLR“) ukládá legislativa povinnost jednotlivcům i společnostem spolupracovat s čínskými státními autoritami. Jedná se např. o mechanismus, který je začleněný v zákoně o společnostech z roku 2013, jež ukládá všem společnostem povinnost ustanovit uvnitř svých struktur stranickou organizaci Komunistické strany ČLR (dále jen „KS ČLR“), pokud ve společnosti pracují nejméně tři členové Strany. V praxi to znamená přímý dosah této strany na dění v jakékoli významné společnosti. KS ČLR vykonává skrze stranické organizace přímou kontrolu nad společnostmi a zajišťuje, že beze zbytku plní, co se od nich očekává, včetně požadavků

[17] Podle Zprávy o stavu kybernetické bezpečnosti za rok 2021 se jedná o typ zranitelnosti, který bývá často využíván např. státem podporovanými skupinami.

[18] Atribuce podle vyjádření Úřad představuje proces, během něhož dochází k určení pravého zdroje útoku a samotného útočníka (Viz Úřad. Bezpečnější zdravotnictví i řešení rizikových dodavatelů – Vláda schválila Akční plán ke strategii kybernetické bezpečnosti. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1735-bezpecnejsi-zdravotnictvi-i-reseni-rizikovych-dodavatelu-vlada-schvalila-akcni-plan-ke-strategii-kyberneticke-bezpecnosti/)

v oblasti státní bezpečnosti.[19] Zákon o kybernetické bezpečnosti ČLR z roku 2017 pak obsahuje řadu ustanovení definujících povinnost spolupráce se státními orgány. Článek 28 tohoto zákona určuje povinnost provozovatelů sítí poskytnout technickou podporu a spolupráci orgánům veřejné bezpečnosti a orgánům státní bezpečnosti.[20] Zákon o státní zpravodajské činnosti ČLR z téhož roku zdůrazňuje, že relevantní státní instituce jsou oprávněny vyžadovat spolupráci po jednotlivcích a organizacích: „*Národní zpravodajské služby mohou v souladu se souvisejícími státními předpisy požádat příslušné orgány, organizace a občany o poskytnutí potřebné podpory, součinnosti a spolupráce*.“[21]

Taktéž Ruská federace (dále jen „RF“) přijala během poslední dekády několik zákonů s významným dopadem v oblasti kybernetické a informační bezpečnosti, které zásadním způsobem zasahují do fungování soukromých společností.[22] Zákon o Federální službě bezpečnosti (FSB) RF (federální zákon č. 40, označován také jako 40-FZ) poskytuje státu právní nástroje donucení ke spolupráci formálně soukromé entity, a to včetně globálně působících výrobců ICT.[23] Ustanovení § 15 tohoto zákona umožňuje FSB instalovat dodatečný software a hardware do ICT produktů ruských společností,[24] stejně tak jako dosazovat důstojníky FSB do struktur soukromých firem.[25] Jedním z konkrétních případů osazeného softwaru je systém SORM (Systém pro operativní vyšetřovací činnost). Ten umožňuje FSB a dalším ruských bezpečnostním složkám monitoring síťového provozu zejména na ruském území. Slouží tak k získávání informací, sledování osob či digitální cenzuře, a je primárně nasazen na síťovém provozu v rámci RF. V rámci ukrajinského konfliktu však RF přistoupila k přesměrování síťového provozu na okupovaných územích právě skrze ruské poskytovatele a infrastrukturu, což ruským bezpečnostním složkám umožnilo systém SORM používat pro výše zmíněné účely i na území Ukrajiny. Okupační autority tak získaly informační kontrolu i nad tamním okupovaným obyvatelstvem.

Také Írán velmi pravděpodobně disponuje kapacitami narušit dodavatelský řetězec, nicméně limitují ho dva výrazné faktory. Těmi jsou technologická zaostalost ve srovnání s RF nebo ČLR a omezení záběru útoků hlavně na Blízký východ (primárně Izrael a Saúdská Arábie) či USA. V případě technologické zaostalosti je třeba brát v potaz, že v islámské republice neleží významné výrobní kapacity hardwaru (jako v ČLR) ani softwaru (jako v ČLR i RF), což tak Teheránem zaštítěným aktérům ztěžuje možnost kompromitace. Přesto země disponuje ofenzivními schopnostmi a technicky vzdělanou populací, kterou ekonomické sankce a nemožnost uplatnit se na legálním trhu práce často nutí participovat na škodlivých aktivitách. Legislativní mechanismy srovnatelné s RF a ČLR nejsou v Íránu veřejně známé, nicméně existují důkazy o tom, že mnoho domácích softwarových produktů je kompromitováno za účelem sledování opozice a potlačování disentu. Nelze tedy vyloučit, že Írán přijal vlastní restriktivní zákony v této oblasti.

[19] Law Bridge. 28.12.2013. Dostupné z: http://www.lawbridge.org/zhong-hua-ren-min-gong-he-guo-gong-si-fa-2013-nian-xiu-ding/

[20] Cyberspace Administration of China. 2017. 中华人民共和国网络安全法. Dostupné z: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[21] National People’s Congress of the People’s Republic of China. 2017. 中华人民共和国国家情报法. Dostupné z: http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml

[22] Human Rights Watch. 2020. Russia: Growing Internet Isolation, Control, Censorship. ttps://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

[23] Peter B. Maggs. 2018. Report of Peter B. Maggs. Dostupné z: https://assets.documentcloud.org/documents/4386053/Report-of-Peter-B-Maggs-Russian-Surveillance-Law.pdf

[24] Federalnyjj zakon ot 03.04.1995 N 40-FZ (red. ot 02.12.2019) "O federalnojj sluzhbe bezopasnosti [Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 02.12.2019) "О федеральной службе безопасности"].

[25] FSB Dossier. 2020. Apparat prikomandirovannykh sotrudnikov. [Аппарат прикомандированных сотрудников.] Dostupné z: https://fsb.dossier.center/prikom/.

Přestože i v ČR, stejně tak jako v dalších zemích EU a spojeneckých zemích ČR, existuje legislativa regulující vztah státu a soukromých společností pro potřeby zajišťování obrany státu a národní bezpečnosti,[26] pravomoci státu jsou ve srovnání s těmi čínskými či ruskými nepoměrně nižší. Případné zásahy musejí být řádně odůvodněné, podléhají soudnímu přezkumu a usilují o co nejmenší rozsah získávaných informací.

Dodavateli (či s jejich asistencí) způsobené úmyslné narušení kybernetické bezpečnosti strategicky významné infrastruktury, a to zejména nejzávažnější případy, jako je narušení dostupnosti systému ve velkém rozsahu, představuje podstatný problém pro významné ekonomické zájmy a bezpečnost státu, jelikož může výrazně narušit fungování státu, ekonomiky, společnosti a v krajním případě ohrozit zdraví a životy obyvatel.

Přestože jsou popsaná rizika spojená s dodavateli známá, v současnosti neexistuje v ČR komplexní mechanismus, který by umožnil rizika plynoucí z těchto strategických hrozeb pro strategicky významnou infrastrukturu cíleně, účinně a flexibilně vyhodnocovat a mitigovat. V rámci EU je toto již spíše ojedinělý stav, naopak napříč státy EU je běžnou praxí, že mechanismy pro posuzování a následné omezení či vynětí rizikových dodavatelů již fungují na zákonné, nebo alespoň podzákonné, rovině. Např. v Německu funguje komplexní mechanismus posuzující možnou nedůvěryhodnost až rizikovost dodavatele kritických komponent napříč kritickou informační infrastrukturou[27], založený na zákoně o bezpečnosti informačních technologií 2.0[28], přičemž v současnosti je německá legislativa podrobněji zaměřena na telekomunikační sektor. Lze konstatovat, že větší část členských států EU se zaměřuje na posuzování bezpečnosti dodavatelů v rámci jednoho, konkrétně telekomunikačního, sektoru. Mezi tyto státy se řadí například Belgie, Dánsko, Estonsko, Francie, Rakousko či třeba Irsko. Další zemí se zavedeným mechanismem pokrývajícím jednotlivé sektory skrze informační infrastrukturu je Slovensko, kde zákon č. 69/2018 Z.z., o kybernetické bezpečnosti, zavádí možnost zákazu technologie nebo služby pro posouzení rizik provedeném Národním bezpečnostním úřadem, přičemž důsledkem novely zmíněného zákona je Národnímu bezpečnostnímu úřadu umožněno zakázat či omezit specifický produkt, proces či službu třetí strany na poskytování základní služby, a to podle § 27a zákona č. 69/2018 Z.z.). Obdobný mechanismus je zaveden i v Rumunsku. Mechanismy některých států umožňují zakázat rizikové dodavatele skrze vládu, jak učinilo například Švédsko, nebo mimo prostor EU také Spojené království, Spojené státy, Kanada či Austrálie.

Legislativní požadavky na národní i EU úrovni v technické rovině zajišťování kybernetické bezpečnosti vedou ke zvyšování zabezpečení ICT na národní úrovni, a to především v infrastruktuře regulované zákonem o kybernetické bezpečnosti, mezi kterou je i strategicky významná infrastruktura. Útočníci tak musejí vynakládat stále vyšší úsilí směřující k narušení a nepozorovanému působení ve strategicky významných informačních systémech, což je zpravidla hlavní cíl škodlivého aktéra, jehož cílem je dlouhodobě narušovat důvěrnost, integritu či dostupnost informací přenášených těmito systémy. Takoví útočníci se musejí adaptovat na nové prostředí a vyhledávat nové vektory útoků. I to je jedním z důvodů zvyšující se atraktivity provádění útoků na dodavatelský řetězec, popř. využívání dodavatelů k prosazování cílů těchto škodlivých aktérů.

Stát nemůže ponechat výhradní výběr potenciálně rizikového dodavatele strategicky významné infrastruktury zcela v rukou soukromých firem, neboť ty nemusí být dostatečně vybaveny nebo motivovány k ochraně bezpečnosti ČR. Stejně tak soukromé společnosti nemusí

[26] V ČR se jedná zejména o zákon č. 289/2005 Sb., o Vojenském zpravodajství.

[27] Kritické infrastruktury se určují dle parametrů vyhlášky o určení kritické infrastruktury dle zákona o Spolkovém úřadu pro bezpečnosti informační techniky, zvané BSI-KritisV.

[28] V Německu je tento zákon taktéž označován jako IT-Sicherheitsgesetz 2.0 (zkráceně též „IT-SiG 2.0“) či IT Security Act 2.0.

mít dostatek informací a podkladů pro zhodnocení, zda jejich dodavatel představuje bezpečnostní riziko pro ČR. Ačkoli mají soukromé společnosti zájem o poskytování kvalitních a bezpečných produktů a služeb, jejich primárním cílem je dosažení zisku, přičemž tyto dva aspekty (bezpečnost versus výše zisku) mohou být v určitých případech v přímém rozporu a společnosti mohou upřednostnit vyšší zisk na úkor bezpečnosti. V souladu s čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů, podle kterého je základní povinností státu: „*zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot",* musí stát ze své podstaty na takové riziko reagovat a usilovat o jeho mitigaci.

Problematika prověřování bezpečnosti dodavatelského řetězce není v požadovaném rozsahu na národní úrovni dosud upravena. Základní mechanismy prověřování dodavatelského řetězce z pozice odběratele služby (správce informačního systému) jsou obsaženy v zákoně o kybernetické bezpečnosti a prováděcí vyhlášce o kybernetické bezpečnosti.

Zákon o kybernetické bezpečnosti v tomto ohledu zejména ukládá v § 5 svým povinným osobám zavádět technická a organizační bezpečnostní opatření, tedy konkrétní kroky k seznámení se s aktivy svých systémů, řízení rizik s nimi spojenými, zavedení minimálních opatření k technickému zabezpečení a jiné. Ve vztahu k dodavatelskému řetězci ukládá stávající právní úprava v oblasti kybernetické bezpečnosti povinným osobám v regulované infrastruktuře toliko znát své významné dodavatele,[29] informovat je o tomto jejich postavení, hodnotit rizika s významnými dodavateli spojená a smluvně své dodavatele zavazovat k přijetí některých kybernetických bezpečnostních politik.[30]

Dalším regulatorním nástrojem v oblasti definovaného problému je institut varování upravený § 12 zákona o kybernetické bezpečnosti a další opatření podle § 11 ZKB. Varování podle ZKB slouží mimo jiné k upozornění veřejnosti na hrozbu v oblasti kybernetické bezpečnosti, o které se Úřad dozvěděl z vlastní činnosti nebo od jiných orgánů nebo osob. Nejen pro výkon této kompetence je Úřadu umožněno provádět analýzu a monitoring kybernetických hrozeb a rizik.[31] Vydané varování podle ZKB pak mají povinné osoby podle ZKB v některých případech povinnost zohlednit v rámci řízení rizik spojených se svými systémy.

Právní řád tedy sice umožňuje zjišťovat a vyhodnocovat informace o hrozbách v oblasti kybernetické bezpečnosti, Úřadu ani ostatním organizačním složkám státu působícím v oblasti bezpečnosti ale nedává možnost seznamovat se s informacemi o dodavatelích v regulované infrastruktuře nebo o dodavatelích, kteří se o zakázky do regulované infrastruktury uchází, způsobem, který by umožňoval odhalit a vyhodnotit hrozbu spojenou s dodavateli ještě před tím, než bude vyhodnocena jako riziko pro regulovanou infrastrukturu.

V případě, kdy se ale Úřadu přesto podaří potřebné informace o současném či budoucím riziku spojenému s dodavatelským řetězcem získat a vyhodnotit, neumožňuje mu zákonná úprava na tato zjištění vhodně reagovat. Možnosti, které Úřad v takové situaci má, jsou pouze informovat o hrozbě formou varování podle zákona o kybernetické bezpečnosti nebo vydat reaktivní opatření podle § 13 ZKB – to však cílí už na určitý kybernetický bezpečnostní incident, a tedy na situaci bezprostředního narušení bezpečnosti regulované infrastruktury v konkrétní podobě. Minimalizovat zjištěnou strategickou hrozbu, spojenou s konkrétním

[29] Významným dodavatelem je podle § 2 písm. n) provozovatel systému podle zákona o kybernetické bezpečnosti a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti systému.

[30] § 8 vyhlášky o kybernetické bezpečnosti.

[31] § 22 písm. u) zákona o kybernetické bezpečnosti.

dodavatelem prostřednictvím omezení jeho přítomnosti ve strategicky významné infrastruktuře, se organizačním složkám státu nenabízí.

Možnost omezovat přítomnost rizikových dodavatelů ve strategicky významné infrastruktuře je tak zcela ponechána na povinných osobách podle zákona o kybernetické bezpečnosti. S ohledem na rozdělení pravomocí a povinností mezi státem a soukromým sektorem, jakož i mezi jednotlivými organizačními složkami státu, ale tyto povinné osoby nejsou motivovány analyzovat a omezovat hrozby pro větší množinu systémů strategicky významné infrastruktury, než za jaké jsou odpovědné. I pokud takovou hrozbu ale některá povinná osoba ve svém řízení rizik podle vyhlášky o kybernetické bezpečnosti reflektovat chce, nemá zpravidla oprávnění, nástroje ani kapacitu shromažďovat a vyhodnocovat informace k tomu potřebné.

Tzv. strategické hrozby spojené s dodavateli, tedy například možnost nepřezkoumatelných zásahů cizích států do aktivit dodavatele či neformální působení na dodavatele směřující k poškození jiného státu (viz část 1.2 Definice problému), vyžadují pro svoji sofistikovanost a komplexitu seznámení se s velkým množstvím informací, často zpravodajského či jiného charakteru. K těmto informacím má z podstaty věci povětšinou přístup pouze stát, resp. jeho bezpečnostní aparát, a neoprávněná dispozice s takovými informacemi, byť subjektem jednajícím v dobré víře (jako například zmiňovaná povinná osoba, mající vůli strategickou hrozbu reflektovat), je právními předpisy přísně sankcionována.[32]

Správci regulované infrastruktury tak stojí před opačným problémem než Úřad – mají přehled o užívaných dodavatelích (tzn. informace, které Úřadu schází), mají možnost omezit v infrastruktuře přítomnost vysoce rizikových dodavatelů, nemají ale možnost získat a vyhodnotit veškeré potřebné informace pro to, aby mohli hrozbu spojenou s dodavatelem účinně redukovat. Nezřídka se navíc stává, že identifikovaná hrozba, před níž Úřad vydal varování podle zákona o kybernetické bezpečnosti, není v analýze rizik povinných osob podle ZKB dostatečně, či dokonce jakkoli, reflektována. Podle výstupů z kontrol a auditů povinných osob prováděných podle ZKB je úskalím tohoto přístupu nejčastěji samotná vyspělost povinných osob v oblasti řízení rizik, kdy povinná osoba nesplňuje samotnou procesní prerekvizitu vykonávání analýzy rizik. V případě, kdy je varování podle ZKB v analýze rizik náležitě zohledněno, často nejsou řízeny následné procesy a alokovány zdroje pro ošetření daného rizika doložitelné formou např. plánu zvládání rizik.

Pro řešení definovaného problému nepostačuje ani současné zmocnění Úřadu k zajišťování metodické podpory v oblasti kybernetické bezpečnosti podle § 22 písm. j) zákona o kybernetické bezpečnosti. V rámci této pravomoci vydal ve snaze adresovat definovaný problém Úřad v únoru 2022 Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice (dále jen „5G Doporučení“).

5G Doporučení představuje podpůrný materiál pro výběr dodavatelů subjektů budujících a provozujících sítě a poskytujících služby elektronických komunikací, které jsou kritickou informační infrastrukturou. Cílem 5G Doporučení je nabídnout operátorům, potažmo celému odvětví elektronických komunikací, pohled Úřadu, Ministerstva průmyslu a obchodu, Ministerstva zahraničních věcí, Bezpečnostní informační služby, Úřadu pro zahraniční styky a informace a Vojenského zpravodajství na základní východiska posuzování důvěryhodnosti dodavatelů technologií do 5G sítí a navrhnout kritéria, která mohou přispět k výběru důvěryhodných dodavatelů.

[32] Např. zajištění si přístupu k utajované informaci bez současného splnění zákonných předpokladů umožňuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, podle § 148 odst. 4 písm. d) a § 155a odst. 2 potrestat pokutou až do 1 000 000 Kč.

Přestože byla vodítka tohoto druhu ze strany správců této infrastruktury dlouhodobě požadována, k reflexi 5G Doporučení jeho adresáty po jeho vydání prakticky nedošlo; mnozí správci kritické informační infrastruktury v sektoru elektronických komunikací nadále uzavírají kontrakty na dodávky technologií do bezpečnostně citlivých částí své infrastruktury s dodavateli, kteří po vyhodnocení kritérií 5G Doporučení na první pohled nevychází jako důvěryhodní.[33]

Na základě této zkušenosti se jeví neregulatorní působení na zohledňování strategické roviny důvěryhodnosti dodavatele v sektoru elektronických komunikací jako nedostatečné. Lze se domnívat, že ani v jiných sektorech hospodářství nebudou podnikatelské subjekty ochotny upřednostňovat strategickou důvěryhodnost dodavatele před ekonomickými aspekty dodávek, jako je například nabídková cena, nebudou-li existovat závazná regulatorní pravidla.

Problematika posuzování subjektů na základě mj. vyhodnocování kritérií netechnického charakteru je v současnosti již zavedena v právním řádu pro vymezené skupiny subjektů. Jedná se zejména o ZoISVS, který v §6m odst. 1 písm. c) stanovuje, že poskytovatel cloud computingu poskytujícího cloud computing orgánu veřejné správy může být pouze osoba nebo jiné právní uspořádání, které jsou způsobilé pro poskytnutí cloud computingu orgánu veřejné správy z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob. Poskytovatel cloud computingu musí zákonem definované požadavky splnit, jestliže má být zapsán v katalogu cloud computingu pro orgány veřejné správy (dále jen „katalog cloud computingu“). Pouze poskytovatelé zapsaní v katalogu cloud computingu mohou poskytovat služby cloud computingu orgánům veřejné správy.

Kromě nedostatečného zmocnění Úřadu k řešení definovaného problému nemají ani orgány a osoby v postavení zadavatele podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“) reálnou možnost zohlednit aspekt strategické bezpečnostní rizikovosti dodavatele v zadávacích podmínkách a při následném hodnocení nabídek. Stanovení a následné posuzování netechnických aspektů dodavatele vyžadují specifickou expertízu a informace, kterými zadavatelé zpravidla nedisponují. V konečném důsledku tak zpravidla dochází k výběru dodavatele veřejné zakázky na základě nabídkové ceny, případně jiných, snadno vyhodnotitelných kritérií.

Další regulací je ZoPZI, v § 1 písm. a) uvádí, že předmětem této právní úpravy je mj. stanovení pravidel prověřování některých zahraničních investic z důvodu ochrany bezpečnosti ČR nebo vnitřního pořádku. Zahraniční investoři do cílových osob definovaných § 7 ZoPZI tak budou podrobeni prověření s cílem získat povolení zahraniční investice, bez nějž tuto investici nemohou uskutečnit.

K účelu udržení nebo obnovení mezinárodního míru a bezpečnosti, boje proti terorismu, dodržování mezinárodního práva, ochraně lidských práv a svobod a podpoře demokracie a právního státu směřuje zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů (dále jen „zákon o mezinárodních sankcích“). Na základě tohoto zákona je možné nařízením či rozhodnutím vlády při splnění jedné z podmínek vymezených v § 2 uplatnit omezení či zákazy v oblastech stanovených v § 4 odst. 2 zákona o mezinárodních sankcích. K omezení či zákazu využívání ICT produktů na území ČR může dojít na základě:

[33] T-MOBILE CZECH REPUBLIC, A.S. T-Mobile pokračuje s rozšiřováním 5G sítí – spustil dalších 270 vysílačů. Dostupné z: https://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-pokracuje-s-rozsirovanim-5g-siti-spustil-dalsich-270-vysilacu.html; SEDLÁK, Jan. Varování navzdory. Vodafone a T-Mobile budou dál v 5G sítích nasazovat zařízení od Huawei. Dostupné z: https://www.e15.cz/byznys/technologie-a-media/varovani-navzdory-vodafone-a-t-mobile-budou-dal-v-5g-sitich-nasazovat-zarizeni-od-huawei-1389914

a) § 5 odst. 1 písm. a) zákona o mezinárodních sankcích, kdy může dojít k omezení nebo zákazu dovozu anebo koupě zboží, na které se vztahují mezinárodní sankce, jeho prodeje nebo jakéhokoli jiného nakládání s ním,

b) § 7 zákona o mezinárodních sankcích, kdy mohou sankce také v oblasti technické infrastruktury spočívat v omezení či zákazu dodávek energie nebo dodávek surovin, strojů nebo zařízení potřebných k její výrobě subjektu, osobě či celému území, na které se mezinárodní sankce vztahují.

Stávající právní úprava umožňuje omezit či zakázat produkty či služby poskytované určitými osobami, a to z důvodu možnosti existence strategického rizika spojeného s těmito osobami, majícího negativní vliv na zajištění ochrany bezpečnosti, veřejného pořádku či bezpečnosti a dodržování práv třetích osob v ČR. Poskytovatelé cloud computingu či zahraniční investoři jsou na základě platné právní úpravy v současnosti regulováni a prověřováni mj. i na základě hodnocení tzv. netechnických kritérií. Obdobná regulace je v současnosti potřebná taktéž pro dodavatele ICT do strategicky významné infrastruktury ČR, a to z důvodu nedostatečnosti platné právní úpravy pro řešení problému definovaného v části 1.2. Definice problému. Zákon o mezinárodních sankcích umožňuje dokonce omezení či zákaz dodávek zboží[34], jež se nemusejí vztahovat pouze ke zboží dodávanému určitým subjektem či osobou, ale i ke zboží pocházejícímu z celého území, na které se sankce vztahují. Ačkoli tento sankční režim umožňuje regulovat dodávky mj. také do strategické infrastruktury, z povahy věci jsou omezení spojená s udělováním sankcí především reaktivního charakteru na vývoj na mezinárodní úrovni. Jejich využívání pro potřeby mitigace rizika úmyslného narušení kybernetické bezpečnosti strategicky významné infrastruktury či vzniku strategické závislosti na rizikovém dodavateli tedy není dostačující. Plánovaná regulace dodavatelů nicméně počítá s využitím informací a poznatků těchto existujících mechanismů pro proces hodnocení důvěryhodnosti dodavatelů do strategické infrastruktury státu, a to z důvodu zvýšení efektivnosti tohoto procesu.

V současnosti je na úrovni EU plánováno zavedení evropského systému certifikace kybernetické bezpečnosti,[35] např. certifikační schéma pro 5G sítě. Evropský certifikační systém zahrnuje pouze technickou certifikaci produktů, služeb a procesů a nevyhodnocuje rovinu strategické důvěryhodnosti dodavatele. Prověřování strategické důvěryhodnosti dodavatelů však především nelze aplikovat na úrovni EU z důvodu vyloučení problematiky vnitřní bezpečnosti z úpravy primárního práva EU.[36] Evropský systém certifikace kybernetické bezpečnosti se tedy v současnosti jeví pouze jako vhodný doplněk k navrhovanému řešení, avšak nemůže a ani nemá ambice jej nahradit.

K výše uvedenému lze obecně doplnit, že především v případě rozvoje informačních technologií a s tím spojené otázky veřejnoprávní regulace kybernetické bezpečnosti může velmi jednoduše nastat situace, že legislativní prostředí zastará a může potenciálně přestat plnit svou funkci, případně aplikační praxe poukáže na jeho nedostatky. Přestože současná právní úprava používá řadu nástrojů, jak se tomuto riziku vyhnout, je vhodné a potřebné na vývoj situace včas reagovat.

V neposlední řadě je nutno uvést, že neprovedení transpozice směrnice NIS 2 do českého právního řádu by pravděpodobně bylo Evropskou komisí považováno za nesplnění povinnosti vyplývající ČR z primárního práva EU (Smlouva o Evropské unii a Smlouva

[34] Popř. v oblasti dodávek energií taktéž veškerých zařízení potřebných k její výrobě.

[35] Tento systém je zaváděn na základě 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“).

[36] Viz např. čl. 72 Smlouvy o fungování EU.

o fungování Evropské unie), přičemž by Evropská komise na základě čl. 258 Smlouvy o fungování Evropské unie mohla předložit tuto záležitost Soudnímu dvoru Evropské unie. V českém právním řádu aktuálně nejsou připraveny legislativní podmínky pro to, aby bylo možné jednoduše rozšířit okruh adresátů této normy, a tím zavést všechny požadavky směrnice.

Výše uvedená analýza skutkového stavu týkající se zavedení nových pravidel kybernetické bezpečnosti vycházejících z požadavků směrnice NIS 2 a níže rozebraný právní stav koresponduje s analýzou obsaženou v odůvodnění původního komisního návrhu směrnice NIS 2 [COM(2020)823 z 16. 12. 2020].

1.3.2. Návrh změnového zákona

V důsledku změn, které nastanou v českém právním řádu přijetím návrhu zákona, dojde k ovlivnění dosavadních procesů stanovených některými dalšími právními předpisy. Obecně lze shrnout, že se jedná především o tyto dva typy změn:

1) Změny se dotknou předpisů odkazujících na ZKB

2) Změny se dotknou předpisů, jejichž procesy budou návrhem zákona nově ovlivněny.

Příkladem prvního typu změny je právní úprava regulace cloud computingu v rámci ZoISVS. Účinné znění § 6i odst. 3 ZoISVS odkazuje na současný výčet povinných osob v ZKB, který se v novém návrhu zákona mění na jedinou povinnou osobu (poskytovatele regulované služby), což je potřeba reflektovat. Rovněž současná regulace využívání cloud computingu orgány veřejné správy podle ZoISVS počítá se dvěma vydanými vyhláškami podle ZKB. Konkrétně se jedná o vyhlášky stanovující bezpečnostní úrovně pro využívání cloud computingu orgány veřejné moci a bezpečnostní pravidla pro orgány veřejné moci využívající služeb cloud computingu. Tyto vyhlášky návrh zákona ruší a nadále Úřad nezmocňuje k jejich vydání.

Dalším příkladem prvního typu je obsah § 7 písm. c) ZoPZI. Tento zákon ve svém § 7 vymezuje okruh subjektů, do kterých nesmí být bez povolení podle § 14 odst. 1 nebo podmíněného povolení podle § 15 odst. 3 tohoto zákona uskutečněna zahraniční investice. Ustanovení § 7 písm. c) zní: *„cílové osoby, která je správcem informačního systému kritické informační infrastruktury, správcem komunikačního systému kritické informační infrastruktury, správcem informačního systému základní služby nebo provozovatelem základní služby“*. Zrušením ZKB a přijetím návrhu zákona dojde ke zrušení takto vymezených subjektů, a pokud by návrh zákona danou změnu nereflektoval, dojde k faktickému vyprázdnění vymezení daného v § 7 písm. c) ZoPZI.

Příkladem druhého typu je potřeba změn v účinném znění ZEK, případně zákona o poštovních službách. Oba tyto zákony shodně stanoví, že jejich adresáti (osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací v případě ZEK a držitel poštovní licence podle zákona o poštovních službách) jsou povinni ve vztahu k ČTÚ plnit povinnosti, které mohou být ve svém důsledku duplicitní k povinnosti hlášení kybernetických bezpečnostních incidentů stanovených návrhem zákona.

Další identifikovanou potřebou je úprava účinného znění ZoISVS týkající se stanovení bezpečnostních standardů pro dotčené systémy. Současná úprava v § 5a obsahuje zmocnění pro vydání vyhlášky o dlouhodobém řízení informačního systému veřejné správy, ve které měla být obsažena i kybernetická bezpečnost. V souvislosti s rozšířením okruhu povinných osob podle návrhu zákona zbývá druhově menší okruh povinných osob podle ZoISVS, které by uplatňovaly jiná pravidla než orgány, které jsou zahrnuty mezi povinné osoby podle návrhu zákona. To by vedlo k nekoncepčnímu uplatňování různých standardů kybernetické bezpečnosti a komplikacím v případě možného sdílené zkušeností napříč veřejnou správou. Stejně tak by bylo ztíženo případné resortní řízení bezpečnosti.

Pokud jde o změny zvláštních zákonů upravujících povinnost mlčenlivosti a povinnost dodržet bankovní tajemství (ZoB, ZPMS, AML, daňový řád, ZCS, ZoPZI), jejich neprovedení by mělo za následek, že by příslušné subjekty nemohly z důvodu povinnosti mlčenlivost, resp. bankovního tajemství, poskytovat Úřadu informace, které získaly při své činnosti či nezbytnou součinnost, jak je upraveno v návrhu zákona.

Přestože by se mohla jako relevantní jevit také změna zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, nebyla tato potřeba identifikována.

1.4. Popis existujícího právního stavu v dané oblasti

Problematika kybernetické bezpečnosti je v ČR aktuálně řešena zákonem o kybernetické bezpečnosti. Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti, stejně tak jako zapracovává příslušný předpis EU (výše zmíněnou směrnici NIS), zároveň navazuje na přímo použitelný předpis EU (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“), a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.

Prováděcími právními předpisy zákona o kybernetické bezpečnosti jsou vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, a vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, na základě kterých dochází ke stanovení kritérií části povinných osob spadajících pod zákon o kybernetické bezpečnosti, stejně tak jako vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti), která konkretizuje těmto povinným osobám povinnosti, především v otázce zavádění bezpečnostních opatření. S problematikou stanovení povinných osob spadajících pod zákon o kybernetické bezpečnosti souvisí úzce také nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které je vydáno k provedení zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), a které stanovuje kritéria pro určení jedné kategorie povinných osob podle zákona o kybernetické bezpečnosti – kritické informační infrastruktury. Zákon o kybernetické bezpečnosti také v jednom svém ustanovení řeší problematiku veřejnoprávní regulace cloud computingu, s čímž souvisí vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, resp. zákon o informačních systémech veřejné správy a o změně některých dalších zákonů. K provedení tohoto zákona je pak s užším vztahem k problematice kybernetické bezpečnosti vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

Problematika prověřování bezpečnosti dodavatelského řetězce není v požadovaném rozsahu na národní úrovni dosud upravena. Základní mechanismy prověřování dodavatelského řetězce z pozice odběratele služby (správce informačního systému) jsou obsaženy v zákoně o kybernetické bezpečnosti a prováděcí vyhlášce o kybernetické bezpečnosti (zejména jde o povinnost zavádět bezpečnostní opatření, jejichž obsahem je také povinnost řídit dodavatele).

Dílčí aspekty kybernetické bezpečnosti a ochrany ČR před kybernetickými útoky nad rámec výše uvedených předpisů jsou předmětem především následujících právních předpisů:

1.4.1. Ústavní pořádek České republiky

Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů,

Listina základních práv a svobod,

Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky.

1.4.2. Zákony České republiky

Zákon č. 110/2019 Sb., o zpracování osobních údajů,

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů,

Zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic),

Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů,

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů,

Zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů,

Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů,

Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů,

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů,

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů,

Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů,

Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů,

Zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů,

Zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů.

Zákon č. 21/1992 Sb., o bankách (zákon o bankách), ve znění pozdějších předpisů.

Zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů,

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů,

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů,

Zákon č. 280/2009 Sb., daňový řád (daňový řád), ve znění pozdějších předpisů,

Zákon č. 17/2012 Sb., o Celní správě České republiky (zákon o Celní správě České republiky), ve znění pozdějších předpisů.

1.4.3. Podzákonné předpisy České republiky

Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy,

Vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací,

Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací,

Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti,

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků,

Vyhláška č. 525/2011 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací,

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor,

Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací,

Vyhláška č. 241/2012 Sb., o stanovení náležitostí technicko-organizačních pravidel k zabezpečení bezpečnosti a integrity veřejné komunikační sítě a interoperability veřejně dostupných služeb elektronických komunikací za krizových stavů,

Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů,

Vyhláška č. 380/2022 Sb., o kritériích určení závažného narušení bezpečnosti sítě a služby a ztrátě integrity sítě a rozsahu a formě předávání informací o narušení.

Vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu,

1.4.4. Primární právo Evropské unie

Listina základních práv Evropské unie.

1.4.5. Sekundární právo Evropské unie

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),

Směrnice Evropského parlamentu a Rady o posílení odolnosti kritických subjektů (směrnice CER),

Nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru (nařízení DORA),

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),

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),

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (nařízení eIDAS),

Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center,

Nařízení Evropského parlamentu a Rady (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (akt o správě dat),

Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách),

Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích),

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích),

Nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou,

Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002,

Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU,

Rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU ze dne 25. října 2011 o podmínkách přístupu k veřejné regulované službě nabízené globálním družicovým navigačním systémem vytvořeným na základě programu Galileo.

Nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie,

Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace,

Směrnice Komise 2002/77/ES o hospodářské soutěži na trzích sítí a služeb elektronických komunikací,

Směrnice 2014/53/EU Evropského parlamentu a Rady ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES ve znění 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,

Směrnice Evropského parlamentu a Rady 97/67/ES ze dne 15. prosince 1997 o společných pravidlech pro rozvoj vnitřního trhu poštovních služeb Společenství a zvyšování kvality služby,

Směrnice Evropského parlamentu a Rady 2002/39/ES ze dne 10. června 2002, kterou se mění směrnice 97/67/ES s ohledem na další otevření poštovních služeb Společenství hospodářské soutěži,

Směrnice Evropského parlamentu a Rady 2008/6/ES ze dne 20. února 2008, kterou se mění směrnice 97/67/ES s ohledem na úplné dotvoření vnitřního trhu poštovních služeb Společenství,

Směrnice Evropského parlamentu a Rady 97/67/ES ze dne 15. prosince 1997 o společných pravidlech pro rozvoj vnitřního trhu poštovních služeb Společenství a zvyšování kvality služby. Směrnice Evropského parlamentu a Rady 2009/44/ES ze dne 6. května 2009, kterou se mění směrnice 98/26/ES o neodvolatelnosti zúčtování v platebních systémech a v systémech vypořádání obchodů s cennými papíry a směrnice 2002/47/ES o dohodách o finančním zajištění, pokud jde o propojené systémy a pohledávky z úvěru.

Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES.

Nařízení Evropského parlamentu a rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012.

Směrnice Evropského parlamentu a Rady 2008/6/ES ze dne 20. února 2008, kterou se mění směrnice 97/67/ES s ohledem na úplné dotvoření vnitřního trhu poštovních služeb Společenství.

Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (přepracované znění).

Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES.

Směrnice Evropského parlamentu a Rady (EU) 2019/1153 ze dne 20. června 2019 o stanovení pravidel usnadňujících používání finančních a dalších informací k prevenci, odhalování, vyšetřování či stíhání určitých trestných činů a o zrušení rozhodnutí Rady 2000/642/SVV.

Nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie.

1.4.6. Poziční a koncepční dokumenty veřejné správy ČR

S ohledem na přijetí zákona o kybernetické bezpečnosti v roce 2015 došlo k přesunutí rámce řešení kybernetické bezpečnosti právě do obsahu tohoto zákona. Na druhou stranu, doprovodné poziční a koncepční dokumenty stále hrají významnou roli.

Z nejaktuálnějších dokumentů se jedná především o Národní strategii kybernetické bezpečnosti ČR na období let 2021–2025 a na ni navazující Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025. Samotná strategie je založená na vizi, ve které ČR bude mít odolnou společnost a infrastrukturu, v kyberprostoru bude vystupovat sebevědomě a bude aktivně čelit celému spektru kybernetických hrozeb za pomocí spolehlivých spojenectví. K naplnění této vize stanovuje strategické cíle ve třech hlavních oblastech, které tvoří její základní pilíře, a které označuje jako Sebevědomě v kyberprostoru, Silná a spolehlivá spojenectví a Odolná společnost. Tyto tři pilíře dohromady tvoří základ kybernetické bezpečnosti ČR v letech 2021 až 2025.

Bezpečnostní rada státu vydala usnesení ze dne 21. června 2022 č. 41, k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu.

Relevantním dokumentem je Bezpečnostní strategie ČR z roku 2023.

V roce 2016 byl také zpracován tzv. Audit národní bezpečnosti.

Byl schválen Národní plán výzkumu a vývoje v oblasti kybernetické a informační bezpečnosti do roku 2020.

Dne 17. srpna 2020 schválila vláda v utajovaném režimu také Koncepci rozvoje Národního úřadu pro kybernetickou a informační bezpečnost.

1.4.7. Další relevantní dokumenty

Na mezinárodní bezpečnostní konferenci o 5G v Praze byly dne 3. května 2019 vyhlášeny tzv. Pražské návrhy („Prague Proposals“) týkající se doporučení v oblasti zabezpečení sítí 5. generace. Na to navázaly členské státy EU s podporou Evropské komise a Evropské agentury pro bezpečnost sítí a informací a vydaly sadu opatření na zmírnění rizik spojených s budováním sítí 5. generace, tzv. 5G security toolbox.

1.4.8. Zhodnocení právního stavu

Jak plyne z výše uvedeného, legislativa v oblasti kybernetické bezpečnosti začala nabývat na důležitosti a došlo k vydání celé řady stěžejních dokumentů. Zákon o kybernetické bezpečnosti a jeho prováděcí právní předpisy celou řadu těchto potřeb reflektoval prostřednictvím novelizací, nicméně praktická aplikace těchto ustanovení poukazuje na stále závažnější nedostatky. S ohledem na přijetí směrnice NIS 2, spolu s tím celé řady dalších výše uvedených právních aktů EU, a zároveň na legislativní úkol zpracovat a vládě předložit návrh zákona, zpracovaný na základě Bezpečnostní radou státu zvoleného přístupu A – Prověřování dodavatelů podle aktuální bezpečnostní situace uvedeného v materiálu „Bezpečnost dodavatelských řetězců strategické infrastruktury státu“, je potřeba zvážit, jakým způsobem dané požadavky v českém právním řádu reflektovat. Jako optimální se jeví zpracování nového zákona o kybernetické bezpečnosti i všech jeho prováděcích právních předpisů (viz níže).

1.5. Identifikace dotčených subjektů

Návrh zákona označuje hlavní skupinu dotčených subjektů jako tzv. poskytovatele regulovaných služeb. Toto označení tak reflektuje akcent nové právní úpravy na nutnost zabezpečení služeb, které jsou významné pro zabezpečení důležitých společenských nebo ekonomických činností. Vzhledem ke smyslu a účelu návrhu zákona, tj. k ochraně aktiv před kybernetickými bezpečnostními incidenty, jakož i vzhledem k dominantní roli principu technologické neutrality, se návrh zákona nedotýká uživatelů ani poskytovatelů obsahu ve službách informační společnosti.

Poskytovateli regulované služby jsou tak orgány nebo osoby, které poskytují jednu nebo více regulovaných služeb. Forma nebo charakter takového poskytovatele regulované služby, tedy zda jde o veřejnou nebo soukromou společnost nebo státní orgán, není rozhodná. Do regulace tedy spadnou jak soukromí poskytovatelé regulovaných služeb, tak státní orgány poskytující služby v odvětvích stanovených příslušným prováděcím předpisem. Orgánem nebo osobou spadající do působnosti návrhu zákona bude také orgán nebo osoba určený jako subjekt kritické infrastruktury podle krizového zákona, resp. podle zákona transponujícího směrnici CER.

Přestože návrh zákona stále maximálně vychází z principů, na nichž byl postaven již původní zákon o kybernetické bezpečnosti, a tedy, že za standardní situace jsou konkrétní povinnosti k zavedení bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů a provádění opatření ukládány pouze těm subjektům, jejichž služby mají zásadní

význam pro fungování státu nebo informační společnosti, musí dojít vzhledem ke změně přístupu směrnice k výraznému rozšíření této množiny.

Návrh zákona stanovuje definici poskytovatele regulované služby zcela novým způsobem. Důvody k tomu jsou tři.

Prvním důvodem je, že pojmosloví používané ostatními právními předpisy nikdy zcela nevystihuje dané požadavky, a je ve většině případů příliš omezené na technické pojmosloví – síť elektronických komunikací, informační systém, komunikační systém, provozovatel informačního systému apod. Ačkoli se toto pojmosloví zdá v oblasti kybernetické bezpečnosti nanejvýš logické, vede k celé řadě praktických problémů. Kybernetická bezpečnost, resp. její zajišťování, je souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v ČR, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže, ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Přílišnou vazbou pojmů a definic na technický aspekt kybernetické bezpečnosti dochází k výkladovým problémům a k omezování rozsahu tohoto pojmu.

Druhým důvodem je potřeba odlišit označení povinné osoby podle návrhu zákona od množin povinných osob podle dosavadního zákona o kybernetické bezpečnosti. Naprostá většina povinných osob přejde pod rozsah návrhu zákona, a právě proto je potřeba rozlišit jejich původní a novou roli v této právní úpravě.

Třetí podstatnou součástí identifikace dotčených subjektů je také nově zaváděný institut tzv. režimů. Návrh zákona zná dva režimy – režim vyšších a režim nižších povinností poskytovatele regulované služby – a poskytovatele regulovaných služeb do těchto dvou množin rozděluje. Každý provozovatel regulované služby se jako povinná osoba nachází vždy jen v jednom režimu. Režim mu stanovuje přesnější povinnosti, které mu ze návrhu zákona plynou.

Pokud odhady počtu povinných osob v důsledku změny jejich identifikace v návaznosti na obsah směrnice hovoří o minimálním počtu 6 000 povinných osob podle návrhu zákona, zaváděná kritéria rozdělení těchto povinných osob do režimů pak vedou k odhadům v poměru cca 1:5, tj. 1 000 poskytovatelů regulované služby v režimu vyšších povinností a 5 000 poskytovatelů regulované služby v režimu nižších povinností. Odhad počtu povinných osob je problematický, a to zejména z důvodu, že ještě v tuto chvíli, několik měsíců po přijetí směrnice NIS2, probíhají na úrovni EU diskuze o tom, jak některé definice povinných osob chápat a pojímat, případně jak aplikovat velikostní kritérium. Úřad se dlouhodobě snaží vyjednávat racionální přístup, a tím omezovat počet regulovaných osob na účelné minimum. Stanovený počet minimálně 6 000 povinných osob vychází z porovnání těch regulovaných služeb, u kterých je jejich rozsah jasný a není předmětem diskuze, při současné aplikaci kritéria velikosti více než 50 zaměstnanců (nebo využití jiného počtu zaměstnanců, relevantně podle směrnice NIS2). Pokud je za současného stavu regulovaných osob cca 400 (v čase se také proměňuje), vychází pak při porovnání těchto dvou čísel minimálně patnáctinásobné navýšení počtu povinných osob, nicméně toto číslo není konečné. Typové označení konkrétně dotčených firem pak odpovídá návrhu vyhlášky o regulovaných službách, resp. v příloze směrnice NIS2. Jednou z největších kategorií v rámci povinných osob budou zejména podnikatelé poskytující veřejně dostupnou službu elektronických komunikací podle zákona o elektronických komunikacích, poskytovatelé zdravotní péče podle zákona o zdravotních službách, provozovatelé vodovodů a kanalizací podle zákona o vodovodech a kanalizacích a další. Celkový počet povinných osob není možné v rámci ČR v tomto okamžiku odhadnout.

Je to dáno jednak tím, co je uvedeno výše, za druhé také tím, že pro úplné srovnání a stanovení velikostního kritéria je nutný alespoň omezený přístup k obratu a hodnotě aktiv relevantních společností, což je ovšem informace, kterou Generální finanční ředitelství nemůže před účinností zákona poskytnout. Na tuto skutečnost reaguje návrh v § 64 odst. 4.

Spolu s výše uvedenou hlavní množinou povinných osob – poskytovatelů regulovaných služeb – je směrnicí pod návrh zákona zavedena také dílčí množina subjektů poskytujících služby registrace doménových jmen. Tato množina povinných osob není s množinou poskytovatelů regulovaných služeb nijak provázána a její povinnosti jsou minimální.

Návrh zákona zavádí ve specifických situacích také další typy povinných osob. Katalog povinností založených návrhem zákona orgánům a osobám je uveden v tabulce níže:

Typ povinné osoby	Režim povinné osoby	Základní povinnosti
Poskytovatel regulované služby	Režim vyšších povinností	Hlášení údajů Stanovení rozsahu řízení kybernetické bezpečnosti Zavádění bezpečnostních opatření (vyšší požadavky) Hlášení kybernetických bezpečnostních incidentů Plnění informační povinnosti vůči odběratelům služby Provádění protiopatření Zohlednění požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele Speciální úprava předání informací a dat od významného dodavatele Pro stanovenou část poskytovatelů regulované služby v režimu vyšších povinností zajištění dostupnosti strategicky významné služby Pro stanovenou část poskytovatelů regulované služby v režimu vyšších povinností povinnost mechanismu prověřování bezpečnosti dodavatelského řetězce
	Režim nižších povinností	Hlášení údajů Stanovení rozsahu řízení kybernetické bezpečnosti

		Zavádění bezpečnostních opatření (základní požadavky) Hlášení kybernetických bezpečnostních incidentů s významným dopadem Plnění informační povinnosti vůči odběratelům služby Provádění protiopatření Zohlednění požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele
Subjekt poskytující službu registrace doménových jmen	-	Shromažďování a uchovávání údajů o registraci doménových jmen
Významný dodavatel, resp. osoba disponující požadovanými daty	-	Předání informací a dat souvisejících s provozem aktiv sloužících k poskytování regulované služby na základě rozhodnutí Úřadu
Osoby povinné plnit opatření k řešení stavu kybernetického nebezpečí	-	Plnění opatření k řešení stavu kybernetického nebezpečí vyhlášených Úřadem Poskytnutí součinnosti
Držitel evropského certifikátu kybernetické bezpečnosti Výrobce nebo poskytovatel produktů, služeb nebo procesů vydávající EU prohlášení o shodě Právnická nebo podnikající fyzická osoba	-	Povinnosti plynoucí z přímo použitelného předpisu EU vydaného na základě aktu o kybernetické bezpečnosti
Fyzická osoba jako zaměstnanec Úřadu	-	Mlčenlivost
Orgány veřejné moci	-	Součinnost ve formě podnětů, informací a jiné formy součinnosti potřebné k plnění úkolů Úřadu

Každý	-	Součinnost k posouzení naplnění kritérií regulované služby Součinnost při zajišťování podkladů pro vydání protiopatření

Navrhované řešení bude mít přímý dopad na Úřad, a to zejména pokud jde o zajištění procesů vyplývajících z jeho postavení jakožto gestora problematiky kybernetické bezpečnosti v ČR.

Co se podrobněji týče zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, návrh zákona bude mít přímý dopad jak na vybrané povinné osoby návrhu zákona, tak na jejich dodavatele, jejichž specificky vymezené typy dodávek do strategicky významné infrastruktury ČR mohou být po zavedení regulace omezeny. V neposlední řadě budou regulací významně ovlivněny taktéž státní orgány, které budou do procesu prověřování bezpečnostní spolehlivosti dodavatelů zapojeny.

1.5.1. Poskytovatelé strategicky významné služby

Dotčenými subjekty mechanismu prověřování bezpečnosti dodavatelského řetězce jsou v prvé řadě poskytovatelé strategicky významné služby. Konkrétně se jedná o poskytovatele regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, a to podle vyhlášky o regulovaných službách. Jedná se o poskytovatele takových regulovaných služeb, které naplňují kritéria pro určení regulované služby v režimu vyšších povinností, a zároveň by narušení bezpečnosti informací poskytovatele regulované služby mohlo způsobit závažný dopad na bezpečnost ČR nebo vnitřní pořádek. Odhadem se jedná o 150 subjektů, kterými jsou strategicky nejvýznamnější subjekty působící v odvětvích veřejné správy, energetiky, dopravy a digitální infrastruktury. V tomto dokumentu je množina poskytovatelů těchto regulovaných osob označována jako „strategicky významná infrastruktura“ nebo „poskytovatelé strategicky významné služby“.

Hlavní přímý dopad návrhu zákona na poskytovatele strategicky významné služby spočívá ve stanovení několika nových povinností, a to zejména povinnosti nahlašovat Úřadu specificky vymezený okruh dodavatelů, jejichž dodávky využívají v rámci vymezené regulované části infrastruktury. Dále bude poskytovatelům strategicky významné služby uložena povinnost reflektovat opatření obecné povahy vydaná Úřadem ve vztahu ke svým dodavatelům. Podle výsledků dotazníkového šetření[37] respondenti uvedli, že mají v průměru 9 dodavatelů plnění do infrastruktury tvořící informační nebo komunikační systém regulovaný zákonem o kybernetické bezpečnosti.[38] Průměrně 5 dodavatelů dodává respondentům aktiva (kromě objektů), která jsou hodnocena jako vysoká nebo kritická podle přílohy č. 1 k vyhlášce o kybernetické bezpečnosti (dále jen „kritická a vysoká aktiva“).[39] 5 dodavatelů je v průměru také zapojených do vývoje, výroby, sestavení, servisu či dodávek do vysokých a kritických technických aktiv respondentů.[40]

[37] Dotazníkové šetření bylo adresovaného všem orgánům a osobám podle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně Úřad vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. Úřad obdržel 65 takových odpovědí (dále jen „respondenti“).

[38] Na tento dotaz poskytlo kvantifikovatelnou odpověď 64 respondentů.

[39] Na tento dotaz poskytlo kvantifikovatelnou odpověď všech 65 respondentů.

[40] Na tento dotaz poskytlo kvantifikovatelnou odpověď všech 65 respondentů.

Dojde ke zvýšení nákladů poskytovatelů strategicky významné služby. Náklady mohou mít podobu jak finanční, tak personální, ty však lze rovněž převést na finanční, dále se proto zvažují již jen finanční náklady. Zvýšené náklady vyplývají z povinnosti hlásit přímé dodavatele a vyvinout přiměřenou snahu k zjišťování nepřímých dodavatelů, tedy vyžadují odpovídající kapacity pro zmapování dodavatelského řetězce, udržování a aktualizaci této informace.

Další ze zvýšených nákladů vyplývá z povinnosti reagovat na vydaná omezení, ke splnění této povinnosti je tak třeba uvažovat kapacity pro sledování vydaných omezení, vyhodnocení nezbytných zdrojů pro reakci na omezení (např. vyčíslení finančních nákladů na implementaci omezení), nastavení plánu reakce na konkrétní omezení (např. rozplánování jednotlivých kroků projektu implementace omezení s ohledem na stanovenou lhůtu pro splnění omezení), a zejména kapacity nezbytné pro snížení hrozby v případě mírnějšího omezení dodavatele (např. přijetí technického bezpečnostního opatření – pořízení nového prvku, úprava nastavení prvku atp.), nebo obměnu plnění poskytovaného dodavatelem v případě zákazu využívání konkrétního dodavatele (např. náklady spojené s ukončením smlouvy, odpisem nevyužitého majetku, pořízením nového majetku).

Cílem možnosti udělování takovýchto výjimek je předejít paralýze infrastruktury (resp. ohrožení poskytování regulované služby podstatným způsobem) v důsledku zákazu nenahraditelné technologie. Zároveň ovšem bude udělování výjimek prováděno až na základě žádosti některého poskytovatele strategicky významné služby, který bude mít povinnost uvést a vysvětlit důvody, které by k udělení výjimky měly vést, vč. řádného podložení svých tvrzení důkazy. K udělení výjimky může Úřad přistoupit i z moci úřední, např. na základě podnětu. Úřad následně získané informace vyhodnotí z pohledu potřeby stanovení výjimky ze zákazu daného vysoce rizikového dodavatele, a to v procesu připomínek k návrhu opatření obecné povahy (dále jen „OOP“), prostřednictvím kterého budou rozhodnutí o identifikované míře rizikovosti dodavatele sdělována veřejnosti, a na základě kterého budou poskytovatelům strategicky významné služby plynout povinnosti související s využíváním plnění daného identifikovaného dodavatele.

Vyčíslení nákladů není dobře možné, protože do něj vstupuje řada neznámých proměnných, a to zejména, jak často bude nutné přistoupit k omezení některého z dodavatelů, v jakém rozsahu bude omezovaný dodavatel ve strategické infrastruktuře zastoupen a jaký způsob reakce na dané omezení přijme konkrétní poskytovatel strategicky významné služby.

Za další dopad je možné považovat omezení nabídky a konkurenčního prostředí na trhu. Při využití některého z omezených dodavatelů bude nezbytné vynaložit vyšší finanční náklady (viz první negativní dopad) ke snížení jeho hrozby, nebo bude přímo zakázáno využití konkrétního dodavatele. Tento stav povede ke snížení významu nebo odstranění omezeného dodavatele z relevantního trhu (trh s plněním do strategické infrastruktury), což bude mít za následek omezení nabídky, a v některých oblastech i konkurenčního prostředí, a tedy zvýšení ceny plnění ostatních dodavatelů.

Poskytovatelé strategicky významné služby mají právo v průběhu procesu vydávání OOP (kterým bude zakázáno využívání plnění konkrétního dodavatele) podávat připomínky. Cílem regulace je zvýšení odolnosti a bezpečnosti strategicky významné infrastruktury v ČR, v žádném případě však cílem není ohrožení poskytování regulované služby. Pokud dodavatel poskytuje bezpečnostně významnou dodávku, která je nezbytná pro poskytování regulované služby v požadované kvalitě, a zároveň neexistuje žádný jiný dodavatel, který by takovou dodávku mohl poskytnout, Úřad může udělit výjimku pro využívání bezpečnostně významné dodávky. V některých případech může jít např. o zajištění minimálního fungování služby, v některých případech o zajišťování služby na úrovni odpovídající posledním poznatkům – high-end technologie. Jedná se např. o možnost využívat unikátní (např. patentované)

technologie od dodavatele vyhodnoceného jako vysoce rizikového, které jsou nezbytné pro poskytování regulované služby.

Dojde-li k udělení výjimky a využije-li tuto výjimku některý z poskytovatelů strategicky významné služby, stane se ČR závislá na vysoce rizikovém dodavateli. Tato závislost bude umocněna tím, že Úřad potvrdí, že pro danou typovou dodávku na trhu neexistuje alternativní dodavatel. Toto riziko bude mít poskytovatel strategicky významné služby povinnost mitigovat určitými bezpečnostními opatřeními, nicméně jak bylo popsáno v části 1.2. Definice problému, strategické riziko plynoucí ze závislosti na rizikovém dodavateli není možné uspokojivě mitigovat technickými či organizačními opatřeními. Vhodně nastavená opatření mohou značně snížit míru rizika pro důvěrnost a integritu informací, nicméně rizika plynoucí pro dostupnost informací, a tedy i služby jako takové, příslušnými opatřeními uspokojivě mitigovat nelze.

1.5.2. Dodavatelé poskytovatelů strategicky významné služby

Dalšími přímo dotčenými subjekty jsou dodavatelé plnění do strategicky významné infrastruktury v pozici přímého dodavatele nebo subdodavatele. Budou-li tito dodavatelé vyhodnoceni jako bezpečnostně rizikoví či vysoce rizikoví, Úřad vydáním varování podle návrhu zákona nebo vydáním OOP omezí či zakáže využití jejich zboží či služeb ve výše uvedené infrastruktuře.

Ačkoli samotným dodavatelům mechanismus prověřování bezpečnosti dodavatelského řetězce nestanoví žádné povinnosti, návrh zákona by na ně měl nepřímý dopad, jelikož může zasáhnout do jejich podnikatelských aktivit. Úřad omezí poskytovatelům strategicky významné služby možnost využití dodávek takových dodavatelů, kteří budou podle kritérií stanovených v prováděcím právním předpisu vyhodnoceni jako rizikoví z hlediska ochrany bezpečnosti ČR, veřejného pořádku a dodržování práv třetích osob.

Negativním dopadem je pak reputační dopad na dodavatele, na kterého bude veřejně aplikováno omezení. Lze předpokládat, že i ostatní zákazníci omezeného dodavatele, kteří nejsou poskytovateli strategicky významné služby, budou vydané omezení vnímat negativně, což může vést v konečném důsledku ke snížení poptávky po plnění poskytovaném omezeným dodavatelem, a tedy zvýšení poptávky na trhu, a tedy nárůstu ceny obdobného plnění.

1.5.3. Státní orgány

Nepřímo dotčenými subjekty jsou státní orgány, které by měly být přímo zapojeny do procesu shromažďování informací o rizikovosti dodavatelů. Jde o orgány, které z povahy své činnosti budou disponovat informacemi, které budou nezbytné pro posouzení naplnění kritérií rizikovosti dodavatele a které si Úřad nemůže opatřit sám ze své činnosti.

Jmenovitě se jedná o Úřad, Bezpečnostní informační službu, Finanční analytický úřad, Ministerstvo průmyslu a obchodu, Ministerstvo vnitra, Ministerstvo zahraničních věcí, Nejvyšší státní zastupitelství, Policii ČR, Úřad pro ochranu hospodářské soutěže, Úřad pro zahraniční styky a informace, Vojenské zpravodajství a další státní orgány, které budou osloveny k poskytnutí informací a součinnosti v případě potřeby. Tyto státní orgány shromažďují informace o rizikovosti dodavatelů a tyto informace poskytují Úřadu, a to vždy na základě své zákonné působnosti a expertízy v dané oblasti prověřování. Úřad dále tyto obdržené informace vyhodnotí, a v případě identifikace rizika vydává omezení vztahující se k danému dodavateli.

V případě, že Úřad určí lhůtu pro zavedení omezení či vyloučení plnění od dodavatele v souladu s délkou odpisování podle právního předpisu upravujícího zdanění příjmů, Bezpečnostní rada státu dostane v dostatečném předstihu návrh OOP obsahující omezení či vyloučení plnění do strategicky významné služby pro informaci, a to poté, co Úřad návrh

OOP projedná s ostatními orgány uvedenými v § 28 odst. 1 až 3, Ministerstvem financí, a v případě, že se návrh OOP dotýká jejich působnosti, s Českým telekomunikačním úřadem a Energetickým regulačním úřadem.

V případě, že Úřad navrhne lhůtu kratší, než je uvedeno v předchozím odstavci, Úřad předloží návrh OOP po projednání podle předchozího odstavce k projednání vládě. Vláda poté uloží Úřadu, jakým způsobem bude Úřad ve věci návrhu OOP postupovat.

Důvodem pro tento postup je to, aby vláda zvážila v případě navržení kratší lhůty proporcionalitu zásahu způsobeného návrhem OOP s ohledem na významné ohrožení bezpečnosti ČR nebo vnitřního pořádku ve srovnání s dalšími chráněnými hodnotami.

1.5.4. Adresáti právních předpisů dotčených návrhem změnového zákona

1.5.4.1. ZoISVS

Návrh zákona se dotýká práv a povinností správců informačních systémů veřejné správy podle § 2 odst. 1 písm. c) ZoISVS.

1.5.4.2. ZoPZI

V případě prověřování investic podle tohoto zákona je okruh subjektů, do kterých nesmí být bez povolení podle § 14 odst. 1 nebo podmíněného povolení podle § 15 odst. 3 uskutečněna zahraniční investice, vymezen prostřednictvím tzv. cílové osoby. Cílové osoby jsou vymezeny v § 7 písm. a) až d). Jednou z množin takto stanovených cílových osob je také množina stanovená v písm. c) jako *„správci informačního systému kritické informační infrastruktury, správci komunikačního systému kritické informační infrastruktury, správci informačního systému základní služby a provozovatelé základní služby*“. Osoby z této množiny jsou zároveň povinnými osobami podle zákona č. 181/2014 Sb.

1.5.4.3. ZEK

Adresáty příslušné normy uvedenými v § 98 jsou osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací.

1.5.4.4. Zákon o poštovních službách

Adresáty příslušné normy jsou v tomto případě držitelé poštovní licence podle § 33.

1.5.4.5. ZoB

Adresáty příslušné normy jsou banky.

1.5.4.6. ZPMS

Adresátem příslušné normy je Finanční analytický úřad.

1.5.4.7. AML

Adresátem příslušné normy je stejně jako v případě ZPMS Finanční analytický úřad.

1.5.4.8. Daňový řád

Adresátem příslušné normy je správce daně.

1.5.4.9. ZCS

Adresáty příslušné normy jsou celníci podle § 15 odst. 1 ZCS a občanští zaměstnanci podle § 15 odst. 2 ZCS.

1.6. Popis cílového stavu

1.6.1. Návrh zákona

Cílem návrhu zákona je úplná a správně provedená transpozice směrnice NIS 2, zavedení funkčního a efektivního mechanismu prověřování bezpečnosti dodavatelského řetězce a reflexe dosavadních zkušeností s fungováním a praktickou použitelností zákona o kybernetické bezpečnosti tak, aby vznikl jednotící předpis, který bude srozumitelný pro adresáty a povede k zajištění bezpečného fungování informační společnosti ČR, tj. zajištění bezpečné realizace základního práva na informační sebeurčení prostřednictvím informačních systémů, služeb a sítí elektronických komunikací. Cílem návrhu zákona je též ochrana nedistributivních práv státu, tj. zajištění veřejného zájmu na bezpečnosti regulovaných služeb.

Cílovým stavem je ve shora uvedeném smyslu fungující systém kybernetické bezpečnosti zahrnující:

- bezpečnostní opatření,
- hlášení kybernetických bezpečnostních incidentů,
- systém opatření k reakci na kybernetické bezpečnostní incidenty,
- činnost dohledových pracovišť (národní CERT a vládní CERT),
- a výkon státní správy v oblasti kybernetické bezpečnosti s tím spojený.

Jak plyne ze shora uvedeného, není cílem návrhu zákona regulovat obsah jednotlivých informačních transakcí. Návrh zákona tedy nezasahuje do obsahového fungování informační společnosti, ale pouze si klade za cíl zabezpečit proti úmyslným nebo nahodilým kybernetickým bezpečnostním incidentům informační kanály, jimiž člověk realizuje své právo na informační sebeurčení, a jimiž stát vykonává svá nedistributivní informační práva.

Stejně, jako tomu bylo v případě zákona o kybernetické bezpečnosti, je cílem návrhu zákona především stanovit minimální požadavky na standardní zabezpečení poskytovatelů regulovaných služeb (v režimu vyšších nebo nižších povinností), a zajistit vládnímu dohledovému pracovišti v reálném čase přehled o kybernetické bezpečnostní situaci u těchto poskytovatelů. Poskytovatelům regulovaných služeb zajistí návrh zákona nepřetržitý kontakt s vládním dohledovým pracovištěm umožňující kvalitnější identifikaci kybernetických bezpečnostních rizik s původem mimo příslušný systém, službu nebo síť, efektivnější analýzu kybernetických bezpečnostních událostí a účinnější reakci na kybernetické bezpečnostní incidenty.

Specifickým cílem zavedení funkčního a efektivního mechanismu prověřování bezpečnosti dodavatelského řetězce v návrhu zákona je omezit závislost strategicky významné infrastruktury ČR na rizikových dodavatelích představujících strategickou hrozbu v oblasti kybernetické bezpečnosti, a přispět tak k zajištění dlouhodobě udržitelné bezpečnosti a odolnosti strategicky významné infrastruktury. Při dosažení cílového stavu by měla být ve strategicky významné infrastruktuře omezena přítomnost rizikových a potenciálně rizikových dodavatelů, jež mohou představovat bezpečnostní hrozbu pro ČR. Mělo by tak dojít k významnému omezení možnosti negativního zahraničního působení na zajištění základních funkcí státu prostřednictvím zneužití závislosti v dodavatelsko-odběratelských vztazích, jako je proprietární uzamčení odběratele, tzv. vendor lock-in, nevynucené omezení dodávek či zneužití infrastruktury nebo neoprávněný zásah do ní.

Návrh zákona si dále klade za cíl prostřednictvím intenzivnějšího informování poskytovatelů strategicky významné služby o hrozbách spojených s rizikovými dodavateli přispívat k tomu, že i poskytovatelé strategicky významné služby začnou sami klást větší důraz na bezpečnost, včetně aspektů rizikovosti, které posuzuje stát. Dlouhodobým cílem návrhu zákona je tedy také změnit přístup samotných poskytovatelů strategicky významné služby k výběru dodavatelů. Poskytovatelé strategicky významné služby by měli klást větší důraz

na bezpečnost a menší důraz pouze na pořizovací cenu ICT produktů a služeb. Dodavatelé, kteří budou nabízet bezpečná ICT řešení, a to jak z pohledu technického, tak strategického, by tak získávali konkurenční výhodu oproti dodavatelům, kteří nejsou schopni takové záruky poskytnout.

Rizika v oblasti kybernetické bezpečnosti nelze zcela eliminovat. Akceptace míry rizika, která je uvedena v části 1.2. Definice problému, je ovšem nepřijatelná, a cílem návrhu zákona je umožnit státu disponovat takovými nástroji, které toto riziko sníží na akceptovatelnou úroveň. Návrh zákona si mj. dává za cíl přispět k výběru takových dodavatelů do strategicky významné infrastruktury, kteří při jakémkoli zjištění zranitelnosti či narušení dodávaného technologického řešení budou se svými odběrateli tyto informace ihned sdílet, flexibilně a transparentně postupovat při řešení a nápravě identifikovaných zranitelností a vynakládat úsilí k dosažení opětovného zabezpečení takových produktů či služeb.

Konkrétně prostřednictvím návrhu zákona dojde k plnění:

a) Bezpečnostní strategie ČR,[41] a to především při čelení hrozbám jako jsou kybernetické útoky či ohrožení funkčnosti a bezpečnosti komunikačních a informačních systémů, dodavatelských řetězců a kritické infrastruktury, včetně dodávek kritických surovin, potravin a energetických komodit.

b) Národní strategie kybernetické bezpečnosti,[42] konkrétně v provádění systematického a pečlivého hodnocení rizik, které zahrnuje technické i netechnické aspekty kybernetické bezpečnosti, které je nezbytné pro vytvoření a udržení skutečně odolné infrastruktury. Stěžejní otázkou v této problematice je pak bezpečnost dodavatelského řetězce, tedy nutnost zajistit, že externí subjekty a osoby mající vliv na nejdůležitější infrastrukturu státu nejsou z bezpečnostního hlediska rizikovými. Návrh zákona je i plněním konkrétního úkolu v Akčním plánu Národní strategie kybernetické bezpečnosti, který zní: *„Vytvořit návrh posuzování rizikového profilu dodavatelů na národní úrovni a uplatňování omezování vysoce rizikových dodavatelů do systémů regulovaných ZKB“*.

c) Národní strategie pro čelení hybridnímu působení,[43] konkrétně prostřednictvím posilování odolnosti státu a společnosti na základě komplexního, celospolečenského přístupu k bezpečnosti, jehož účelem je omezování zranitelností, jichž původci hybridního působení využívají. ČR dále taktéž touto právní úpravou bude posilovat schopnosti prvků kritické infrastruktury uchovávat svoji dostatečnou funkčnost pro případ svého vystavení hybridnímu působení. V neposlední řadě návrh zákona přispívá k snižování strategické závislosti ČR na zemích s odlišnou ideově-hodnotovou orientací. Taková závislost by mohla být zneužita v působení proti zájmům ČR.

d) Programového prohlášení vlády ČR,[44] a to při naplňování cílů *„Kritická infrastruktura bude stát na bezpečných, otevřených a auditovatelných*

[41] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. Bezpečnostní strategie České republiky. 2023. Dostupná zde: https://mocr.army.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_Ceske_republiky_2023.pdf

[42] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Národní strategie kybernetické bezpečnosti. Dostupná zde: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[43] MINISTERSTVO OBRANY ČR. Národní strategie pro čelení hybridnímu působení. Dostupná zde: https://mocr.army.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf

[44] VLÁDA ČR. Programové prohlášení vlády České republiky. 2022. Dostupné zde: https://www.vlada.cz/assets/jednani-vlady/programove-prohlaseni/programove-prohlaseni-vlady-Petra-Fialy.pdf

technologiích“ (…) (v části „Kybernetická bezpečnost“) a *„nedemokratickým státům nebyl umožněn přístup ke klíčové infrastruktuře ČR“.*

e) Souboru opatření EU pro bezpečnost sítí 5G[45] (tzv. EU 5G Toolboxu), a to zejména strategického opatření 03, jež požaduje stanovení rámce na národní úrovni k posouzení rizikového profilu dodavatelů a uplatňování omezování u dodavatelů považovaných za vysoce rizikové, včetně jejich vyloučení pro účinné zmírnění rizik v nezbytných případech, pokud jde o klíčová aktiva (dále jen „SM03“). Přijetím návrhu zákona bude ČR disponovat nástrojem, který SM03 naplní a zařadí se tak mezi další státy EU, jako je např. Německo.

f) Závěrů Rady EU o bezpečnosti dodavatelského řetězce IKT,[46] které vyzývají členské státy EU k posílení bezpečnosti dodavatelského řetězce IKT s cílem řešení hrozeb nežádoucí strategické závislosti v rámci dodavatelských řetězců IKT.

g) Strategického konceptu NATO,[47] zejména odstavce 26, který upozorňuje na důležitost identifikace a mitigace strategické závislosti a zranitelností mimo jiné ve své kritické infrastruktuře a dodavatelských řetězcích.

h) Článku 3 Severoatlantické smlouvy,[48] který uvádí, že zajištění bezpečného a odolného dodavatelského řetězce přispívá k plnění spojeneckého závazku rozvíjení kolektivních i individuálních kapacit ČR k odolávání jakékoli formě útoků, včetně těch kybernetických.

i) Tzv. Strengthened Resilience Commitment,[49] v němž se v roce 2021 členské státy NATO dohodly na závazku posílit odolnost s cílem neustále zvyšovat národní, kolektivní odolnost a civilní připravenost. Členské státy NATO se mimo jiné dohodly, že zvýší úsilí v zabezpečení a diverzifikaci dodavatelských řetězců a zajistí odolnost kritické infrastruktury a klíčových průmyslových odvětví.

j) Prague Proposals,[50] které upozorňují mimo jiné na důležitost provádění systematického a pečlivého posuzování rizik, jež je nezbytné pro vytvoření a udržení skutečně odolné infrastruktury. Takové posuzování zahrnuje technické i netechnické aspekty kybernetické bezpečnosti.

1.6.2. Návrh změnového zákona

Tak jako je cílem návrhu zákona úplná a správně provedená transpozice směrnice NIS 2, zavedení funkčního a efektivního mechanismu prověřování bezpečnosti dodavatelského řetězce a reflexe dosavadních poznatků s fungováním a praktickou použitelností stávajícího ZKB, je obecným cílem návrhu změnového zákona provést v českém právním řádu změny, které přispějí k naplnění výše uvedených cílů a odstranění nedostatků, které by obsah návrhu zákona bez dodatečných změn mohl v relevantních právních předpisech způsobit.

---

[45] NIS COOPERATION GROUP. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. 01/2020. Dostupné zde: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

[46] RADA EVROPSKÉ UNIE. Závěry Rady o bezpečnosti dodavatelského řetězce IKT. Říjen 2022. Dostupné zde: https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/cs/pdf

[47] NATO. NATO 2022 Strategic Concept. Dostupné zde: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

[48] NATO. Severoatlantická Smlouva. 1949. Dostupné zde: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=cs

[49] NATO. Strengthened Resilience Commitment. 2022. Dostupné z: https://www.nato.int/cps/en/natohq/official_texts_185340.htm

[50] PRAGUE 5G SECURITY CONFERENCE. The Prague Proposals. The Chairman Statement on cyber security of communication networks in a globally digitalized world. 2019. Dostupné z: https://www.nukib.cz/en/infoservis-en/conferences/prague-5g-security-conference-2019/

Cílovým stavem ve vztahu ke změnám jednotlivých právních předpisů je:

1.6.2.1. ZoISVS

Cílovým stavem je v oblasti regulace využívání cloud computingu orgány veřejné správy podle ZoISVS zachování kontinuity stávajícího procesu. Ten zahrnuje jednak přesun povinnosti zařadit informační systém veřejné správy, k jehož zajištění má být využit cloud computing včetně zmocnění k vydání vyhlášky, která tyto bezpečnostní úrovně stanoví, a dále přesun povinnosti orgánů veřejné správy zajistit dodržování bezpečnostních pravidel rovněž včetně zmocnění k vydání vyhlášky, která tyto bezpečnostní pravidla stanoví, do ZoISVS.

Ve vztahu k problematice dvojkolejnosti bezpečnostních opatření pro zajištění kybernetické bezpečnosti ze strany správců informačních systémů veřejné správy je nutno zrušit zmocnění Ministerstva vnitra stanovené § 5a ZoISVS, které Ministerstvo vnitra zmocňuje k vydání normy definující povinnosti týkající se bezpečnostních opatření pro zajištění kybernetické bezpečnosti správců informačních systémů veřejné správy. Dále je nutno v § 5b téhož právního předpisu stanovit množině osob povinných podle ZoISVS (nikoliv však podle návrhu zákona) povinnost dodržovat vyhlášku o povinnostech pro poskytovatele regulovaných služeb v nižším režimu přiměřeně, respektive přiměřeně zavádět bezpečnostní opatření v této vyhlášce obsažená.

Dalším z cílů je doplnění možnosti sankcionovat nedodržování některých povinností stanovených v ZoISVS, které se týkají cloud computingu. Za současného stavu se jedná o imperfektní normy a existuje pouze velmi omezený způsob, jak subjekty donutit k postupu v souladu se zákonem.

1.6.2.2. ZoPZI

Ustanovení tohoto zákona musí doznat takových změn, aby bylo dosaženo funkčního vymezení nového okruhu tzv. cílových osob, respektive aby došlo k doplnění okruhu cílových osob, které nejsou ovlivněny zrušením ZKB a přijetím návrhu zákona, o nový okruh cílových osob nahrazující dosavadní vymezení v § 7 písm. c). Tento okruh cílových osob je potřeba nastavit přiměřeným a dosavadnímu stavu co nejvíce odpovídajícím způsobem, aby byly zachovány v nejvyšší možné míře dosavadní nastavené procesy.

1.6.2.3. ZEK

Procesy obsažené v ZEK je potřeba upravit způsobem, který bude respektovat rozdělení agendy spadající věcně pod ČTÚ a pod Úřad za současného omezení možnosti, že budou adresáti ZEK zatíženi povinností plnit stejnou povinnost, v tomto případě hlášení, na oba úřady zároveň.

1.6.2.4. Zákon o poštovních službách

Podobně jako v případě ZEK, také v případě zákona o poštovních službách je potřeba docílit stavu, v němž budou procesy obsažené v zákoně o poštovních službách upraveny takovým způsobem, který bude respektovat rozdělení agendy spadající věcně pod ČTÚ a pod Úřad, opět za omezení možnosti, že budou adresáti této normy zatíženi povinností plnit stejnou povinnost vůči oběma úřadům zároveň.

1.6.2.5. Zvláštní zákony upravující povinnost mlčenlivosti a povinnost dodržet bankovní tajemství

Pokud jde o uvedené zákony (jmenovitě ZoB, ZPMS, AML, daňový řád, ZCS a ZoPZI), je potřeba docílit stavu, v němž bude dodržena legislativní zásada, že v taxativních výčtech obsažených v těchto předpisech jsou uvedeny jednotlivé případy poskytování informací ve vztahu k povinnosti mlčenlivosti a povinnosti dodržet bankovní tajemství bez dalšího.

1.7. Zhodnocení rizika spojeného s nečinností

Neprovedení transpozice směrnice do národního právního řádu by mohlo být Evropskou komisí považováno za nesplnění povinnosti vyplývající ČR z primárního práva EU (Smlouva o Evropské unii a Smlouva o fungování Evropské unie), přičemž by Evropská komise na základě čl. 258 Smlouvy o fungování Evropské unie mohla předložit tuto záležitost Soudnímu dvoru Evropské unie.

V souvislosti s mechanismem prověřování bezpečnosti dodavatelského řetězce je namístě uvést, že současný stav je nedostatečný a může způsobit závislost státu prostřednictvím strategicky významné infrastruktury na rizikových dodavatelích, což by v důsledku mohlo vést až k nenaplňování základních funkcí státu a ohrožení bezpečnosti ČR či vnitřního pořádku.

Při zachování současného stavu, v němž stát nemá nástroje k hodnocení a omezování rizik spojených s dodavateli do strategicky významné infrastruktury, by dodavatelé do této infrastruktury byli na základě proběhnuvšího dotazníkového šetření[51] i nadále vybíráni pouze na základě posouzení poskytovatelů strategicky významné služby, a tedy vyhodnocením kritérií souvisejících zejména s požadavky zákona o kybernetické bezpečnosti (resp. vyhlášky o kybernetické bezpečnosti) (41 % respondentů), cenou (14 % respondentů), kvalitou nabízeného řešení a technologickou způsobilostí dodavatele (44 % respondentů) a dalších požadavků zákona o veřejných zakázkách těmi orgány a osobami, které se tímto zákonem jsou povinni řídit.[52]

Nutno podotknout, že i správci strategicky významné infrastruktury vyhodnocují některá kritéria související s netechnickými aspekty dodavatelů či nabízených technických řešení. Jedná se zejména o posuzování a vyhodnocování kritérií souvisejících se sídlem dodavatele (zdali má dodavatel sídlo v zemi EU či NATO vyhodnocuje 73 % respondentů,[53] zdali dodavatel podléhá právním řádům zemí, na které veřejně upozorňují bezpečnostní instituce ČR vyhodnocuje 68 % respondentů[54]. Vlastnickou strukturu dodavatele zná a vyhodnocuje 80 % respondentů.[55] Zdali byl dodavatel pravomocně odsouzen pro trestný čin zajímá 56 % respondentů,[56] o poznání méně respondentů (44 %)[57] pak hodnotí, zdali je dodavatel pod výkonem účinné míry kontroly hospodářské činnosti cizího státu, resp. zdali dodavatel jedná eticky, v souladu s pravidly mezinárodního obchodu a s péčí řádného hospodáře (36 %)[58]. Další hrozby spojené s dodavatelským řetězcem jako hrozba nedodržení smluvního závazku ze strany dodavatele nevyhodnocuje 9 % respondentů,[59] hrozbu zneužití vnitřních prostředků či sabotáž nevyhodnocuje 19 % respondentů[60] a hrozbu použití

[51] Dotazníkové šetření bylo adresovaného všem orgánům a osobám podle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně Úřad vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. Úřad obdržel 65 takových odpovědí (dále jen „respondenti“).

[52] Na tento dotaz poskytlo vyhodnotitelnou odpověď 63 respondentů.

[53] Na tento dotaz poskytlo odpověď 64 respondentů.

[54] Na tento dotaz poskytlo odpověď 63 respondentů.

[55] Na tento dotaz poskytlo odpověď 64 respondentů.

[56] Na tento dotaz poskytlo odpověď 64 respondentů.

[57] Na tento dotaz poskytlo odpověď 62 respondentů.

[58] Na tento dotaz poskytlo odpověď 64 respondentů.

[59] Na tento dotaz poskytlo odpověď 64 respondentů.

[60] Na tento dotaz poskytlo odpověď 64 respondentů.

špionážních technik ze strany či prostřednictvím dodavatele nevyhodnocuje dokonce 40 % respondentů[61].

Posuzování a vyhodnocování takovýchto kritérií či hrozeb by ovšem i nadále zůstalo zcela na vůli a míře posouzení samotných správců strategicky významné infrastruktury a nebylo by vyžadováno, aby k posuzování takového typu kritérií docházelo. Absence posuzování strategických rizik plynoucích ze strany dodavatelů do významné strategické infrastruktury by tak nebyla výjimečná, a jelikož značná část dotázaných subjektů takovou analýzu neprovádí nyní, existuje velice nízká pravděpodobnost, že by došlo ke změně jejich přístupu k této problematice bez existence regulatorních nástrojů. V krajních případech by tak mohlo dojít k narušení až ochromení fungování některé strategicky významné infrastruktury, což by mělo celospolečenský dopad.

Dalším problémem současného stavu souvisejícím s bezpečností dodavatelského řetězce je to, že ačkoli podle výsledků dotazníkového šetření[62] respondenti smluvně zavazují své dodavatele k plnění požadavků na kybernetickou bezpečnost, pouze 80 % respondentů potvrdilo, že po dodavatelích vyžaduje plnění těchto požadavků i jejich subdodavateli. Ačkoli 92 % respondentů[63] získává informace i o subdodavatelích svých významných dodavatelů, pouze 5 % z nich získává informace o subdodavatelích 2. úrovně, přičemž žádný z respondentů nezískává informace o subdodavatelích 3. a další úrovně. V průměru má přitom každý významný dodavatel 4 až 5 subdodavatelů.[64]

Navíc pro identifikaci rizikovosti dodavatele je kromě vyhodnocení uvedených netechnických kritérií konkrétním dodavatelem nutné také zhodnocení dalších informací (vč. zpravodajských) o možných strategických hrozbách a rizicích spojených s konkrétním dodavatelem. Jedná se tedy o kritéria, která není schopen adekvátně vyhodnotit správce strategicky významné infrastruktury, a to ani pokud se o to vyhodnocováním alespoň dílčích aspektů sám pokouší. Z takového důvodu nejsou současné nástroje státu cílící na omezení rizika spojeného s rizikovými dodavateli dostatečná (více viz část 1.3. Popis existujícího právního stavu v dané oblasti).

Evropská agentura pro bezpečnost sítí a informací (dále jen „ENISA“) ve výroční zprávě Threat Landscape pro rok 2022,[65] která sleduje stav kybernetické bezpečnosti v zemích EU a identifikuje hlavní hrozby, trendy či aktéry útoků v této oblasti uvádí, že ve sledovaném období (červenec 2021–červenec 2022) byl opět pozorován nárůst tohoto typu útoků, přičemž se jednalo o druhý nejrozšířenější typ kompromitace. Ze zprávy dále vyplývá, že dochází k nárůstu útoků na dodavatelské řetězce státem podporovanými aktéry a zároveň rostou i jejich schopnosti a motivace. V souvislosti s válkou na Ukrajině se ukázalo, že geopolitický kontext má zcela zásadní dopad na operace v kyberprostoru a podle předpovědí ENISA bude tento trend nadále pokračovat. Zpráva zmiňuje i nárůst útoků na dodavatelský řetězec softwaru prostřednictvím kompromitace oblíbených softwarových balíčků, platforem nebo open-source knihoven pro vývoj softwaru. Útoky tohoto typu mohou mít podle ENISA zcela zásadní dopad v případě narušení kritických služeb nebo i služeb, které nejsou přímo zasaženy.

[61] Na tento dotaz poskytlo odpověď 62 respondentů.

[62] Dotazníkové šetření bylo adresovaného všem orgánům a osobám podle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně Úřad vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. Úřad obdržel 65 takových odpovědí (dále jen „respondenti“).

[63] Na tento dotaz poskytlo odpověď 63 respondentů.

[64] Na tento dotaz poskytlo odpověď 51 respondentů.

[65] ENISA. ENISA Threat Landscape 2022. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Konflikt na Ukrajině dále jasně poukazuje na důležitost pochopení bezpečnosti a odolnosti všech dodavatelů v našich strategicky důležitých dodavatelských řetězcích. V dnešním nejistém globalizovaném bezpečnostním prostředí lze rozumně předpokládat možné náhlé zhoršení vztahů s jakýmkoli státem, jehož zájmy nejsou v souladu se zájmy ČR či jejími spojenci. Je tedy důležité, aby stát měl nástroje pro omezení využívání dodavatelů s vazbami na takové státy. V případě eskalace vztahů či vzniku konfliktu by závislost strategicky významné infrastruktury na takových dodavatelích mohla mít pro ČR nepředstavitelné důsledky.

Další rizika spojená s nečinností jsou:

a) Vytvoření strategické hrozby státu v podobě závislosti na rizikových dodavatelích. V případě realizace hrozby by došlo k ohrožení strategicky významné infrastruktury, jejíž narušení by mohlo mít dopad na fungování celé ČR.

b) Existence nepředvídatelného prostředí a nejistota poskytovatelů strategicky významné služby, kteří ačkoli mají přehled z ostatních států o rizikovosti vybraných dodavatelů, mohou při výběru i nadále upřednostňovat jiné, zejména ekonomické aspekty nabízeného řešení, což je podněcováno zejména obavou z nekonkurenceschopnosti na trhu a taktéž podmínkami, které jim jsou v ČR nabízeny.

c) Reputační dopad ČR, kdy absence regulatorního rámce dodavatelů do strategicky významné infrastruktury bude řadit ČR mezi státy, jež zaostávají, a proto je důležité zachovat své jméno a vybudovat strategicky významnou infrastrukturu na bezpečném základu s adekvátně nastavenou regulací. Absence regulace bezpečnosti dodavatelského řetězce by tak v budoucnu mohla vést ke zhoršení pozice podnikatelských subjektů působících v ČR, které by nemohly nabídnout stejnou míru bezpečnosti svého produktu či služby jako subjekty ve státech, které obdobnou regulaci přijaly. Nepřijetí předmětné právní úpravy by tedy mohlo vyvolat nucené odmítání dodávek českých společností zahraničními odběrateli kvůli bezpečnostním a strategickým hrozbám plynoucím z dodávek subdodavatelů. České společnosti by se tím de facto staly nespolehlivými dodavateli pro zahraniční obchodní partnery, kteří by byli v takovém případě nucení svým národním legislativním systémem upřednostnit dodavatele ze zemí, které rizika dodavatelského řetězce legislativně ošetřují.

d) Vznik strategické hrozby v podobě závislosti na rizikových dodavatelích či přítomnosti technologií vysoce rizikových dodavatelů ICT ve strategické infrastruktuře. Může také dojít k omezení volnosti strategického rozhodování ČR, kdy bude nutné vzít v potaz možnost zneužití přítomnosti rizikových dodavatelů cizím státem.

e) Může docházet k výskytu vícero závažných zranitelností, a tím k navýšení počtu kybernetických incidentů a útoků ze strany států, které mohou zneužívat svého vlivu nad dodavateli operujícími pod jejich jurisdikcí. Tito dodavatelé poskytující hardware či software do strategické infrastruktury ČR mohou cíleně narušit důvěrnost, integritu a dostupnost dat.

f) Vznik nepřiměřených finančních dopadů pro ČR, jelikož náprava kybernetických incidentů s sebou může přinášet náklady pohybující se v řádech desítek miliónů až miliard korun. Dále je nutné zmínit nežádoucí finanční dopady spojené se situací, kdy může být nezbytné produkty strategicky rizikových dodavatelů bezodkladně nahradit až ve chvíli, kdy se již hrozba bezprostředně realizovala. A to navíc pouze v případě, že by takové odstranění bylo po technické, finanční a legislativní stránce

vůbec proveditelné. Časový rámec potřebný pro nahrazení pak navíc může násobně překračovat lhůtu pro efektivní reakci, což jen podtrhuje potřebu včasného a proaktivního řešení, nikoli až reakci ex post.

g) Sekundárně dochází k nepřímému financování států, které mohou tyto prostředky následně využívat pro narušování zájmů ČR a jejích spojenců. Tuto situaci lze pozorovat například při nákupu plynu či ropy pocházejících z RF, kdy jsou získané finance vynakládány na vedení ozbrojeného konfliktu na Ukrajině.

h) V neposlední řadě může docházet k poškození reputace ČR, která je dlouhodobě v Evropě považována za vedoucí stát v oblasti kybernetické bezpečnosti.

V neposlední řadě je zde při nečinnosti riziko, že neodstranění identifikovaných nedostatků zákona o kybernetické bezpečnosti by – v kombinací se snahou provést výše uvedenou transpozici směrnice do návrhu zákona prostřednictvím novelizace, a nikoli vytvořením zákona nového – mohlo způsobit systematické riziko a nemožnost zákon aplikovat správně. Výsledkem by opět bylo riziko nesprávného provedení směrnice.

2. Návrhy variant řešení

Návrh variant řešení pracuje s kombinací tří nejdůležitějších kroků, které byly identifikovány:

1. potřeba transpozice směrnice do českého právního řádu,
2. zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce do českého právního řádu v souladu s usnesením Bezpečnostní rady státu ze dne 21. června 2022 č. 41 a
3. odstranění zjištěných nedostatků (a s tím spojených přímo identifikovaných nedostatků, které by nastaly v případě transpozice směrnice bez dalších úprav) a reflexe dosavadních zkušeností.

S ohledem na to, že již předchozí právní úprava některé varianty úpravy regulace kybernetické bezpečnosti v ČR – řešení kybernetické bezpečnosti jen v rámci ochrany utajovaných systémů, řešení jen v rámci informačních systémů veřejné správy, nebo řešení metodou přímé regulace – přezkoumávala a následně je zavrhla, nepracuje s takovými variantami ani toto hodnocení.

2.1. Varianta I: Nulová varianta – zachování současného stavu

Nulová varianta spočívá v nepřijetí žádných úprav a nezasahování do současně platného právního stavu. Přijetí nulové varianty by pravděpodobně bylo Evropskou komisí považováno za nesplnění povinnosti vyplývající ČR z primárního práva EU (Smlouva o Evropské unii a Smlouva o fungování Evropské unie), přičemž by Evropská komise na základě čl. 258 Smlouvy o fungování Evropské unie mohla předložit tuto záležitost Soudnímu dvoru Evropské unie.

V souvislosti s nezavedením mechanismu prověřování bezpečnosti dodavatelského řetězce by varianta zachování současného stavu současně znamenala nečinit žádné legislativní změny směřující k omezení strategických bezpečnostních rizik spojených s důvěryhodností dodavatelů do strategicky významné infrastruktury. Zachování současného stavu bude i nadále podporovat existenci strategické hrozby v podobě závislosti na rizikových dodavatelích či přítomnosti technologií rizikových dodavatelů ICT ve strategicky významné infrastruktuře. Výběr dodavatelů do strategicky významné infrastruktury bude i nadále probíhat pouze na základě kritérií definovaných, posuzovaných a vyhodnocených správci této infrastruktury. Tento postup by byl v rozporu s výše uvedeným plánem legislativních prací vlády (viz část 1. Důvod předložení a cíle), a dále s výše uvedenými dokumenty, k jejichž plnění se ČR

přihlásila, a to např. Prague Proposals (viz část 1.5. Popis cílového stavu) či EU 5G Toolboxem (viz tamtéž).

2.2. Varianta II: Transpozice směrnice bez zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce a bez odstranění zjištěných nedostatků a reflexe dosavadních zkušeností (minimální transpozice směrnice)

Varianta II stanovující minimalistickou změnu zákona o kybernetické bezpečnosti pracuje se snahou splnit podmínky řádné transpozice směrnice do českého právního řádu s co nejmenším zásahem do zákona o kybernetické bezpečnosti, tedy i bez zásahů do jeho znění s cílem zohlednit dosavadní zjištěné nedostatky a reflektovat dosavadní zkušenosti s aplikací aktuálně účinné právní úpravy.

V této variantě tedy nedochází k zavedení mechanismu bezpečnosti dodavatelského řetězce, ani k odstranění zjištěných nedostatků a reflexi dosavadních poznatků.

Nové povinné osoby, jejich kritéria i další povinnosti plynoucí ze směrnice se v co nejvyšší míře aplikují v rámci stávajících institutů obsažených v zákoně o kybernetické bezpečnosti.

K nezavedení mechanismu prověřování bezpečnosti dodavatelského řetězce lze odkázat na předchozí výklad k variantě I.

2.3. Varianta III: Transpozice směrnice bez zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, ovšem při odstranění zjištěných nedostatků a reflexe dosavadních zkušeností

Varianta III pracuje se změnou zákona o kybernetické bezpečnosti, jejímž cílem je splnit podmínky řádné transpozice směrnice do českého právního řádu, zároveň se ovšem neomezovat pouze na rozsah toho, co je optikou směrnice skutečně nezbytné.

Tato varianta proto pracuje s tím, že nové povinné osoby, jejich kritéria i další povinnosti plynoucí ze směrnice budou zasazeny do nových institutů upravených návrhem zákona, které nejenže budou v minimální míře představovat transpozici požadavků směrnice NIS 2, ale budou také reflektovat dosavadní zkušenosti s aplikací obdobných institutů podle zákona o kybernetické bezpečnosti, resp. budou doplněny o instituty, jejichž zařazení do regulace je nezbytné pro racionalizaci celé právní úpravy. Vzniklý jednotící předpis bude srozumitelný pro adresáty a povede k zajištění bezpečného fungování informační společnosti ČR.

V této variantě tak v rámci návrhu zákona dochází oproti předchozím variantám k rozsáhlým a podstatným změnám, reprezentovaných především:

- sloučením dosavadních kategorií povinných osob do jedné nové kategorie „poskytovatele regulované služby“,
- celkovými změnami pojmosloví,
- úpravami celého procesu identifikace a registrace poskytovatele regulované služby,
- hlubším rozpracováním tzv. dvourychlostní kybernetické bezpečnosti, tedy přidělení různých povinností, resp. různé míry povinností regulovaným osobám na základě jejich režimu (základ tohoto ustanovení by ovšem musel být proveden i v případě předchozí varianty),
- reflexí zkušeností do úpravy dosavadních opatření, nově tzv. protiopatření,

- reflexí zkušeností do úpravy současného znění § 6a a § 15a zákona o kybernetické bezpečnosti,
- úpravou stavu kybernetického nebezpečí, nebo
- novou právní úpravou vzniku Portálu Úřadu.

K nezavedení mechanismu prověřování bezpečnosti dodavatelského řetězce lze odkázat na předchozí výklad k variantě I.

2.4. Varianta IV: Transpozice směrnice zároveň zohledňující mechanismus prověřování bezpečnosti dodavatelského řetězce, ovšem bez odstranění zjištěných nedostatků a reflexe dosavadních zkušeností

Varianta IV stanovující minimalistickou změnu zákona o kybernetické bezpečnosti pracuje se snahou splnit podmínky řádné transpozice směrnice do českého právního řádu s co nejmenším zásahem do zákona o kybernetické bezpečnosti, stejně jako je tomu ve variantě II.

V této variantě však dochází k zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, a to s následujícími podvariantami.

2.4.1. Podvarianta IVa: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře

Podvarianta IVa cílí na rozšíření pravomoci Úřadu v oblasti kybernetické bezpečnosti tak, aby byl zaveden komplexní mechanismus prověřování bezpečnosti dodavatelského řetězce do strategicky významné infrastruktury napříč sektory, včetně možnosti omezování či zákazu využití dodavatelů, kteří budou vyhodnoceni jako rizikoví či vysoce rizikoví. S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů navrhovaného řešení na veřejný i soukromý sektor, podvarianta IVa cílí na omezení dodavatelů pouze v kritických částech strategicky významné infrastruktury.

Strategicky významnou infrastrukturou se rozumí infrastruktura, kterou spravují poskytovatelé regulovaných služeb, kterým plynou povinnosti z mechanismu prověřování. Takovou kritickou částí systému je soubor aktiv regulovaného systému:

i) u kterých správce regulované služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací úrovní vysoká nebo kritická, nebo

ii) které zajišťují funkce regulovaného systému, stanovené prováděcím právním předpisem.

Dodavatelem, který může být omezen prostřednictvím mechanismu prověřování, pak bude pouze takový dodavatel, který poskytuje bezpečnostně významnou dodávku. Bezpečnostně významnou dodávkou se rozumí plnění, spočívající ve vývoji, výrobě, sestavení či servisu technického vybavení s výpočetní kapacitou nebo programového vybavení nebo ve vývoji, sestavení, poskytnutí či servisu informační či komunikační služby směřující do kritické části systému.

Úřad bude moci prověřovat současné i potenciální dodavatele poskytovatelů strategicky významné služby, a to z moci úřední. Rizikovost dodavatelů je posuzována na základě kritérií rizikovosti dodavatele (kritéria související se zemí, která má na dodavatele vliv, a kritéria související přímo s dodavatelem, jako je existence nekalých praktik či jednání v rozporu s pravidly hospodářské soutěže) směřují k prověření strategických bezpečnostních hrozeb, resp. strategických bezpečnostních rizik netechnického charakteru, vycházejících bezprostředně od osoby dodavatele a souvisejících s jeho aktivitami. Varování podle návrhu zákona

bude vydáno, vyhodnotí-li Úřad naplnění jednoho či více kritérií rizikovosti dodavatele, které může znamenat ohrožení bezpečnosti ČR nebo vnitřního pořádku. Zákaz využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu bude vydán prostřednictvím vydání OOP Úřadem, vyhodnotí-li státní orgány zapojené do prověřování dodavatelů ve vztahu k orgánu či osobě naplnění jednoho či více kritérií rizikovosti dodavatele, které může znamenat významné ohrožení bezpečnosti ČR nebo vnitřního pořádku.

Do procesu vydání OOP je zapojena i Bezpečnostní rada státu, některá ministerstva, další orgány a sektoroví regulátoři, a to dvojím způsobem.

V případě, že Úřad určí lhůtu pro zavedení omezení či vyloučení plnění v souladu s délkou odpisování podle právního předpisu upravujícího zdanění příjmů, členové Bezpečnostní rady státu dostanou v dostatečném předstihu návrh OOP obsahující omezení či vyloučení plnění ze strategicky významné služby pro informaci poté, co byl návrh předložen ostatním zapojeným orgánům státu, Ministerstvu financí, Českému telekomunikačnímu úřadu a Energetickému regulačnímu úřadu, pokud se OOP týká jejich působnosti.

V případě, že Úřad navrhne lhůtu kratší, než je uvedeno v předchozím odstavci, Úřad předloží návrh OOP po projednání podle předchozího odstavce ke schválení formou závazného stanoviska Ministerstvu průmyslu a obchodu, Ministerstvu zahraničních věcí a Ministerstvu vnitra. Důvodem pro tento postup je, že Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí a Ministerstvo vnitra zváží v případě navržení kratší lhůty proporcionalitu zásahu způsobeného návrhem OOP s ohledem na významné ohrožení bezpečnosti ČR nebo vnitřního pořádku ve srovnání s dalšími chráněnými hodnotami. Následně bude o tomto informována Bezpečnostní rada státu, jakožto pracovní orgán vlády v bezpečnostních otázkách.

Podvarianta IVa vychází z principů a hodnot zákona o kybernetické bezpečnosti. Respektuje tak v maximální možné míře stávající performativní povahu pravidel řízení dodavatelů a jiných ustanovení vyhlášky o kybernetické bezpečnosti a zaměřuje prověřování ze strany státu toliko na ty strategické aspekty důvěryhodnosti dodavatelů, jež poskytovatelé strategicky významné služby z podstaty své činnosti (a vzhledem k distribuci pravomocí mezi stát a soukromý sektor) nemohou provádět. Podvarianta IVa je založena na principu, že poskytovatelé strategicky významné služby budou povinni nahlašovat Úřadu dodavatele, kteří jim poskytují bezpečnostně významnou dodávku.

Rozdíl oproti podvariantě IVb spočívá v tom, že vláda ČR je zapojena do procesu zprostředkovaně, skrze svůj pracovní orgán, tj. Bezpečnostní radu státu. Neprovádí přímé posouzení omezení bezpečnostně významných dodávek, nýbrž proporcionálně hodnotí závěry, ke kterým došel Úřad a další orgány státu zapojené do procesu prověřování dodavatelů. Tím je zachována operativnost procesu a současně s tím je implementován dohledový a kontrolní mechanismus nad celým procesem.

Kontrolní činnost související s mechanismem prověřování je zařazena mezi standardní kontrolní činnost, kterou Úřad (Odbor kontroly) provádí, a jejíž systém i metodika je nastavená a fungující.

2.4.2. Podvarianta IVb: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře se zapojením vlády ČR

Podvarianta IVb je velice podobná podvariantě IVa. Zásadním rozdílem mezi těmito dvěma podvariantami je zapojení vlády ČR do procesu posuzování v případě podvarianty IVb. Na základě inspirace zákonem o prověřování zahraničních investic či zákona č. 1/2023 Sb., o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (dále jen „sankční zákon“), podvarianta IVb podmiňuje vydání opatření obecné

povahy stanovujícího podmínky či zakazující využití dodavatele přijetím usnesení vlády ČR v této věci. Na rozdíl od podvarianty IVa zde nedochází k zapojení ministerstev a sektorových regulátorů.

Posouzení případného omezení využívání bezpečnostně významných dodávek dodavatele z důvodu možného významného ohrožení bezpečnosti ČR nebo vnitřního pořádku by tak bylo přeneseno na nejvyšší politickou úroveň. Vládě ČR by přitom nebyly předkládány výstupy všech procesů prověřování k rozhodnutí. Taková prověření dodavatele, jejichž výstupem by nebylo možné významné ohrožení bezpečnosti ČR nebo vnitřního pořádku, by vládě ČR předkládána k projednání nebyla. Vláda ČR by tedy nebyla přetěžována projednáváním vysokého počtu výstupů prověřování dodavatelů a projednávala by pouze ty případy, u nichž by Úřad identifikoval možné významné ohrožení bezpečnosti ČR nebo vnitřního pořádku, a rozhodovala by o možném zákazu využívání plnění těchto dodavatelů do vymezené strategicky významné infrastruktury ČR.

V případě podvarianty IVb by nebyla prováděcím právním předpisem specifikována kritéria rizikovosti dodavatele, jelikož by sloužila pouze jako podpůrná vodítka pro prvotní vyhodnocení Úřadem a ostatních zapojených státních orgánů týkající se rizikovosti dodavatele. Úřad by shromáždil informace získané z vlastní činnosti, stejně tak jako informace obdržené od ostatních zapojených státních orgánů do procesu prověření. Následně by obdržené informace vyhodnotil a výsledky tohoto procesu předložil vládě ČR. Finální rozhodnutí o zákazu využívání plnění možného vysoce rizikového dodavatele pro dodávku bezpečnostně významných dodávek by ovšem bylo rozhodnutí politické. Toto rozhodnutí by provedla vláda ČR prostřednictvím svého usnesení, které by bylo prováděno na základě předložených podkladů od Úřadu, jež shromáždí z vlastní činnosti a z obdržených informací od ostatních státních orgánů zapojených do procesu prověřování.

2.4.3. Podvarianta IVc: Mechanismus plošného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře

Účelem tohoto přístupu je *ex ante* prověřování všech dodavatelů bezpečnostně významných dodávek. Hlavní rozdíl této podvarianty a podvarianty IVa spočívá v tom, že poskytovatelé strategicky významné služby by v případě volby této podvarianty pro bezpečnostně významné dodávky nemohli využít jiné než předem prověřené dodavatele. Dalším rozdílem je to, že prověřování by probíhalo na žádost přímého dodavatele ve správním řízení. Rozsah regulované infrastruktury i kritéria rizikovosti dodavatele by byly shodné s podvariantou IVa.

2.4.4. Podvarianta IVd: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce pouze v sektoru elektronických komunikací

Podvarianta IVd cílí na rozšíření pravomoci Úřadu v oblasti kybernetické bezpečnosti tak, aby byl zaveden komplexní mechanismus posuzování bezpečnostní spolehlivosti dodavatelů do strategicky významné infrastruktury toliko v sektoru elektronických komunikací, včetně možnosti omezování či zákazu využití dodavatelů, kteří budou vyhodnoceni jako rizikoví či vysoce rizikoví. Podvarianta vychází z předpokladu, že sektor elektronických komunikací, resp. sítě elektronických komunikací, představují kritickou infrastrukturu ČR, na jejichž dostupnosti je závislá celá řada služeb, stejně tak jako celá řada dalších odvětví. V současné době dochází k budování páté generace sítí elektronických komunikací (dále jen „5G sítě“). Význam této infrastruktury pro společnost je zcela zásadní a míra závislosti se v budoucnu bude nadále zvyšovat, a to zejména z důvodu digitalizace společnosti, vzniku nových technologií a jejich implementaci do nových ekosystémů. V této oblasti se ČR přihlásila také k celé řadě mezinárodních dokumentů, a to např. Prague Proposals či EU 5G Toolboxu (více viz část 1.5. Popis cílového stavu), jež mj. upozorňují na to, že předpokladem

pro bezpečné budování, zavádění a správu 5G sítí byla v dokumentu identifikována i důvěryhodnost dodavatele technologií. Hardware i software technologických řešení 5G sítí jsou již natolik komplexní, že snižovat rizika spojená s dodavateli 5G sítí pouze technickými prostředky je nedostatečné; zásadním faktorem je tudíž důvěryhodnost dodavatele. Významnou součástí kybernetické bezpečnosti 5G sítí je bezpečnost dodavatelského řetězce. V případě 5G sítí je z důvodu jejich vysoké komplexity a nákladnosti typickým fenoménem na trhu těchto technologií závislost odběratele, tedy subjektu budujícího a provozujícího 5G síť, na dodavateli technologie a jeho dodavatelském řetězci. Tato závislost s sebou přináší nové kybernetické hrozby a zvyšuje riziko spojené s některými stávajícími hrozbami, a to například možností implementovat do dodávaného technologického řešení zranitelnost, která umožňuje narušení důvěrnosti, dostupnosti nebo integrity přenášených dat. Důvěra v dodavatele a jím dodávaná technologická řešení je v tomto ohledu zásadní. Narušení kybernetické bezpečnosti 5G sítí, a to zejména jeho nejzávažnější případy, jako je narušení dostupnosti sítě ve velkém rozsahu vedoucí ke značným škodám, či kybernetická špionáž, představuje podstatný problém jak pro významné ekonomické zájmy a bezpečnost státu, tak pro operátory a jejich uživatele. Vzhledem k roli, jakou budou 5G sítě v následujících letech hrát v souvislosti s rozvojem nových technologií, komunikačních ekosystémů a zvyšováním počtu připojených zařízení, by mělo naplnění výše uvedených hrozeb zásadní celospolečenské důsledky. Dlouhodobě udržitelná bezpečnost a odolnost těchto sítí je proto strategickým zájmem státu i společnosti jako celku.

2.5. Varianta V: Transpozice směrnice, zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce a odstranění zjištěných nedostatků a reflexe dosavadních zkušeností

Varianta V pracuje se změnou zákona o kybernetické bezpečnosti, jejímž cílem je splnit podmínky řádné transpozice směrnice do českého právního řádu a zároveň se neomezovat pouze na rozsah toho, co je optikou směrnice skutečně nezbytné, stejně jako v případě varianty III.

Z toho důvodu i zde platí, že tato varianta pracuje s tím, že nové povinné osoby, jejich kritéria i další povinnosti plynoucí ze směrnice budou zasazeny no nových institutů upravených návrhem zákona, které nejenže budou v minimální míře představovat transpozici požadavků směrnice NIS 2, ale budou také reflektovat dosavadní zkušenosti s aplikací obdobných institutů podle zákona o kybernetické bezpečnosti, resp. budou doplněny o instituty, jejichž zařazení do regulace je nezbytné pro racionalizaci celé právní úpravy.

V této variantě tak v rámci úprav zákona dochází k rozsáhlým a podstatným změnám, reprezentovaným především:

- sloučením dosavadních kategorií povinných osob do jedné nové kategorie „poskytovatele regulované služby“,
- celkovými změnami pojmosloví,
- úpravami celého procesu identifikace a registrace poskytovatele regulované služby,
- hlubším rozpracováním tzv. dvourychlostní kybernetické bezpečnosti, tedy přidělení různých povinností, resp. různé míry povinností regulovaným osobám na základě jejich režimu (základ tohoto ustanovení by ovšem musel být proveden i v případě předchozí varianty),
- reflexí zkušeností do úpravy dosavadních opatření, nově tzv. protiopatření,
- reflexí zkušeností do úpravy § 6a a § 15a zákona o kybernetické bezpečnosti,

- úpravou stavu kybernetického nebezpečí nebo
- novou právní úpravou vzniku Portálu Úřadu.

V této variantě navíc také dochází k zohlednění mechanismu prověřování bezpečnosti dodavatelského řetězce, a to s následujícími podvariantami.

2.5.1. Podvarianta Va: Mechanismus prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře

Podvarianta Va cílí na rozšíření pravomoci Úřadu v oblasti kybernetické bezpečnosti tak, aby byl zaveden komplexní mechanismus prověřování bezpečnosti dodavatelského řetězce do strategicky významné infrastruktury napříč sektory, včetně možnosti omezování či zákazu využití dodavatelů, kteří budou vyhodnoceni jako rizikoví či vysoce rizikoví. S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů navrhovaného řešení na veřejný i soukromý sektor, podvarianta Va cílí na omezení dodavatelů pouze v kritických částech strategicky významné infrastruktury.

Strategicky významnou infrastrukturou se rozumí infrastruktura, kterou spravují poskytovatelé regulovaných služeb, kterým plynou povinnosti z mechanismu prověřování. Takovou kritickou částí systému je soubor aktiv regulovaného systému:

i) u kterých správce regulované služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací úrovní vysoká nebo kritická, nebo

ii) které zajišťují funkce regulovaného systému, stanovené prováděcím právním předpisem.

Dodavatelem, který může být omezen prostřednictvím mechanismu prověřování pak bude pouze takový dodavatel, který poskytuje bezpečnostně významnou dodávku. Bezpečnostně významnou dodávkou se rozumí plnění, spočívající ve vývoji, výrobě, sestavení či servisu technického vybavení s výpočetní kapacitou nebo programového vybavení nebo ve vývoji, sestavení, poskytnutí či servisu informační či komunikační služby směřující do kritické části systému.

Úřad bude moci prověřovat současné i potenciální dodavatele povinných osob mechanismu, a to z moci úřední. Rizikovost dodavatelů je posuzována na základě kritérií rizikovosti dodavatele (kritéria související se zemí, která má na dodavatele vliv, a kritéria související přímo s dodavatelem, jako je existence nekalých praktik či jednání v rozporu s pravidly hospodářské soutěže) směřují k prověření strategických bezpečnostních hrozeb, resp. strategických bezpečnostních rizik netechnického charakteru, vycházejících bezprostředně od osoby dodavatele a souvisejících s jeho aktivitami. Varování podle návrhu zákona bude vydáno, vyhodnotí-li Úřad naplnění jednoho či více kritérií rizikovosti dodavatele, které může znamenat ohrožení bezpečnosti ČR nebo vnitřního pořádku. Zákaz využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu bude vydán prostřednictvím vydání OOP Úřadem, vyhodnotí-li státní orgány zapojené do prověřování dodavatelů ve vztahu k orgánu či osobě naplnění jednoho či více kritérií rizikovosti dodavatele, které může znamenat významné ohrožení bezpečnosti ČR nebo vnitřního pořádku.

Do procesu vydání OOP je zapojena i Bezpečnostní rada státu, některá ministerstva, další orgány a sektoroví regulátoři, a to dvojím způsobem.

V případě, že Úřad určí lhůtu pro zavedení omezení či vyloučení plnění v souladu s délkou odpisování podle právního předpisu upravujícího zdanění příjmů, Bezpečnostní rada státu dostane v dostatečném předstihu návrh OOP obsahující omezení či vyloučení plnění ze strategicky významné služby pro informaci poté, co byl návrh předložen ostatním zapojeným

orgánům státu, Ministerstvu financí, Českému telekomunikačnímu úřadu a Energetickému regulačnímu úřadu, pokud se opatření obecné povahy týká jejich působnosti.

V případě, že Úřad navrhne lhůtu kratší, než je uvedeno v předchozím odstavci, tedy lhůta pro zohlednění zákazu obsaženého v návrhu opatření obecné povahy pro stávající či minulá plnění dodavatele bezpečnostně významné dodávky je kratší než stanovená doba odpisování podle právního předpisu upravujícího zdanění příjmu, pokud ji tento právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo je kratší než 5 let od pořízení bezpečnostně významné dodávky v případě, že ji právní předpis upravující zdanění příjmů ve vztahu k dotčené bezpečnostně významné dodávce nestanoví, pak Úřad předloží návrh OOP po projednání podle předchozího odstavce ke schválení formou závazného stanoviska Ministerstvu průmyslu a obchodu, Ministerstvu zahraničních věcí a Ministerstvu vnitra.

Důvodem pro tento postup je to, že Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí a Ministerstvo vnitra zváží v případě navržení kratší lhůty proporcionalitu zásahu způsobeného návrhem OOP s ohledem na významné ohrožení bezpečnosti ČR nebo vnitřního pořádku ve srovnání s dalšími chráněnými hodnotami. Následně bude informována Bezpečnostní rada státu, jakožto pracovní orgán vlády v bezpečnostních otázkách.

Podvarianta Va vychází z principů a hodnot zákona o kybernetické bezpečnosti. Respektuje tak v maximální možné míře stávající performativní povahu pravidel řízení dodavatelů a jiných ustanovení vyhlášky o kybernetické bezpečnosti a zaměřuje prověřování ze strany státu toliko na ty strategické aspekty důvěryhodnosti dodavatelů, jež poskytovatelé strategicky významné služby z podstaty své činnosti (a vzhledem k distribuci pravomocí mezi stát a soukromý sektor) nemohou provádět. Podvarianta Va je založena na principu, že poskytovatelé strategicky významné služby budou povinni nahlašovat Úřadu dodavatele, kteří jim poskytují bezpečnostně významnou dodávku.

Rozdíl oproti podvariantě Vb spočívá v tom, že vláda ČR je zapojena do procesu zprostředkovaně, skrze svůj pracovní orgán, tj. Bezpečnostní radu státu. Neprovádí přímé posouzení omezení bezpečnostně významných dodávek, nýbrž proporcionálně hodnotí závěry, ke kterým došel Úřad a další orgány státu zapojené do procesu prověřování dodavatelů. Tím je zachována operativnost procesu a současně s tím je implementován dohledový a kontrolní mechanismus nad celým procesem.

Kontrolní činnost související s mechanismem prověřování je zařazena mezi standardní kontrolní činnost, kterou Úřad (Odbor kontroly) provádí, a jejíž systém i metodika je nastavená a fungující.

2.5.2. Podvarianta Vb: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře se zapojením vlády ČR

Podvarianta Vb je velice podobná podvariantě Va. Jediným rozdílem mezi těmito dvěma podvariantami je to, že v případě nutnosti určit lhůtu pro omezení či vyřazení dodavatele z rozsahu strategicky významné služby ve lhůtě kratší, než by bylo stanoveno podle odpisové lhůty, nepředkládá Úřad ke schválení formou závazného stanoviska návrh OOP Ministerstvu průmyslu a obchodu, Ministerstvu zahraničních věcí a Ministerstvu vnitra, ale předkládá jej k projednání vládě ČR.

V případě, že Úřad určí lhůtu pro zavedení omezení či vyloučení plnění od dodavatele v souladu s délkou odpisování podle právního předpisu upravujícího zdanění příjmů, dostane i v této variantě Bezpečnostní rada státu v dostatečném předstihu návrh OOP obsahující omezení či vyloučení plnění do strategicky významné služby pro informaci, a to poté, co Úřad

návrh OOP projedná s ostatními orgány uvedenými v § 28 odst. 1 až 3, Ministerstvem financí, a v případě, že se návrh OOP dotýká jejich působnosti, s Českým telekomunikačním úřadem a Energetickým regulačním úřadem.

V případě, že Úřad navrhne lhůtu kratší, než je uvedeno v předchozím odstavci, tedy že lhůta pro zohlednění zákazu obsaženého v návrhu OOP pro stávající či minulá plnění dodavatele bezpečnostně významné dodávky je kratší než stanovená doba odpisování podle právního předpisu upravujícího zdanění příjmu, pokud ji tento právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo je kratší než 5 let od pořízení bezpečnostně významné dodávky v případě, že ji právní předpis upravující zdanění příjmů ve vztahu k dotčené bezpečnostně významné dodávce nestanoví, pak Úřad předloží návrh OOP po projednání podle předchozího odstavce k projednání vládě ČR. Vláda ČR poté uloží Úřadu, jakým způsobem bude Úřad ve věci návrhu OOP postupovat.

Tento postup má za cíl vládě ČR umožnit zvážit v případě navržení kratší lhůty proporcionalitu zásahu způsobeného návrhem OOP s ohledem na významnost ohrožení bezpečnosti ČR nebo vnitřního pořádku ve srovnání s dalšími chráněnými hodnotami. V případě kratší lhůty lze předpokládat dopady, které budou s ohledem na kratší lhůty hůře rozložitelné na zvládnutelnější segmenty. Tyto dopady lze předjímat jak u samotných poskytovatelů strategicky významných služeb, tak u strategicky významné služby jako takové. Ve velmi specifických případech lze očekávat i zvýšené riziko případné arbitráže. Je tudíž vhodné, aby do celého procesu byla zapojena přímo vláda ČR, která musí posoudit, jestli výhody pro bezpečnost ČR odpovídají případným rizikům plynoucím z tohoto postupu. Tato varianta je inspirována zavedeným procesem posuzování přímých zahraničních investic upravených ZoPZI či procesem zařazování subjektů na sankční seznamy upraveným sankčním zákonem.

Finální znění případného OOP by zůstalo s ohledem na proces vydávání OOP v rukou Úřadu (jedná se zejména o proces vypořádání se s připomínkami dotčených subjekt a potenciální udílení výjimek), nicméně vláda ČR bude mít konečné slovo v otázce, zdali představuje v takovém konkrétním případě využívání rizikového dodavatele dostatečné ohrožení bezpečnosti, aby odůvodnilo vydání OOP stanovující lhůtu pro plnění z něj vyplývajících povinností kratší, než je odpisová lhůta.

2.5.3. Podvarianta Vc: Mechanismus plošného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře

Účelem tohoto přístupu je *ex ante* prověřování všech dodavatelů vymezených dodávek do vymezené části regulované infrastruktury. Správci této infrastruktury by tak pro dané dodávky do dané strategické infrastruktury nemohli využít jiné než předem prověřené dodavatele. Rozsah regulované infrastruktury i kritéria rizikovosti dodavatele by byly shodné s podvariantou Va. Hlavní rozdíl této podvarianty a podvarianty Va je ten, že v podvariantě Vc prověřování probíhá na žádost přímého dodavatele ve správním řízení, přičemž prověřován není jenom žadatel – přímý dodavatel, který je smluvní stranou správce regulované strategické infrastruktury – nýbrž celý jeho relevantní dodavatelský řetězec.

2.5.4. Podvarianta Vd: Mechanismus prověřování bezpečnosti dodavatelského řetězce pouze v sektoru elektronických komunikací

Podvarianta Vd cílí na rozšíření pravomoci Úřadu v oblasti kybernetické bezpečnosti tak, aby byl zaveden komplexní mechanismus posuzování bezpečnostní spolehlivosti dodavatelů do strategicky významné infrastruktury toliko v sektoru elektronických komunikací, včetně možnosti omezování či zákazu využití dodavatelů, kteří budou vyhodnoceni jako rizikoví či vysoce rizikoví. Podvarianta vychází z předpokladu, že sektor elektronických komunikací, resp. sítě elektronických komunikací představují kritickou infrastrukturu

ČR, na jejichž dostupnosti je závislá celá řada služeb, stejně tak jako celá řada dalších odvětví. V současné době dochází k budování 5G sítí. Význam této infrastruktury pro společnost je zcela zásadní a míra závislosti se v budoucnu bude nadále zvyšovat, a to zejména z důvodu digitalizace společnosti, vzniku nových technologií a jejich implementaci do nových ekosystémů. V této oblasti se ČR přihlásila také k celé řadě mezinárodních dokumentů, a to např. Prague Proposals či EU 5G Toolboxu (více viz část 1.5. Popis cílového stavu), jež mj. upozorňují na to, že předpokladem pro bezpečné budování, zavádění a správu 5G sítí byla v dokumentu identifikována i důvěryhodnost dodavatele technologií. Hardware i software technologických řešení 5G sítí jsou již natolik komplexní, že snižovat rizika spojená s dodavateli 5G sítí pouze technickými prostředky je nedostatečné; zásadním faktorem je tudíž důvěryhodnost dodavatele. Významnou součástí kybernetické bezpečnosti 5G sítí je bezpečnost dodavatelského řetězce. V případě 5G sítí je z důvodu jejich vysoké komplexity a nákladnosti typickým fenoménem na trhu těchto technologií závislost odběratele, tedy subjektu budujícího a provozujícího 5G síť, na dodavateli technologie a jeho dodavatelském řetězci. Tato závislost s sebou přináší nové kybernetické hrozby a zvyšuje riziko spojené s některými stávajícími hrozbami, a to například možností implementovat do dodávaného technologického řešení zranitelnost, která umožňuje narušení důvěrnosti, dostupnosti nebo integrity přenášených dat. Důvěra v dodavatele a jím dodávaná technologická řešení je v tomto ohledu zásadní. Narušení kybernetické bezpečnosti 5G sítí, a to zejména jeho nejzávažnější případy, jako je narušení dostupnosti sítě ve velkém rozsahu vedoucí ke značným škodám, či kybernetická špionáž, představuje podstatný problém jak pro významné ekonomické zájmy a bezpečnost státu, tak pro operátory a jejich uživatele. Vzhledem k roli, jakou budou 5G sítě v následujících letech hrát v souvislosti s rozvojem nových technologií, komunikačních ekosystémů a zvyšováním počtu připojených zařízení, by mělo naplnění výše uvedených hrozeb zásadní celospolečenské důsledky. Dlouhodobě udržitelná bezpečnost a odolnost těchto sítí je proto strategickým zájmem státu i společnosti jako celku.

3. Vyhodnocení nákladů a přínosů

3.1. Identifikace nákladů a přínosů

Před odlišením a identifikací nákladů a přínosů jednotlivých variant je vhodné uvést hodnocení nákladů a přínosů regulace kybernetické bezpečnosti jako celku.

Jak již uvádělo odůvodnění prvního znění zákona o kybernetické bezpečnosti, na které se dá v obecnosti stále plně odvolat, protože ani po letech nepozbylo svou platnost, ekonomické hodnocení přínosů jednotlivých variant představuje obtížné zadání, neboť dominantní přínos, který je navrhovanou právní úpravou sledován, spočívá v eliminaci nebo omezení bezpečnostních rizik a posílení základních aspektů fungování informační společnosti. Rizika plynoucí z kybernetických bezpečnostních incidentů nemají dominantně ekonomický charakter, neboť spočívají v zajištění nedistributivních práv (veřejných statků), k jejichž ochraně je legitimován a povinen stát.

Jen velmi těžko se v ekonomických termínech dá vyjádřit zvýšení bezpečnosti např. v případě výkonu práva na svobodu projevu nebo práva na informační sebeurčení. Podobně obtížná je kvantifikace přínosů návrhu zákona, pokud jde o subsidiární efekty, např. o zvýšení důvěry občana ve stát a jeho instituce nebo ve fungování moderních informačních a komunikačních technologií. V situaci, kdy je stále větší část veřejné agendy včetně kontaktu s občany realizována prostřednictvím informačních a komunikačních technologií, je pak navíc bezpečnost kybernetického prostoru, v němž se tyto veřejnoprávní informační transakce odehrávají, tím přínosnější, čím větší procento veřejnoprávní komunikace je realizováno elektronicky.

Informační a komunikační technologie se kromě výkonu veřejné správy významně podílejí též na fungování jiných společenských funkcionalit, z nichž některé mají pro život člověka a společnosti zásadní význam. Systémy zajišťují chod energetických sítí, zásobování obyvatelstva životně důležitými komoditami, fungování vitálně důležitých institucí např. v oborech ochrany veřejného zdraví, ochrany životního prostředí, dopravy, ale také v celé řadě dalších. Přínosem sledovaným u shora popsaných variant (varianty II a následujících) je tedy i zvýšení bezpečnosti důležitých společenských funkcionalit.

Uvedené neznamená, že by přínosy shora popsaných variant neměly vůbec ekonomický aspekt nebo finanční dopad – již původní odůvodnění prvního znění zákona o kybernetické bezpečnosti však nepovažovalo za vhodné předřazovat tyto ekonomické efekty před společenské přínosy.

Mezi čistě ekonomické přínosy může patřit snížení škodlivých následků kybernetických bezpečnostních incidentů, tj. snížení míry ekonomických škod, které tyto incidenty způsobují. Čím kvalitnější bude ochrana kybernetického prostoru před výskytem takového incidentu, tím může být realizovaný incident méně intenzivní, a tím rychleji dochází k vyrovnání se s jeho následky. U služeb informační společnosti realizovaných v kybernetickém prostoru přitom platí, že kvůli jejich permanentnímu charakteru dochází k ekonomickým ztrátám vždy, pokud služba není pro jejich uživatele technicky dostupná.

Dalším ekonomickým efektem shora popsaných variant může být zvýšená míra motivace tuzemských a zahraničních investic do informačních a komunikačních technologií. Díky tomu, že v ČR působí špičková univerzitní a vědecká pracoviště, je zde realizována celá řada úspěšných investičních či inkubačních projektů zaměřených na pokročilé informační a komunikační technologie. Adekvátní zabezpečení kybernetického prostoru může v tomto směru posloužit k další pozitivní motivaci investorů (zatímco opomenutí této agendy může naopak investory utvrzovat v názoru, že informační a komunikační technologie nepředstavují pro ČR odpovídající prioritu).

V situaci, kdy se stát rozhodne aktivně přispět ke zvýšení kybernetické bezpečnosti, je pak možno sledovat i další ekonomický přínos, a to nepřímou podporu tuzemských komerčních produktů v oblasti kybernetické bezpečnosti. Vedle toho, že stát má mít tendence primárně využít domácích zdrojů a technologií a veřejnými investicemi podporovat jejich tvůrce a investory, má užití těchto technologií i významný marketingový efekt. V bezpečnostních oborech totiž platí, že užití určité bezpečnostní technologie na domácím trhu dodavatele je vnímáno jako důležitý předpoklad úspěchu této technologie v zahraničí. Stát, který se v oblasti kybernetické bezpečnosti buďto vůbec neangažuje, nebo preferuje zahraniční technologická řešení, tedy vlastním vývojářům a investorům těchto technologií příliš nepomáhá.

Nepřímá podpora tuzemských komerčních produktů v oblasti kybernetické bezpečnosti má vliv i na chování investorů v jiných oblastech. Faktorem sledovaným mezinárodními investory při rozhodování o umístění investičních akcí nejsou jen otázky daňové, finanční nebo otázky dopravní dostupnosti, vzdělanosti, pracovních sil nebo bezpečnosti místního právního prostředí, ale též fungující informační a komunikační infrastruktura. Přestože bezpečně fungující kybernetický prostor nemusí být u investorů mimo obory ICT dominantním faktorem pro jejich rozhodování o místě, typu a výši investic, úroveň kybernetické bezpečnosti ve státě tvoří nesporně jeden z důležitých aspektů jejich ekonomických analýz.

Z právě uvedeného nepřímo plyne i další přínos, který je možno u shora popsaných variant sledovat, a který se týká podpory konkurenceschopnosti tuzemských podniků působících na trhu služeb informační společnosti. Je-li v dnešní době běžné, že čeští podnikatelé oslovují prostřednictvím služeb informační společnosti zákazníky v zahraničí,

je nasnadě, že bezpečné a fungující služby informační společnosti v rámci ČR mají na rozvoj takového podnikání pozitivní vliv. Státy s fungujícím systémem kybernetické bezpečnosti mohou svým podnikatelům nabídnout v porovnání se státy, které tuto problematiku neřeší, bezpečnější prostředí nejen k realizaci tuzemských obchodů, ale též k mezinárodní expanzi.

Typologii přínosů sledovaných u shora popsaných variant lze tedy shrnout následovně:

- zvýšení míry ochrany práva na informační sebeurčení, práva na svobodu projevu a dalších informačních práv člověka,
- zvýšení míry ochrany důvěry člověka ve stát a jeho instituce,
- zvýšení míry bezpečnosti důležitých společenských funkcionalit,
- omezení ekonomických škod jako důsledků kybernetických bezpečnostních incidentů,
- zvýšení atraktivity ČR pro investory v oboru ICT,
- podpora českých dodavatelů bezpečnostních ICT technologií,
- obecné zvýšení atraktivity ČR pro zahraniční a tuzemské investory,
- zvýšení konkurenceschopnosti tuzemských podnikatelů využívajících ICT k podnikání na evropském nebo mezinárodním trhu.

Zachování nebo dosažení výše uvedeného je tak měřítkem při hodnocení přínosů jednotlivých variant níže.

V otázce nákladů, především optikou jednotlivých variant, je potřeba si uvědomit, že podstata nových požadavků spočívá v nutnosti řádně transponovat směrnici do českého právního řádu. Hlavními body zvyšujícími ekonomickou náročnost návrhu zákona jsou jak rozsah úpravy, tak nutnost vztáhnout regulaci na službu, a nikoli na konkrétní systém. Vedle požadavků směrnice generují významnou část nákladů také procesy spojené se zavedením mechanismu prověřování bezpečnosti dodavatelského řetězce – zejména varianty IV a V. Náklady spojené s dalšími úpravami návrhu zákona ve variantách III a V již podstatné náklady oproti předchozím dvěma negenerují a v některých případech mají naopak tendenci náklady snižovat.

Plnění požadavků ze zákona o kybernetické bezpečnosti – ať už jeho současného znění, nebo ze znění návrhu zákona – je kontinuální proces. Vybrané organizace veřejného i soukromého práva jsou povinny zabezpečovat své systémy v souladu se zákonnými požadavky již nyní, a tuto povinnost budou mít i do budoucna (zahrnutí současných regulovaných osob a podstatné rozšíření regulace je základním požadavkem směrnice, a proto s touto změnou pracují všechny varianty s výjimkou varianty nulové). Ekonomické dopady spojené s těmito subjekty je třeba analyzovat spíše ve vztahu ke změněné šíři regulace v rámci dané organizace. Uvedené varianty provazují – v souladu s požadavkem směrnice – regulaci nikoli s konkrétními informačními systémy, ale se službou, kterou organizace poskytuje.

Problematickým prvkem analýzy finančních dopadů na organizace je skutečnost, že distribuce nákladů na kybernetickou bezpečnost není plošná a existuje naprostá informační asymetrie ve směru od regulovaných subjektů k regulačnímu orgánu (jen regulovaná organizace samotná je schopna identifikovat její vlastní náklady na zavedení a udržování přiměřené úrovně kybernetické bezpečnosti).

Výši finančních dopadů není možné předem stanovit a veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídající hodnotou.

Distribuce nákladů na kybernetickou bezpečnost není plošná z důvodu velkého počtu neznámých a proměnlivých indikátorů:

- aktuální stav zabezpečení každé jedné organizace,
- různý cílový stav každé organizace související s významností její činnosti a potřebou zajistit její fungování,
- široká variabilita rozsahu opatření na zajištění kybernetické bezpečnosti, která může být naprosto odlišná u jednotlivých organizací,
- identifikace toho, co je nákladem na zajištění kybernetické bezpečnosti, a co je nákladem na běžný provoz informačních a komunikačních technologií u daného subjektu (tyto množiny se velmi prolínají),
- soulad se zákonem o kybernetické bezpečnosti,
- neznámý přesný počet výsledných regulovaných subjektů,
- nepředvídatelnost rozsahu zasažených odvětví a opatření k řešení stavu kybernetického nebezpečí, dokud nevznikne hrozba v oblasti kybernetické bezpečnosti, případně dokud nebude aktivován její zdroj nebo nenastane kybernetický bezpečnostní incident, na základě kterého budou opatření k řešení stavu kybernetického nebezpečí nařizována,
- proměnlivost nákladů v čase související jak s makroekonomickými otázkami, tak s vývojem technologií a mnoho dalších indikátorů.

Tyto indikátory jsou bohužel spjaty se systémem zajištění kybernetické bezpečnosti, ať už podle zákona o kybernetické bezpečnosti, návrhu zákona, tak i z obecně přijímaných norem upravujících kybernetickou bezpečnost.

Pro stanovení alespoň orientačního výpočtu nákladů lze vzít v úvahu následující indikátory. Je vhodné také uvést, že jak vyplývá z metodiky některých z níže citovaných zdrojů, podstatou některých výpočtů uvedených níže byl proces obdobný tomu uvedenému v Metodice měření a přeměřování administrativní zátěže podnikatelů Ministerstva průmyslu a obchodu.

3.1.1. Výpočet nákladů podle návrhu novelizace zákona o kybernetické bezpečnosti (2017)

Odůvodnění komplexní novelizace zákona o kybernetické bezpečnosti (2017) pracovalo s premisou, že v nejvyšší kategorii regulovaných subjektů mají všechny subjekty shodné povinnosti. Do této kategorie byly zařazeny i tehdy nově přidané subjekty (provozovatelé základní služby). Bylo proto možné dovodit, že náklady vzniklé nově regulovaným subjektům budou srovnatelné s těmi, které se zaváděním povinností měly již regulované subjekty. Z tehdy získaných dat vyplynulo, že souhrnné náklady na zavádění technických opatření podle zákona o kybernetické bezpečnosti činily na 77 systémů kritické informační infrastruktury a významných informačních systémů téměř 95 000 000 Kč. K provádění organizačních opatření podle zákona o kybernetické bezpečnosti pak bylo podle správců vydáno celkem 23 000 000 Kč na zmíněných 77 systémů. Tyto náklady byly počítány za první rok od určení, tj. ve lhůtě stanovené pro zavádění bezpečnostních opatření. Bylo tedy možné shrnout, že průměrně náklady na zavedení technických opatření na jeden významný informační systém nebo informační nebo komunikační systém kritické informační infrastruktury činí přibližně 1 233 000 Kč, průměrné náklady na zavedení organizační opatření pak vycházejí na cca 300 000 Kč. Důvodová zpráva již tehdy uváděla, že jde o velmi hrubé odhady, neboť někteří správci nebyli schopni náklady na zavádění zákonných opatření přesně vyčíslit. V rámci důvodové zprávy se také uváděl výsledek dotazníkového průzkumu prováděného mezi členy Pracovní skupiny I[66], ze kterého vyplynulo, že v závislosti na provádění povinností uložených zákonem o kybernetické bezpečnosti je zabezpečení informačních systémů hodnoceno jako

[66] Pracovní skupina I byla vytvořena v únoru 2016 pro transpozici směrnice NIS 1 na resortní úrovni.

poměrně vysoké, přičemž náklady na doplnění bezpečnostních opatření na úroveň stanovenou pro správce a provozovatele informačního systému základní služby by činily v průměru na jeden subjekt cca 6 000 000 Kč, pokud by požadovaná úroveň zabezpečení byla nastavena na úrovni významných informačních systémů, nebo cca 11 500 000 Kč, pokud by byla požadována stejná úroveň zabezpečení jako pro kritickou informační infrastrukturu.

3.1.2. Výpočet nákladů podle návrhu novelizace vyhlášky o významných informačních systémech (2019)

Při zpracovávání hodnocení dopadů regulace k vyhlášce o významných informačních systémech (v roce 2019) došlo k orientačnímu výpočtu nákladů na zabezpečení jednoho typového informačního systému ve veřejné správě, a to na základě tou dobou dostupných dat a průzkumu mezi vybranými regulovanými osobami. Pro ilustraci může sloužit, že se jednalo o částku 821 000 Kč na jeden informační systém (tedy cca 50 % z odhadu výpočtu nákladů podle návrhu novelizace zákona o kybernetické bezpečnosti z roku 2017, a jen cca 13 % vůči výsledku dotazníkového průzkumu mezi členy Pracovní skupiny I). Počet takových jednotlivých systémů, které bude nutno v rámci organizací zabezpečit podle návrhu zákona, však může být v rámci jednotlivých organizací velmi různorodý v závislosti na jejich velikosti.

3.1.3. Výpočet nákladů podle Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2021)

Evropská agentura pro bezpečnost sítí a informací (ENISA) je agentura EU zřízená pro věci kybernetické bezpečnosti. Od roku 2020 zpracovává ENISA každoroční zprávu o výši investic povinných osob spadajících pod směrnici NIS do kybernetické bezpečnosti a vliv povinností plynoucích ze směrnice na výši těchto investic. Relevantní informace do této zprávy poskytují stovky organizací ze všech členských států EU.

Cílem zprávy je zdokumentovat, jak regulované subjekty v odvětvích stanovených původní směrnicí NIS investují do kybernetické bezpečnosti a jak plní cíle stanovené ve směrnici. Spolu s tím se také zaměřuje na další aspekty, jakými jsou certifikace, kybernetické pojištění a organizace bezpečnosti informací u těchto organizací.

Zpráva z roku 2021 (za rok 2020) vychází ze specializovaného průzkumu trhu provedeného mezi 947 organizacemi – s minimálně 35 organizacemi z každého členského státu, které byly identifikovány jako povinné osoby podle původní směrnice NIS. Kvantitativní ukazatele v průzkumu byly analyzovány na základě mediánu i průměru (mediánová hodnota by měla být považována za typickou hodnotu).

Jak závěry zprávy uvádějí, typický povinný subjekt v EU vynakládá na implementaci požadavků směrnice NIS 40 000 EUR, tedy cca 1 000 000 Kč (hodnota je medián). Průměrná hodnota činila 98 000 EUR (cca 2 400 000 Kč). V ČR se jedná podle zprávy průměrně o částku 60 000 EUR (cca 1 500 000 Kč).

3.1.4. Výpočet nákladů podle Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2022)

Zpráva za rok 2021 (z roku 2022) navazuje na výše uvedenou zprávu za rok 2020 a vychází ze specializovaného průzkumu trhu provedeného mezi 1080 organizacemi.

Jak závěry zprávy uvádějí, celkově se zdá, že řada absolutních hodnot, jako jsou rozpočty na IT a informační bezpečnost nebo procento nákladů v rámci rozpočtů na IT vynaložených na bezpečnost, je ve srovnání s předchozím rokem výrazně nižší. Podle Zprávy lze toto však přičíst složení vzorku pro průzkum a vyššímu zastoupení provozovatelů

základní služby ze sektorů energetiky a zdravotnictví v důsledku nových sektorových výzev, ale také k makroekonomickému prostředí, např. dopad COVID-19 na příslušné rozpočty.

Medián nákladů na bezpečnost vynaložených v rámci IT rozpočtů je 6,7 %, což je o jeden procentní bod méně než v předchozím roce. Velcí provozovatelé investují do ICT výrazně více než menší provozovatelé. Odhadované přímé náklady na závažný bezpečnostní incident činí v průměru 200 000 EUR (cca 4 900 000 Kč), což je dvakrát více než v předchozím roce, což naznačuje nárůst nákladů na incidenty. Zdravotnictví a bankovnictví zůstávají na prvních dvou místech z hlediska nákladů na incidenty. Pouze 27 % dotázaných provozovatelů základní služby v sektoru zdravotnictví má specializovaný program na obranu proti ransomware a 40 % dotázaných nemá žádný program zvyšování povědomí o bezpečnosti pro zaměstnance mimo IT.

Zpráva za rok 2021 konkrétní náklady na implementaci požadavků směrnice NIS pro typický povinný subjekt v EU již neuvádí. Medián výdajů na IT u dotazovaných organizací činil ve zkoumaném roce 10 000 000 EUR (cca 245 000 000 Kč), průměrná hodnota výdajů na IT byla ve stejném období 60 000 000 EUR (cca 1 470 000 000 Kč). Medián výdajů na bezpečnost informací podle stejných kritérií činil 600 000 EUR (14 600 000 Kč), průměrná hodnota výdajů byla 4 000 000 EUR (97 000 000 Kč).

Na základě všech výše uvedených výpočtů a metodik je možné konstatovat, že v případě výpočtu nákladů na zavedení a následné provádění především bezpečnostních opatření se jedná o velmi hrubé odhady, pohybující se přibližně mezi 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému. Změny v přístupu k regulaci zavedené směrnicí NIS 2, výše uvedené proměnné (především různý stav současného zabezpečení u regulovaných organizací), rozdělení povinností uložených těmto subjektům, stejně jako agregace řady bezpečnostních opatření u více systémů v rámci organizace, mohou tyto hodnoty ovlivnit, nicméně s ohledem na výše uvedené je možné očekávat požadavky na veřejné rozpočty v této přibližné míře (v souladu s postupem uvedeným v části 3.1 Shrnutí závěrečné zprávy RIA). Podstatnou proměnnou bude především to, jaký je počet systémů u regulované organizace.

3.2. Náklady

3.2.1. Varianta I: Nulová varianta – zachování současného stavu

Mezi náklady na nulovou variantu lze řadit náklady za případná řízení před orgány EU, neboť přijetí nulové varianty by pravděpodobně bylo Evropskou komisí považováno za nesplnění povinnosti vyplývající ČR z primárního práva EU (Smlouva o Evropské unii a Smlouva o fungování Evropské unie), přičemž by Evropská komise na základě čl. 258 Smlouvy o fungování Evropské unie mohla předložit tuto záležitost Soudnímu dvoru Evropské unie.

Pokud jde o mechanismus prověřování bezpečnosti dodavatelského řetězce, nepřijetí legislativních změn může přinést náklady spojené s náhradou či nápravou škod, které by vyplynuly z činnosti rizikového dodavatele, jenž by poškodil významnou strategickou infrastrukturu ČR.

V první řade je nutné zmínit nevyčíslitelnou strategickou hrozbu v podobě závislosti na rizikových dodavatelích či přítomnosti technologií vysoce rizikových dodavatelů ICT v této infrastruktuře. Může také dojít k omezení volnosti strategického rozhodování ČR, neboť bude nutné vzít v potaz možnost zneužití přítomnosti rizikových dodavatelů cizím státem, což může zamezit strategické autonomii ČR.

Dále lze identifikovat vznik nepřiměřených finančních dopadů pro ČR a subjekty působící v její jurisdikci, které se pohybují v řádech miliónů korun. Tyto náklady jsou spojené se sanací kybernetických incidentů, a to na základě možného výskytu vícero závažných

zranitelností a souvisejícího navýšení počtu kybernetických incidentů a útoků např. ze strany států nebo státem sponzorovaných kriminálních aktérů, kteří mohou zneužívat svého vlivu nad dodavateli operujícími pod jejich jurisdikcí. Tito dodavatelé poskytující hardware či software do strategické infrastruktury ČR mohou cíleně narušit důvěrnost, integritu a dostupnost dat. Mezi náklady spojené s nulovou variantou by mohly dále náležet škody způsobené nečinností státu v oblasti zajišťování kybernetické bezpečnosti ze strany rizikových dodavatelů.

Z veřejně dostupných informací a dat např. vyplývá, že škody kybernetického útoku na nemocnici Rudolfa a Stefanie Benešov z roku 2019 byly vyčísleny na více než 23 milionů Kč,[67] kybernetický útok na Fakultní nemocnici Brno z roku 2020 měl za důsledek škody v řádech desítek milionů Kč[68]. Kybernetický útok v roce 2022 na Ředitelství silnic a dálnic způsobil škody v minimální hodnotě 30 milionů Kč[69]. Finanční škody ovšem nejsou jedinými dopady kybernetických útoků na strategickou infrastrukturu státu. Nemocnice využívají pokročilé technologie a IT systémy pro monitorování pacientů, provoz lékařských zařízení a správu elektronických zdravotních záznamů. Kybernetický útok, který tyto systémy naruší, může vést k selhání životně důležitého vybavení nebo k přerušení poskytování zdravotní péče, což může mít přímý dopad na životy pacientů. Kromě toho je třeba si uvědomit, že těžko vyčíslitelná, avšak neopominutelná, je i úplná ztráta citlivých dat, ke které v důsledku kybernetického útoku nezřídka dochází. Zdravotnická zařízení uchovávají obrovské množství citlivých informací o pacientech, včetně jejich zdravotní historie, osobních údajů a finančních informací. Únik těchto dat může vést k vážným narušením soukromí a potenciálnímu zneužití osobních informací.

3.2.1.1. Náklady na řešení kybernetických incidentů

Kybernetické incidenty mohou mít značné ekonomické dopady na různé sektory v ČR. Bez účinných bezpečnostních opatření mohou incidenty způsobit vysoké finanční ztráty, narušení provozu a ztrátu důvěry zákazníků. Podniky by musely investovat více prostředků do obnovy a řešení škod, což by mohlo vést k vyšším cenám jejich produktů a služeb. Navíc by absence regulace mohla ohrozit strategickou autonomii a reputaci státu na mezinárodní úrovni.

Podle zprávy "Cost of a Data Breach Report 2023" od IBM Security dosáhly průměrné globální náklady na únik dat rekordní výše 4,45 milionu USD, tedy 103,5 milionu Kč. To zároveň představuje nárůst o 15 % za poslední tři roky.[70] Nejvyšší průměrné náklady byly zaznamenány v sektoru zdravotnictví (10,93 milionu USD, tedy cca 254 milionu Kč). Kybernetické incidenty nejčastěji způsobují phishing a kompromitace přihlašovacích údajů.[71] Náklady na řešení kybernetických incidentů zahrnují přímé finanční ztráty, náklady na obnovu dat a technickou podporu, ale také nepřímé náklady jako ztráta důvěry a reputace, právní následky a ztráty v důsledku přerušení provozu. Průměrná doba k identifikaci úniku dat byla 207 dní a průměrná doba k jeho omezení byla 70 dní. Tyto dlouhé doby naznačují nedostatečnou připravenost a potřebu rychlých a účinných bezpečnostních opatření. Firmy

[67] ČTK. Benešovská nemocnice získá 12,5 milionů na úhradu nákladů spojených s kyberútokem. Dostupné z: https://www.seznamzpravy.cz/clanek/regiony-zpravy-stredocesky-kraj-benesovska-nemocnice-ziska-125-milionu-na-uhradu-nakladu-spojenych-s-kyberutokem-182158

[68] ČTK, IDNES.CZ. Kybernetický útok stál nemocnici v Brně desítky milionů, klesly odběry krve. Dostupné z: https://www.idnes.cz/brno/zpravy/fakultni-nemocnice-brno-kyberneticky-utok-skody-odber-krve.A200417_093436_brno-zpravy_krut

[69] ČTK. Obnova systémů ŘSD po kyberútoku stála desítky milionů. Brzy má opět fungovat i web s dopravními informacemi. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3518463-obnova-systemu-rsd-po-kyberutoku-stala-desitky-milionu-brzy-ma-opet-fungovat-i-web-s

[70] IBM Investing now can save millions. Dostupné z: https://www.ibm.com/reports/data-breach

[71] The Hacker News. Dostupné z: https://thehackernews.com/2023/12/cost-of-data-breach-report-2023.html

s mplementovanými pokročilými bezpečnostními technologiemi, jako je šifrování a umělá inteligence pro detekci hrozeb, měly nižší náklady na incidenty. Naopak organizace bezdostatečné kybernetické ochrany čelily vyšším nákladům a delším dobám obnovy.

Podle článku "123 SMB Cybersecurity Statistics" se 61 % malých a středně velkých podniků stalo terčem kybernetického útoku. Průměrné náklady na řešení kybernetických incidentů se u těchto subjektů v roce 2023 pohybovaly od 826 do 653 587 USD. Polovina malých podniků zaznamenala výpadky webových stránek na 8 až 24 hodin a 40 % ztratilo následkem kybernetického útoku kritická data. Navíc 95 % incidentů je způsobeno lidskou chybou, což podtrhuje důležitost školení a zvýšení povědomí o kybernetické bezpečnosti.[72]

Podle zprávy "Data Breach Investigations Report 2024" od Verizon zahrnoval jeden ze tří úniků dat ransomware nebo jiné techniky vydírání, což představuje 32 % všech útoků. Podle FBI Internet Crime Complaint Center byla mediánová ztráta spojená s těmito útoky 46 000 USD, přičemž 95 % případů se pohybovalo mezi 3 až 1 141 467 USD. Kybernetické incidenty, včetně chyb uživatelů, tvořily 28 % všech případů a lidský faktor byl přítomen u 68 % úniků dat.[73]

Dalším podkladem pak může být rovněž Odhad ekonomických nákladů způsobených kybernetickými útoky v Izraeli – analýza INCD. Nová zpráva INCD poprvé představuje ekonomickou analýzu nákladů kybernetických útoků na izraelskou ekonomiku, odhadovaných na nejméně 12 miliard NIS (nový izraelský šekel) ročně (přes 76 miliard Kč). Zpráva uvádí, že investice do základních obranných opatření mohou snížit šance na útok o 30–50 %. Tato data ukazují významnou ekonomickou zátěž na HDP země způsobenou kybernetickými útoky. Bez zvýšení úrovně kybernetické ochrany se náklady budou nadále zvyšovat. Pochopení nákladů na škody pomůže politickému rozhodování a určí vyvážené kroky pro investice do kybernetické obrany na národní úrovni. Analýza zahrnuje krátkodobé náklady (platby prvnímu respondentovi, prostoje, obnova dat, právní poradenství) i střednědobé až dlouhodobé náklady (ztráta příjmů, ztráta obchodních příležitostí, poškození dobrého jména, soudní spory).

Empirická studie z Telavivské univerzity prokázala, že základní kybernetická obranná opatření mohou výrazně snížit pravděpodobnost útoků. Například velké společnosti, které využívají e-commerce a cloudové služby, mohou snížit šance na útok o 50 % implementací základních bezpečnostních opatření, jako je vícefaktorové ověřování, politika silných hesel, antivirus, používání originálního softwaru a pravidelné aktualizace. Zpráva uvádí, že snížení pravděpodobnosti útoku o 10 % a snížení průměrných nákladů o 10 % může přinést úspory nejméně 2 miliardy NIS ročně (12,7 miliard Kč). INCD pracuje na zavedení vhodné úrovně ochrany pro klíčové organizace nezbytné pro ekonomiku. Politika zahrnuje regulace, ekonomické pobídky a další opatření k podpoře kybernetické obrany.

INCD klade důraz na ekonomické úvahy při rozhodování o kybernetické obraně, a to jak na makroúrovni (stát), tak na mikroúrovni (podniky a vládní organizace). Ekonomická analýza zahrnuje přehled mezinárodních studií, článků a dat o ekonomických nákladech kybernetických útoků a výhodách zvýšení ochrany. Odhad nákladů byl proveden pomocí metod „shora dolů“ a „zdola nahoru“. Studie ukazují, že náklady na kybernetické útoky lze snížit zvýšením ochrany v kyberprostoru za relativně nízkou cenu ve srovnání s potenciálními škodami. INCD proto podporuje aktivní ochranu, průběžné monitorování a zvyšování povědomí. Zpráva zdůrazňuje potřebu robustních mechanismů kybernetické obrany k zmírnění ekonomických škod způsobených útoky. Zvýšením úrovně ochrany a podporou přesného hlášení může Izrael snížit finanční dopady těchto hrozeb a posílit národní kybernetickou

[72] Packetlabs. Dostupné z: https://www.packetlabs.net/posts/123-smb-cybersecurity-statistics/

[73] Verizon business. Dostupné z: https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/

odolnost. Odhadované náklady slouží jako varovný signál pro tvůrce politik i podniky, aby kybernetickou bezpečnost zahrnuli do svých strategických plánů.

Úřad dále za účelem zjištění nákladů spojených s řešením kybernetických bezpečnostních incidentů oslovil Českou asociaci pojišťoven. Zjišťování mezi pojišťovnami ukázalo, že pojištění kybernetických rizik není běžně nabízeno samostatně a je častěji dostupné na poptávku větších firem s jinými druhy pojištění. Škody se pohybují v rozmezí 200 tisíc Kč až 30 milionů Kč, přičemž celkové škody za poslední 3 roky nepřesáhly 50 milionů Kč. Pojištění poptávají převážně velké firmy a na IT zaměřené střední firmy. Mezinárodní firmy si krytí kybernetických rizik často obstarávají prostřednictvím mezinárodních programů, které jsou pojištěny mimo ČR. Před pojištěním jsou firmy podrobovány detailnímu zkoumání. Právě to se ukazuje jako velký problém, jelikož subjekty na českém trhu nejsou často schopny splnit ani základní úroveň maturity v kybernetické bezpečnosti a jsou proto *de facto* nepojistitelné.

Úřad v téže věci oslovil nadnárodní pojišťovnou Chubb, která patří mezi největší pojistitele kyber na světě a je zároveň číslo jedna v USA. Z obdržených materiálů plyne následující: 80-90 % všech incidentů byl ransomware, průměrné výkupné se pohybuje okolo 200 tisíc USD, zhruba 25 % požadavků na výkupné je uhrazeno a následně pracují s poměrně vysokou úspěšností obnovy dat tzv. recovery. Hackeři v drtivé většině poskytnou dekódovací klíče vč. případné podpory. Náklady na pojistná plnění pak průměrně vycházejí na 505 186 USD, tedy 11,7 milionu Kč. Tato částka obsahuje oznámení/call centrum, PR/krizová reakce, právní služby, forenzní služby.

Chubb kromě jiného poskytl také anonymizované údaje o dvou menších příkladech incidentů, které proběhly v ČR. V jednom případě se jednalo o lidskou chybu týkající se nakládání s osobními údaji. Celkové plnění pak vyšlo na 5 650 000 Kč. Neoprávněné nakládání s údaji: náklady na obranu v souvislosti s šetřením regulátora 1,7 milionu Kč, odškodnění pro poškozené zaměstnance 3 milionu Kč. Náklady na řešení incidentu: náklady na krizového manažera 150 tisíc Kč, náklady na oznámení poškozeným 100 tisíc Kč, náklady na monitoring možných následných škod 400 tisíc Kč, náklady na právní konzultace 300 tisíc Kč. Ve druhém případě se jednalo o odepření služby (DOS). Celkové plnění vyšlo na 4,5 milionu Kč. Náklady na obnovu: zvýšené náklady na pracovní sílu 270 tisíc Kč, náklady na externí dodavatele služeb 360 tisíc Kč. Přerušení provozu: ztráta příjmu z důvodu nefunkčnosti webových stránek 3 miliony Kč. Náklady na řešení incidentu: náklady forenzní analýzu 370 tisíc Kč, náklady na právní konzultace 300 tisíc Kč, náklady na krizového manažera 200 tisíc Kč.

Nadto je třeba uvést, že v těchto plněních nejsou zahrnuty náklady spojené s poškozením dobrého jména či případné škody na životě či zdraví, které jsou hrazeny z jiného pojištění (u života a zdraví typicky pojištění odpovědnosti).

V tomto kontextu je vhodné také upozornit, že globální ekonomika kyberkriminality bude podle odhadů do roku 2025 dosahovat výše 10,5 bilionu USD, čímž se stane třetí největší „ekonomikou“ světa podle HDP po USA a Číně. Tato temná ekonomika zahrnuje sofistikované operace včetně náboru, vývoje ransomware, vyjednávání o výkupném a praní bitcoinů.[74]

Nelze opomenout skutečnost, že subjekty podnikající v různých odvětvích budou po kybernetickém útoku často nuceny promítnout náklady na jeho řešení do cen svých služeb a výrobků. Náklady spojené s obnovou systémů, ztrátou dat a přerušením provozu mohou být značné a mohou negativně ovlivnit finanční stabilitu podniků. Tyto dodatečné výdaje se obvykle přenesou na zákazníky, tj. i spotřebitele ve formě vyšších cen, což může snížit konkurenceschopnost těchto subjektů na trhu. Zvýšené ceny mohou také vést ke ztrátě

[74] Cybercrime magazine. Dostupné z: https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/

zákazníků, kteří hledají levnější alternativy, což dále ohrožuje udržitelnost podnikání. Zavedení účinných kybernetických bezpečnostních opatření může významně přispět k minimalizaci těchto rizik a udržení cen na konkurenceschopné úrovni.

V neposlední řadě je nutné zmínit možné poškození reputace ČR, která je dlouhodobě v Evropě považována za vedoucí stát v oblasti kybernetické bezpečnosti.

Všechny výše uvedené údaje zdůrazňují vysoké náklady spojené s nulovou variantou, tedy bez zavedení potřebných bezpečnostních opatření, což podtrhuje důležitost investic do kybernetické bezpečnosti.

3.2.1.2. Náklady na řešení kybernetických incidentů u strategicky významných služeb

Mezi klíčové oblasti, které by byly nejvíce zasaženy v případě incidentu v oblasti dodavatelského řetězce, patří tzv. strategicky významné služby v oblasti veřejné správy, energetiky, letecké a drážní dopravy a služby v oblasti digitální infrastruktury a služeb. Tyto služby jsou mezi strategicky významné služby zahrnuty proto, že incidenty v těchto sektorech mají největší potenciál šíření a mohou způsobit rozsáhlé sekundární škody napříč ekonomikou. Telekomunikace a digitální služby jsou klíčové pro komunikaci a provoz všech ostatních sektorů, energetický sektor je nezbytný pro fungování průmyslu a domácností, a ústřední správní orgány zajišťují klíčové státní služby a bezpečnost. Ochrana těchto služeb je tedy zásadní pro prevenci dalekosáhlých ekonomických a společenských následků.

Telekomunikační a digitální služby jsou nezbytné pro hladké fungování jak veřejného, tak soukromého sektoru. V případě významného incidentu, který by ovlivnil dostupnost těchto služeb, by došlo k paralýze komunikace a internetových služeb, což by mělo za následek rozsáhlé narušení běžného provozu. Takovýto výpadek by se promítl do všech dalších sektorů. Úniky citlivých osobních a firemních údajů by vedly k reputačním škodám s dalekosáhlými právními důsledky. Manipulace s daty by navíc mohla podkopat důvěru v digitální transakce a komunikace. Na základě expertního odhadu s náklady u kybernetických incidentů odhadujeme, že náklady způsobené narušením dostupnosti, důvěrnosti a integrity v tomto sektoru mohou dosáhnout výše až 2,5–10 % denního HDP, což představuje přibližně částku od 411 milionů Kč do 1,644 miliard Kč denně.

Rozděleno na časové řezy po jednotlivých dnech by kybernetický incident v telekomunikačním sektoru ČR mohl mít ekonomický dopad od 411 milionů Kč do 1,644 miliard Kč za jeden den, od 1,233 miliard Kč do 4,932 miliard Kč za tři dny a od 2,055 miliard Kč do 8,22 miliard Kč za pět dní.

Odhad bere v potaz, že na telekomunikačním sektoru je částečně nebo zcela závislá většina ostatních sektorů. Právě pro jeho klíčovost jsou však sektory částečně připraveny na to, aby výpadek v této oblasti pokryly, nebo alespoň nahradily. Telekomunikační a digitální služby jsou navíc dostatečně robustně budované systémy, tudíž lze očekávat jejich vzájemnou zastupitelnost a nahraditelnost. V případě komplexního výpadku způsobeného závislostí všech poskytovatelů na jednom či několika rizikových dodavatelích lze však předpokládat, že by náklady za incident samotný i obnovu po něm spočívali řádově ve vyšších desítkách až nižších stovkách miliard Kč.

Energetický sektor je dalším kritickým odvětvím, jehož narušení by mělo dalekosáhlé důsledky. Přerušení dodávek energie by mohlo zastavit průmyslovou výrobu a ovlivnit každodenní život občanů, což by vedlo k rozsáhlým ekonomickým škodám. Takovýto výpadek by se promítl do všech dalších sektorů. Přístup k citlivým operačním datům by mohl vést k cíleným útokům na kritickou infrastrukturu, rozsáhlým výpadkům v distribuční energetické soustavě a případně k omezení či zastavení výroby. Manipulace s řídicími systémy v energetickém sektoru by mohla způsobit fyzické škody a další bezpečnostní rizika.

Na základě expertního odhadu s náklady u kybernetických incidentů odhadujeme, že náklady způsobené velmi závažným narušením dostupnosti, důvěrnosti a integrity v tomto sektoru mohou dosáhnout výše až 5–15 % denního HDP, což je přibližně 822 milionů až 2,466 miliard Kč denně.

Kybernetický incident v energetickém sektoru by tak mohl mít ekonomický dopad od 822 milionů Kč do 2,4666 miliard za jedeně den. Za tři dny by se jednalo o 2,466 až 7,398 miliard Kč. V případě pěti dní jsme vzali v potaz i to, že náklady exponenciálně rostou v závislosti na délce incidentu a výslednou částku vynásobili koeficientem 1,5. Výsledný rozptyl se tedy pohybuje v rozmezí 6,165 až 18,495 miliard Kč.

Odhad bere v potaz, že na energetickém sektoru je částečně nebo zcela závislá většina ostatních sektorů. Právě pro jeho klíčovost jsou však sektory částečně připraveny na to, aby výpadek v této oblasti pokryly, nebo alespoň nahradily. Stejně tak je sektor nastaven tak, aby krátkodobé výpadky pokryly další poskytovatelé (například ze zahraničí, ale i vnitrostátní). S postupem času by však byly důsledky výpadku v této oblasti naprosto katastrofální a s velkou pravděpodobností by vedly k dalekosáhlým škodám (na životech a zdraví, finančním, reputačním) na celém území ČR. Tyto škody v případě výpadku energetického sektoru již lze pouze odhadnout na řádově stovky miliard Kč.

Ústřední správní orgány a další významné orgány veřejné správy hrají klíčovou roli ve fungování státu a jakékoliv narušení jejich činnosti by mělo vážné důsledky. Přerušení vládních služeb by mohlo zpozdit administrativní procesy a poskytování veřejných služeb, zatímco úniky klasifikovaných informací by mohly mít důsledky v oblasti národní bezpečnosti. Manipulace s vládními daty by mohla vést k šíření dezinformací a veřejné nedůvěře. Na základě expertního odhadu s náklady u kybernetických incidentů odhadujeme, že náklady způsobené narušením dostupnosti, důvěrnosti a integrity v tomto sektoru mohou dosáhnout výše až 1–3 % denního HDP, což odpovídá přibližně 164 až 493 milionů Kč denně.

Kybernetický incident ve veřejné správě ČR by mohl mít ekonomický dopad od 164 do 493 milionů Kč za jeden den, od 493 milionů Kč do 1,4796 miliard Kč za tři dny a od 822 milionů Kč do 2,466 miliard Kč za pět dní.

Odhad bere v potaz to, že na veřejném sektoru a jeho činnostech jsou částečně závislé další sektory, je však zohledněno to, že tomu je tak v nižší míře. Navíc lze s určitou mírou obtíží nahradit při incidentu v kyberprostoru činnost úřadu ve fyzickém světě. Míru dopadu však naopak pozvedá citlivost údajů, které příslušné veřejné orgány schraňují. Míra dopadů ztráty integrity a důvěrnosti je tak výrazně vyšší než u ostatních sektorů.

Dopady kybernetických incidentů v oblasti **letecké a drážní dopravy** jsou také významné. Tyto sektory jsou kritické pro zajištění plynulosti dopravy a logistiky, přičemž jakýkoli incident může způsobit rozsáhlé narušení provozu, zpoždění a ekonomické ztráty. Výpadky v těchto sektorech by mohly narušit dodavatelské řetězce, cestovní ruch a každodenní dojíždění občanů. Na základě expertního odhadu s náklady u kybernetických incidentů odhadujeme, že náklady způsobené narušením dostupnosti, důvěrnosti a integrity v tomto sektoru mohou dosáhnout výše až 0,1 % denního HDP, což představuje přibližně 16,44 milionů Kč denně.

Kybernetický incident v letecké a drážní dopravě ČR by mohl mít ekonomický dopad 16,44 milionů Kč za jeden den, 49,32 milionů Kč za tři dny a 82,2 milionů Kč za pět dní.

Odhad je nižší zejména proto, že povinné osoby jsou zpravidla připraveny zajistit provoz strategicky významné služby i jinými způsoby, a tak předejít vysokým dopadům v oblasti dostupnosti důvěrnosti a integrity.

Závěr

Celkové odhadované ekonomické dopady kybernetických incidentů ve zmíněných sektorech jsou zhruba v rozptylech:

- **Za jeden den**: 1,42–4,62 miliard Kč
- **Za tři dny**: 4,24–13,86 miliard Kč
- **Za pět dní**: 7,1–23,1 miliard Kč

Lze předpokládat, že další náklady by byly spojené s následnou dlouhotrvající obnovou po incidentu. Současně s tím nutné opětovně poukázat na to, že v případě výpadku delšího než pět dní ve strategicky významných službách (řádově desítky dní) mohou nastat až katastrofální dopady na ekonomickou a bezpečnostní situaci v ČR, která by velmi negativně ovlivnila životy a bezpečnost všech jejích občanů.

Tento odhad podtrhuje kritickou potřebu mechanismu, který umožní prověřit dodavatele do strategicky významných služeb, a tím mitigovat či zcela eliminovat ekonomické dopady případného incidentu.

3.2.2. Varianta II: Transpozice směrnice bez zohlednění mechanismu prověřování bezpečnosti dodavatelského řetězce a odstranění zjištěných nedostatků a reflexe dosavadních zkušeností (minimální transpozice směrnice)

Náklady spojené s touto variantou jsou představovány především náklady spojenými s realizací bezpečnostních opatření. Minimalistický způsob zapracování směrnice do českého právního řádu by navazoval na aktuálně aplikovaný princip jednotné kybernetické bezpečnosti vůči hlavním subjektům současné regulace (nové regulované subjekty, resp. jimi poskytované služby, by byly bez dalšího zařazeny do kategorií kritické informační infrastruktury nebo provozovatele základní služby a plnily by všechny povinnosti spojené s těmito kategoriemi povinných osob). Tím by došlo k uložení jednotného a vysokého rámce povinností (v současné právní úpravě reprezentované vyhláškou o kybernetické bezpečnosti) tisícům nových subjektů. Nedošlo by také k žádné dodatečné úpravě hlášení kybernetických bezpečnostních incidentů nebo výkonu kontrol a dalších procesů. V případě této varianty navíc minimalistický přístup vede k realizace požadavků směrnice v rámci dosavadních institutů, které byly ovšem konstruovány na násobně menší rozsah regulace.

Ze směrnice vyplývá potřeba regulace více než 60 služeb v 18 odvětvích, přičemž celá řada těchto organizací se doposud s regulací kybernetické bezpečnosti nesetkala. Směrnice sama rozděluje subjekty, které reguluje, do dvou množin, na tzv. „*essential entities*“ a „*important entities*“. Hlavními povinnostmi, které těmto subjektům směrnice ukládá nehledě na jejich rozdělení, je zavádění bezpečnostních opatření a hlášení incidentů. V případě, že by měly být tyto požadavky zahrnuty do zákona o kybernetické bezpečnosti, bylo by nutné aktualizovat především znění vyhlášky o kritériích pro určení provozovatele základní služby, rozsah směrnice podřadit pod ni, a určit nové povinné osoby v rámci správních řízení vedených Úřadem.

Bez dalších úprav racionalizujících požadavky směrnice NIS 2, což je limita daná touto variantou, by narostl počet povinných osob ze zákona nejméně 15násobně, přičemž povinnost zavádět bezpečnostní opatření v rozsahu dosavadní vyhlášky o kybernetické bezpečnosti by zůstala nezměněna. Stejně tak v případě hlášení kybernetických bezpečnostních incidentů by se i po těchto nově regulovaných organizacích požadovalo hlásit bezodkladně všechny incidenty. Tento přístup by kladl na všechny regulované organizace požadavky spočívající v systematickém řízení jejich rizik. Ačkoli se přitom tento přístup dlouhodobě jeví jako nejvhodnější, protože umožňuje každé organizaci přizpůsobit si bezpečnostní opatření podle potřeby, obsah vyhlášky o kybernetické bezpečnosti je přeci jen cílen na vyspělejší organizace a organizace s národním nebo alespoň regionálním dopadem.

Také na straně Úřadu budou muset být vynaloženy nové náklady, a to zejména v souvislosti se zajištěním procesů vyplývajících ze směrnice pro plnění role tzv. příslušného orgánu a jednotného kontaktního místa. V rámci toho bude nutné oproti současné Koncepci rozvoje Úřadu navýšit razantně počet systemizovaných pracovních míst, čímž dojde ke zvýšení platových nákladů. K enormnímu nárůstu zaměstnanců by muselo dojít především na úseku identifikace povinných osob a kontroly plnění povinností, a to takovým způsobem, aby byl výkon kontroly plněn i u tisíců nových povinných osob. Nehledě na to, změny procesů vyžádané nárůstem počtu povinných osob se bez ohledu na výše uvedený výkon kontroly odhaduje na nižší desítky tabulkových míst oproti aktuální Koncepci rozvoje Úřadu. Personální náklady bude potřeba alokovat především do kapacitního posílení služeb vládního CERT (především v otázkách řešení kybernetických bezpečnostních incidentů a jejich analýzy, pentestů či skenů zranitelností), výkonu metodického řízení povinných osob (lze očekávat, že v souladu s obsahem směrnice NIS 2 budou pod zákonnou regulaci nově spadat také organizace s nižší úrovní kybernetické bezpečnosti) a výkonu kontroly. Násobný nárůst oproti aktuální Koncepci rozvoje Úřadu bude také ve finančních nákladech. Kromě personálních a finančních nákladů se totiž předpokládá vznik informačního systému, který umožní řádný výkon pravomocí a povinností Úřadu v souvislosti s nárůstem počtu regulovaných subjektů a celkovým rozšířením souvisejících agend.

K nezavedení mechanismu prověřování bezpečnosti dodavatelského řetězce je namístě odkázat na vyhodnocení nákladů v případě varianty I.

3.2.3. Varianta III: Transpozice směrnice bez zohlednění mechanismu prověřování bezpečnosti dodavatelského řetězce, ovšem při odstranění zjištěných nedostatků a reflexe dosavadních zkušeností

Náklady varianty III vycházejí z nákladů uvedených v případě varianty II, nicméně právě možnost odchýlit se od požadavku nezasahovat do zákona nad rámec základních požadavků směrnice umožňuje efektivním způsobem snižovat náklady tam, kde je to možné a účelné.

Náklady spojené s realizací bezpečnostních opatření jsou v tomto případě rozděleny do dvou množin podle tzv. režimů poskytovatele regulované služby. Poskytovateli regulované služby v režimu nižších povinností (kterých je v tomto případě několik tisíc) stanovuje novou sadu bezpečnostních opatření, jejichž plnění je s ohledem na zdroje méně náročné. Tato varianta tedy přichází s možností stanovit vedle upravené a nově vydané vyhlášky o kybernetické bezpečnosti (závazné pro provozovatele regulované služby v režimu vyšších povinností) ještě druhý prováděcí právní předpis, který bude klást na subjekty v režimu nižších povinností menší požadavky, a tím i menší náklady na jejich zavedení a udržování. Stejně tak tomu bude i v případě povinnosti hlášení kybernetických bezpečnostních incidentů, kde tato varianta umožňuje u režimu nižších povinností hlásit jen takové incidenty, které mají větší význam (nikoli všechny jako v případě vyššího režimu). Tyto jednotlivé kroky vedou k tomu, že výchozí náklady lze sice odvozovat od hrubého odhadu výše, ale výsledné náklady budou po provedení výše zmíněných úprav nižší, než je tomu v případě varianty II.

Také na straně Úřadu vede možnost širší úpravy procesů k tomu, že sice budou muset být vynaloženy nové náklady v souvislosti se zajištěním procesů vyplývajících ze směrnice pro plnění role tzv. příslušného orgánu a jednotného kontaktního místa, nicméně na rozdíl od varianty II je možné tyto náklady alespoň dílčím způsobem omezit (např. zavedením zjednodušeného způsobu kontroly u poskytovatelů regulované služby v režimu nižších povinností).

K nezavedení mechanismu prověřování bezpečnosti dodavatelského řetězce je namístě odkázat na vyhodnocení nákladů v případě varianty I.

3.2.4. Varianta IV: Transpozice směrnice zároveň zohledňující mechanismus prověřování bezpečnosti dodavatelského řetězce, ovšem bez odstranění zjištěných nedostatků a reflexe dosavadních zkušeností

Tato varianta je v případě nákladů mimo otázky mechanismu prověřování bezpečnosti dodavatelského řetězce zcela shodná s variantou II. S ohledem na skutečnost, že níže (4. Návrh řešení) byla vybrána jako nejvhodnější řešení varianta V, náklady jednotlivých podvariant jsou specifikovány právě v souvislosti s variantou V níže.

3.2.5. Varianta V: Transpozice směrnice, zohlednění mechanismu prověřování bezpečnosti dodavatelského řetězce a odstranění zjištěných nedostatků a reflexe dosavadních zkušeností

Náklady varianty V jsou v případě nákladů mimo otázky mechanismu prověřování bezpečnosti dodavatelského řetězce zcela shodné s variantou III.

Využití režimů pro stanovení konkrétních požadavků, především v případě bezpečnostních opatření a hlášení kybernetických bezpečnostních incidentů, umožňuje stanovit rozdílné sady povinností, které mimo jiné pomáhají snižovat náklady jak na straně povinných osob, tak na straně Úřadu, potažmo státu. Stanovení druhého prováděcího právního předpisu pro režim nižších povinností a odlišných a mírnějších požadavků, stejně tak jako dílčí úpravy v hlášení incidentů, umožní racionalizovat náklady nutné na zabezpečení nových povinných subjektů. Tyto jednotlivé kroky vedou k tomu, že výchozí náklady lze sice odvozovat od nastínění hrubého odhadu výše, ale výsledné náklady budou po provedení výše zmíněných úprav nižší, než je tomu v případě varianty II nebo IV.

Také na straně Úřadu vede možnost širší úpravy procesů k tomu, že sice budou muset být vynaloženy nové náklady v souvislosti se zajištěním procesů vyplývajících ze směrnice pro plnění role tzv. příslušného orgánu a jednotného kontaktního místa, nicméně na rozdíl od varianty II je možné tyto náklady alespoň dílčím způsobem omezit (např. zavedením zjednodušeného způsobu kontroly u poskytovatelů regulované služby v režimu nižších povinností). Násobný nárůst oproti aktuální Koncepci rozvoje Úřadu bude také ve finančních nákladech. Kromě personálních a finančních nákladů se totiž předpokládá vznik informačního systému, který umožní řádný výkon pravomocí a povinností Úřadu v souvislosti s nárůstem počtu regulovaných subjektů a celkovým rozšířením souvisejících agend.

Stejně jako v případě varianty III, a na rozdíl od varianty II, jsou náklady spojené s touto variantou navíc v několika ohledech snižovány, a to jak na straně povinných subjektů, tak na straně Úřadu.

3.2.5.1. Podvarianta Va: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře

Při volbě podvarianty Va vznikají přímé a nepřímé náklady na straně státu a poskytovatelů strategicky významné služby, a potenciální nepřímé náklady dodavatelům poskytovatelů strategicky významné služby. V souvislosti se zavedením mechanismu bude pro relevantní státní orgány třeba přijmout jednotky až nízké desítky nových pracovníků pro posuzování rizikovosti a prověřování rizikových dodavatelů. S ohledem na návaznost procesů spojených s mechanismem prověřování na stávající procesy, které povinné osoby podle zákona o kybernetické bezpečnosti mají již v současnosti povinnost provádět, dojde k minimálnímu vzniku dodatečných administrativních nákladů při zavádění nové regulace do právních předpisů. Potenciální vysoký dopad na poskytovatele strategicky významné služby by měl případný zákaz dodavatele vydaný Úřadem, ovšem v odůvodněných případech má Úřad pravomoc udělit výjimku pro typovou bezpečnostně významnou dodávku. Z důvodu vyloučení

možnosti pořídit bezpečnostně významnou dodávku od vysoce rizikového dodavatele může docházet k obdržení vyšší ceny od alternativních dodavatelů dodávek, současně platí, že takový následek lze očekávat pouze v případech, kdy na trhu není dostatečná konkurence a danou dodávku poskytuje pouze omezený počet dodavatelů. Co se týče případných nákladů vyloučených dodavatelů, dotčení dodavatelé mohou i nadále poskytovat ostatní (méně významné) dodávky do strategické infrastruktury, stejně tak jako dalším subjektům v ČR.

Návrh zákona rozšíří pravomoci Úřadu v oblasti kybernetické bezpečnosti tak, aby byl zaveden komplexní mechanismus prověřování bezpečnostní spolehlivosti dodavatelů do strategicky významné infrastruktury napříč jejími sektory, včetně možnosti omezování či zákazu využití dodavatelů, kteří budou vyhodnoceni jako rizikoví či vysoce rizikoví.

Ve vztahu k návrhu zákona lze předpokládat nutnost vyhrazení jednotek až nízkých desítek tabulkových míst u zapojených státních orgánů a rozšíření stávajících či připravovaných informačních systémů k technické obsluze procesu prověřování. Na straně Úřadu a spolupracujících institucí budou muset být vynaloženy náklady související se zavedením nových procesů, příp. rozšířením stávajících činností a procesů státních orgánů tak, aby mohlo docházet k systematickému a koordinovanému prověřování dodavatele do strategicky významné infrastruktury. V souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy či prověřování zahraničních investorů podle zákona o prověřování zahraničních investic, a to včetně účelného využívání informačních systémů, které tyto agendy podporují.

Noví pracovníci Úřadu a spolupracujících státních orgánů budou podle nařízení vlády č. 222/2010 Sb., o katalogu prací ve veřejných službách a správě, ve znění pozdějších předpisů, provádět šetření rizikových dodavatelů a tuto rizikovost vyhodnocovat.

Náklady vzniknou také poskytovatelům strategicky významné služby. S ohledem na návaznost procesů spojených s mechanismem prověřování na stávající procesy, které povinné osoby podle zákona o kybernetické bezpečnosti mají již v současnosti povinnost provádět, jako je identifikace a hodnocení aktiv, analýza rizik apod., dochází k minimálnímu zásahu, a tedy i k minimálnímu vzniku dodatečných nákladů při zavádění nové regulace do právních předpisů. Nové povinnosti poskytovatelů strategicky významné služby budou sestávat z povinnosti Úřadu hlásit přímé dodavatele bezpečnostně významných dodávek, vynaložit přiměřené úsilí ke zjišťování nepřímých dodavatelů bezpečnostně významných dodávek a zjištěné nepřímé dodavatele taktéž hlásit Úřadu. Tyto nové povinnosti generují na straně poskytovatelů strategicky významné služby minimální administrativní náklady.

Potenciální významnější náklady poskytovatelům strategicky významné služby generuje povinnost dodržovat opatření vydaná Úřadem. V případě vydání varování podle návrhu zákona se bude jednat o reflexi identifikované hrozby v analýze rizik, což je opět proces, který je u poskytovatelů strategicky významné služby již nastavený a fungující. Případný zákaz dodavatele má potenciální vysoký dopad na poskytovatele strategicky významné služby. Pokud by poskytovatel strategicky významné služby identifikovaného zakázaného vysoce rizikového dodavatele využíval v bezpečnostně významné dodávce, bude muset takového dodavatele ze své infrastruktury vyloučit. Z dotazníkového šetření plyne, že vyloučení a nahrazení významného dodavatele může pro poskytovatele strategicky významné služby generovat náklady až ve výši jednotek milionů Kč (3 % respondentů), desítek milionů Kč (34 % respondentů), stovek milionů Kč (16 % respondentů). Tyto náklady spočívají ve výměně stávajícího řešení, pořízení nového řešení a jeho integraci mezi stávající infrastrukturu a procesy, přičemž vždy ale bude záležet, o jakého dodavatele se jedná a jaké podmínky nabízí

dodavatelé alternativní. 22 % respondentů uvedlo, že vyloučení takového dodavatele nebude mít žádný dopad. 25 % respondentů uvedlo náklady vyšší než 1 miliarda Kč, nicméně náklady byly vyčísleny v takové výši z důvodu, že dané orgány či osoby uvažovaly o vyloučení dodavatelů, kteří jako jediní jsou schopni dané plnění poskytnout. Do kalkulace nákladů tak započítávaly mj. dopady ukončení či omezení poskytování regulované služby, včetně ušlého zisku. Pro případ unikátnosti dodávky daného vysoce bezpečnostně rizikového dodavatele Úřad umožňuje v rámci procesu připomínkování návrhu OOP poskytovatelům strategicky významné služby tento fakt Úřadu sdělit. V případě dostatečného odůvodnění a podložení tvrzení důkazy může Úřad udělit výjimku pro typovou bezpečnostně významnou dodávku, a poskytovatelům strategicky významné služby za podmínek reflektování identifikované hrozby v analýze rizik umožní bezpečnostně relevantní dodávku využívat i nadále, čímž jsou případné náklady plynoucí ze zákazu takového dodavatele pro poskytovatele strategicky významné služby minimalizovány. Jelikož tedy návrh zákona pro případy existence jediného možného dodavatele poskytujícího bezpečnostně významnou dodávku umožňuje získat výjimku ze zákazu takového dodavatele pro danou bezpečnostně významnou dodávku, s generací respondenty udaných vysokých nákladů (vyšších než 1 miliarda Kč) předkladatel nepočítá.

Celkem 56 % respondentů jako nejzávažnější možný dopad na poskytování služby identifikuje omezení či ukončení poskytování služby. Právě riziko ohrožení poskytování regulované služby podstatným způsobem také umožňuje poskytovateli strategicky významné služby zažádat o výjimku ze zákazu plnění identifikovaného vysoce rizikového dodavatele. Pro dalších 32 % respondentů jsou nejzávažnější dopady ty finanční.

Následujících 12 % respondentů, v případě aplikace lhůty respektující ekonomickou životnost daného aktiva, pro vyloučení stávajícího dodavatele identifikuje absenci dopadů vyšší, než ty standardně spojené s obnovou technologie a přechodem na alternativní technologická řešení. Úřad při vydávání OOP omezujícího či zakazujícího plnění rizikového dodavatele šetří mimo jiné i dopady na poskytovatele strategicky významných služeb a lhůtu pro zavedení povinností stanoví s ohledem na životní cyklus dodávky (v tomto případě určený dobou daňového odpisu podle právního předpisu upravujícího zdanění příjmů). Je nutné zmínit, že Úřad nemusí při stanovování lhůty životní cyklus plnění reflektovat, v takovém případě však do procesu vstoupí Bezpečnostní rada státu, případně i sektoroví regulátoři, a především Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí a Ministerstvo vnitra, kteří projednají proporcionalitu návrhu OOP. V případě, že poskytovatel strategicky významné služby vysoce rizikového dodavatele v současnosti nevyužívá, nicméně v budoucnu by o bezpečnostně významných dodávkách tohoto dodavatele uvažoval, z důvodu vyloučení možnosti bezpečnostně významnou dodávku od vysoce rizikového dodavatele pořídit může docházet k obdržení vyšší ceny od alternativních dodavatelů dodávek. Tento přístup a zvýšené náklady se mohou objevit obzvláště v případě, když na trhu není dostatečná konkurence a danou dodávku poskytuje pouze omezený počet dodavatelů.

V neposlední řadě podvarianta Va přináší dodatečné nepřímé náklady taktéž dodavatelům bezpečnostně relevantních dodávek. V případě vyloučení vysoce bezpečnostně rizikového dodavatele z možnosti poskytovat bezpečnostně významné dodávky do strategicky významné infrastruktury může dojít k omezení hospodářské soutěže. Takový dodavatel nicméně i nadále může poskytovat ostatní dodávky do strategické infrastruktury, stejně tak jako dalším subjektům v ČR. Tato podvarianta nicméně nevyžaduje iniciativu či jinou součinnost od dodavatelů.

Vzhledem k tomu, že podvarianta Va nevyžaduje *ex ante* prověření všech dodavatelů, resp. dodavatelských řetězců do strategicky významné infrastruktury, minimalizuje také nároky na personální a administrativní kapacity státu i soukromého sektoru, jakož i zásah prověřování

do podnikatelských procesů, nehrozí tedy zdržení investic a zpomalení rozvoje z důvodu zpomalení výběrových řízení.

3.2.5.2. Vb: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře se zapojením vlády ČR

Podvarianta Vb má shodné náklady s výše uvedenou podvariantou Va. Vzhledem k zapojení vlády v případě kratších odpisových lhůt je ovšem třeba brát v úvahu, že proces rozhodování o možném omezení dodavatele by tedy byl delší nežli v případě podvarianty Va, a to odhadem o 30–60 dní v závislosti na rychlosti projednání věci vládou ČR.

3.2.5.3. Vc: Mechanismus plošného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře

Náklady podvarianty Vc jsou ve srovnání s podvariantou Va pro všechny dotčené subjekty vyšší. Všechny náklady identifikované v podvariantě Va jsou přenositelné do podvarianty Vc, podvarianta Vc navíc přináší další náklady.

Vzhledem k tomu, že proces prověřování probíhá *ex ante* před poskytnutím bezpečnostně významné dodávky každým novým dodavatelským řetězcem, nároky na intenzitu prověřování jsou výrazně vyšší. Zátěž bude extrémně vysoká především na začátku účinnosti tohoto právního předpisu, jelikož do předem stanovené lhůty bude nutné prověřit všechny stávající dodavatelské řetězce, které momentálně poskytují bezpečnostně významné dodávky do strategicky významné infrastruktury státu. Tato podvarianta tak předpokládá velmi vysoké personální a administrativní nároky na stát z důvodu vedení velkého a nepředvídatelného množství správních řízení, a z toho možné plynoucí náhrady škody za nesprávný úřední postup z důvodů nesplnění zákonných lhůt.

Náklady na straně státu by tak byly značně zvýšené.

Zvýšené nároky by byly taktéž na dodavatele bezpečnostně významných dodávek. Ti by jakožto prerekvizitu pro poskytování bezpečnostně významných dodávek museli získat „certifikaci“ jak sebe sama, tak každého dodavatelského řetězce, který by využívali pro poskytování bezpečnostně významných dodávek. Podvarianta Vc klade vysoké nároky co do poskytovaných informací o samotném přímém dodavateli, ale i o jeho poddodavatelích. Tento certifikační proces zvyšuje bariéry trhu.

Podvarianta Vc má také výraznější dopady a náklady na poskytovatele strategicky významné služby. Povinnost využívat pouze certifikované dodavatele, resp. dodavatelské řetězce pro poskytování bezpečnostně významných dodávek má značný dopad na podnikatelské procesy poskytovatelů strategicky významné služby. Dojde k prodloužení kontraktačního procesu a dalších procesů souvisejících s pořizováním nových bezpečnostně významných dodávek vč. zpomalení výběrových řízení. V důsledku toho může dojít ke zdržení investic a zpomalení rozvoje, což může způsobit také časové prodlení při realizaci výstavby dané strategicky významné infrastruktury.

3.2.5.4. Vd: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce pouze v sektoru elektronických komunikací

Náklady podvarianty Vd jsou zcela shodné s náklady varianty Va. Jediný rozdíl mezi těmito dvěma variantami je v rozsahu poskytovatelů strategicky významné služby, neboť varianta Va reguluje pouze sektor elektronických komunikací. Náklady se tak budou dotýkat menšího počtu poskytovatelů strategicky významné služby i dodavatelů.

Dále budou i menší náklady na straně státu, jelikož bude posuzován značně menší počet dodavatelů, a to vzhledem k tomu, že poskytovateli strategicky významné služby podle podvarianty Vd jsou pouze jednotky subjektů. Náklady na straně státu by tak byly sníženy zhruba na desetinu nákladů Varianty Va.

3.3. Přínosy

Identifikovaný přínos	Varianta				
	I	II	III	IV	V
plná transpozice směrnice	ne	ano	ano	ano	ano
splnění požadavku Bezpečnostní rady státu na úpravu mechanismu prověřování bezpečnosti dodavatelského řetězce	ne	ne	ne	ano	ano
dvourychlostní kybernetická bezpečnosti	ne	ne	ano	ne	ano
souhrnné náklady	-	VN	VR	VN + BDŘ	VR + BDŘ
reflexe dosavadních poznatků	ne	ne	ano	ne	ano

Legenda

ano – přínos je naplněn

ne – přínos není naplněn

„-“ – přínos není relevantní

VN – náklady jsou výchozí (plnění požadavku směrnice) a neredukované (nejsou zavedeny mechanismy a instituty na jejich úpravu, resp. snížení)

VR – náklady jsou výchozí (plnění požadavku směrnice), ale jsou vhodně redukovány (jsou zavedeny mechanismy a instituty na jejich úpravu, resp. snížení - např. dvourychlostní kybernetická bezpečnosti, apod.)

BDŘ – náklady jsou spojeny s náklady na proces mechanismu prověřování bezpečnosti dodavatelského řetězce

3.3.1. Varianta I: Nulová varianta – zachování současného stavu

Se zachováním současného stavu nejsou (bez přihlédnutí k chybějícímu mechanismu prověřování bezpečnosti dodavatelského řetězce) spojeny žádné přínosy.

Přijetí nulové varianty by s velkou pravděpodobností bylo Evropskou komisí považováno za nesplnění povinnosti vyplývající ČR z primárního práva EU (Smlouva o Evropské unii a Smlouva o fungování Evropské unie), přičemž by Evropská komise na základě čl. 258 Smlouvy o fungování Evropské unie mohla předložit tuto záležitost Soudnímu dvoru Evropské unie.

Pokud jde o mechanismus prověřování bezpečnosti dodavatelského řetězce, za jediný přínos nulové varianty lze považovat, že kontinuita současného stavu (absence mechanismu) není spojena s novými přímými náklady na výkon veřejné správy ani náklady na straně dotčených regulovaných osob.

Současně však platí, že nulová varianta neřeší problémy, které jsou základním důvodem předložení návrhu zákona, a že nepřijetí legislativních změn může přinést náklady spojené s náhradou či nápravou škod, které by vyplynuly z činnosti rizikového dodavatele, jenž by poškodil významnou strategickou infrastrukturu ČR. Dále je namístě zmínit nevyčíslitelnou strategickou hrozbu v podobě závislosti na rizikových dodavatelích či přítomnosti technologií

vysoce rizikových dodavatelů ICT ve strategické infrastruktuře. Může dojít k omezení volnosti strategického rozhodování ČR, neboť bude nutné vzít v potaz možnost zneužití přítomnosti rizikových dodavatelů cizím státem, což může zamezit strategické autonomii ČR.

V neposlední řadě hrozí poškození reputace ČR, která je dlouhodobě v Evropě považována za vedoucí stát v oblasti kybernetické bezpečnosti.

3.3.2. Varianta II: Transpozice směrnice bez zohlednění mechanismu prověřování bezpečnosti dodavatelského řetězce a odstranění zjištěných nedostatků a reflexe dosavadních zkušeností (minimální transpozice směrnice)

V případě varianty II se přínosy realizují jen omezeně. Zajištění nedistributivních práv, práva na informační sebeurčení nebo důvěry občana ve stát a jeho instituce jistě nebude touto variantou poškozeno (při této variantě prakticky dochází „pouze“ k rozšíření stávající regulace, a tedy aplikaci dosavadních požadavků, na nové povinné osoby). Také teze o zvýšení bezpečnosti důležitých společenských funkcionalit, snížení škodlivých následků kybernetických bezpečnostních incidentů nebo zvýšení míry motivace tuzemských a zahraničních investic zde naleznou své uplatnění.

K nezavedení mechanismu prověřování bezpečnosti dodavatelského řetězce je namístě odkázat na vyhodnocení přínosů v případě varianty I.

3.3.3. Varianta III: Transpozice směrnice bez zohlednění mechanismu prověřování bezpečnosti dodavatelského řetězce ovšem při odstranění zjištěných nedostatků a reflexe dosavadních zkušeností

V případě varianty III se výše identifikované přínosy realizuji více než v případě varianty II, avšak bez zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce stále omezeně. Přínosy této varianty jsou odvozeny zejména v racionalizaci procesů upravených návrhem zákona (v návaznosti na reflexi dosavadních zkušeností s jejich aplikací za účinnosti zákona o kybernetické bezpečnosti) a přizpůsobení celého ekosystému enormnímu nárůstu počtu regulovaných subjektů. Stejně jako v případě varianty II dojde k zachování zajištění nedistributivních práv, práva na informační sebeurčení nebo důvěry občana ve stát a jeho instituce. Také teze o zvýšení bezpečnosti důležitých společenských funkcionalit, snížení škodlivých následků kybernetických bezpečnostních incidentů nebo zvýšení míry motivace tuzemských a zahraničních investic zde budou moci být aplikovány. Zařazení nových subjektů do regulace a přizpůsobení jejich povinností a způsobu dohledu plnění těchto povinností počtu a charakteru nově regulovaných organizací by bezesporu mělo vést k celkovému zvýšení úrovně kybernetické bezpečnosti celospolečensky důležitých služeb, stejně jako k pozitivní motivaci tuzemských i zahraničních investorů.

K nezavedení mechanismu prověřování bezpečnosti dodavatelského řetězce je namístě odkázat na vyhodnocení přínosů v případě varianty I.

3.3.4. Varianta IV: Transpozice směrnice zároveň zohledňující mechanismus prověřování bezpečnosti dodavatelského řetězce, ovšem bez odstranění zjištěných nedostatků a reflexe dosavadních zkušeností

V případě varianty IV se identifikované přínosy realizují, s výjimkou mechanismus prověřování bezpečnosti dodavatelského řetězce, stejným způsobem jako v případě varianty II. S ohledem na skutečnost, že níže (4. Návrh řešení) byla vybrána jako nejvhodnější řešení varianta V, náklady jednotlivých podvariant jsou specifikovány právě v souvislosti s variantou V níže.

3.3.5. Varianta V: Transpozice směrnice, zohlednění mechanismu prověřování bezpečnosti dodavatelského řetězce a odstranění zjištěných nedostatků a reflexe dosavadních zkušeností

V případě varianty V se identifikované přínosy realizují naplno.

Zajištění nedistributivních práv, práva na informační sebeurčení nebo důvěry občana ve stát a jeho instituce, stejně tak jako zvýšení bezpečnosti důležitých společenských funkcionalit, snížení škodlivých následků kybernetických bezpečnostních incidentů nebo zvýšení míry motivace tuzemských a zahraničních investic, má v případě této varianty ze všech hodnocených variant největší možnost realizace.

3.3.5.1. Podvarianta Va: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře

Přínos této podvarianty spočívá v přijetí komplexního mechanismu prověřování bezpečnosti dodavatelského řetězce, jenž umožní Úřadu na základě zákonného zmocnění omezit či vyloučit z vymezených dodávek poskytovatelů strategicky významné služby takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií.

Realizace podvarianty Va přispěje ke stabilitě a zabezpečení poskytování služeb jednotlivých strategických sektorů, a také k zajištění dlouhodobě udržitelného zabezpečení a odolnosti infrastruktury, jež je nezbytná pro naplňování základních funkcí státu. Dojde k omezení závislosti strategicky významné infrastruktury ČR na rizikových dodavatelích představujících strategickou hrozbu v oblasti kybernetické bezpečnosti. Dojde tak také k významnému omezení možnosti negativního zahraničního působení na zajištění základních funkcí státu prostřednictvím zneužití závislosti v dodavatelsko-odběratelských vztazích, jako je proprietární uzamčení odběratele, tzv. vendor lock-in, nevynucené omezení dodávek či zneužití infrastruktury nebo neoprávněný zásah do ní.

Dále díky intenzívnějšímu informování poskytovatelů strategicky významné služby o hrozbách spojených s rizikovými dodavateli bude realizace podvarianty Va přispívat k tomu, že poskytovatelé strategicky významné služby začnou i sami klást větší důraz na bezpečnost, a to včetně aspektů rizikovosti, které posuzuje stát. Tato podvarianta má také ambici změnit přístup samotných poskytovatelů strategicky významné služby k výběru dodavatelů. Poskytovatelé strategicky významné služby by měli klást větší důraz na bezpečnost a menší důraz pouze na pořizovací cenu ICT produktů a služeb. Dodavatelé, kteří budou nabízet bezpečná ICT řešení, a to jak z pohledu technického, tak strategického, by tak získávali konkurenční výhodu oproti dodavatelům, kteří nejsou schopni takové záruky poskytnout.

Přínosem pro proces je i zapojení Bezpečnostní rady státu, jakožto pracovního orgánu vlády ČR v bezpečnostních otázkách, ministerstev a případně i sektorových regulátorů. Tyto orgány zváží proporcionalitu zásahu způsobeného návrhem OOP s ohledem na významné ohrožení bezpečnosti ČR nebo vnitřního pořádku ve srovnání s dalšími chráněnými hodnotami.

Rozhodnutí o omezení dodavatele je implicitně zatíženo značným korupčním rizikem, jako vhodné řešení se jeví právě existence transparentních kritérií a rozhodování o možném významném ohrožení bezpečnosti ČR nebo vnitřního pořádku na základě vyhodnocení těchto kritérií. Příslušný ústřední správní orgán rozhodne o případném omezení dodavatele na základě vlastního šetření i sběru informací od ostatních zapojených státních orgánů. Obdobný proces již v českém právním řádu existuje, jedná se např. o proces prověřování žadatelů o zápis do

katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy, který je zaveden do české právní úpravy zákonem o informačních systémech veřejné správy.

3.3.5.2. Podvarianta Vb: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře se zapojením vlády ČR

Přínos této podvarianty, obdobně jako u podvarianty Va, spočívá v přijetí komplexního Mechanismu posuzování dodavatelů. V podvariantě Vb by v případě kratších odpisových lhůt vláda ČR svým usnesením stanovila, jakým způsobem má Úřad postupovat v případě vydávání OOP a tím měla přímý vliv na provádění závažných rozhodnutí v otázkách bezpečnosti státu se značným ekonomickým i zahraničněpolitickým dopadem. Obecně tak lze říci, že by vláda ČR byla zapojena do procesu vydání OOP v případě, že by zjištěné riziko bylo tak velké, že by odůvodňovalo postup pro rychlejší omezení či vyřazení dodavatele, což by sebou přineslo také větší dopady na poskytovatele strategicky významných služeb i na poskytování strategicky významných služeb jako takových. Navržená varianta přistupuje k problematice omezování dodavatelů jako k problematice, jež má být řešena na nejvyšší politické úrovni, neboť v sobě obsahuje řešení zásadních bezpečnostních otázek a zároveň možný významný zásah do soukromého vlastnictví.

Rozhodnutí o omezení dodavatele je implicitně zatíženo značným korupčním rizikem, tudíž jako vhodné řešení se jeví právě zapojení kolektivního orgánu na nejvyšší politické úrovni.

3.3.5.3. Podvarianta Vc: Mechanismus plošného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře

Přínos této podvarianty spočívá v přijmutí komplexního mechanismu prověřování bezpečnosti dodavatelského řetězce, jenž umožní Úřadu na základě zákonného zmocnění omezit či vyloučit z vymezených dodávek poskytovatelů strategicky významné služby takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií. To přispěje ke stabilitě a zabezpečení poskytování služeb jednotlivých strategických sektorů, a také k zajištění dlouhodobě udržitelného zabezpečení a odolnosti infrastruktury, jež je nezbytná pro naplňování základních funkcí státu.

Přínosem této podvarianty je taktéž to, že do vymezené strategicky významné infrastruktury nebudou mít přístup žádní dodavatelé, kteří nebudou předem systematicky a předvídatelně prověřeni.

3.3.5.4. Podvarianta Vd: Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce v sektoru elektronických komunikací

Přínos této podvarianty spočívá v přijmutí komplexního mechanismu prověřování bezpečnosti dodavatelského řetězce, jenž umožní Úřadu na základě zákonného zmocnění omezit či vyloučit z vymezených dodávek poskytovatelů strategicky významné služby v sektoru elektronických komunikací takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií v sektoru elektronických komunikací. To přispěje ke stabilitě a zabezpečení poskytování služeb v sektoru elektronických komunikací, a také k zajištění dlouhodobě udržitelného zabezpečení a odolnosti infrastruktury v sektoru elektronických komunikací, jež se podílí na naplňování základních funkcí státu.

Dále díky intenzivnějšímu informování poskytovatelů strategicky významné služby v sektoru elektronických komunikací o hrozbách spojených s rizikovými dodavateli bude realizace podvarianty Vd přispívat k tomu, že poskytovatelé strategicky významné služby v sektoru elektronických komunikací začnou i sami klást větší důraz na bezpečnost, včetně aspektů rizikovosti, které posuzuje stát. Tato varianta má také ambici změnit přístup samotných poskytovatelů strategicky významné služby v sektoru elektronických komunikací k výběru dodavatelů. Poskytovatelé strategicky významné služby v sektoru elektronických komunikací by měli klást větší důraz na bezpečnost a menší důraz pouze na pořizovací cenu ICT produktů a služeb. Dodavatelé v sektoru elektronických komunikací, kteří budou nabízet bezpečná ICT řešení, a to jak z pohledu technického, tak strategického, by tak získávali konkurenční výhodu oproti dodavatelům, kteří nejsou schopni takové záruky poskytnout.

4. Návrh řešení

4.1. Komparace zahraničních přístupů k mechanismu bezpečnosti dodavatelského řetězce

4.1.1. Přístupy v Evropě

V rámci Evropské unie je vzhledem k principu volného pohybu zboží a služeb na jednotném vnitřním trhu znemožněno plošně zakázat výrobky či služby určitých dodavatelů napříč všemi členskými státy. Přesto však bylo s ohledem na rostoucí bezpečnostní hrozby přijato několik koordinovaných opatření:

Toolbox pro zmírnění rizik 5G sítí (2020) stanovuje soubor objektivních kritérií pro posuzování rizikových dodavatelů 5G technologií a navrhuje opatření k omezení rizik plynoucích z těchto dodavatelů na přijatelnou úroveň. Na základě tohoto dokumentu následně členské státy přistoupily k posílení svých národních bezpečnostních mechanismů v oblasti 5G sítí.

Dalším klíčovým dokumentem je směrnice NIS 2, která by měl ode dne 18. října 2024 nahradit stávající právní úpravu obsaženou ve směrnici NIS. Výše uvedená směrnice NIS 2 nově ukládá členským státům povinnost přijmout opatření vůči dodavatelům, u nichž existují obavy z kybernetických bezpečnostních rizik. Reaguje tak na nové trendy a hrozby, jako je rostoucí koncentrace trhu s klíčovými dodavateli technologií nebo zvyšující se četnost sofistikovaných kybernetických útoků zneužívajících zranitelnosti v komerčním softwaru a hardwaru.

Na základě těchto iniciativ na unijní úrovni řada členských států již přistoupila k přijetí vlastních legislativních nástrojů pro řešení rizik spojených s vlivem rizikových dodavatelů, přičemž tato opatření se zaměřují zejména na problematiku budování 5G sítí. Mezi státy, které přijaly regulaci v této oblasti, patří Polsko, Rumunsko, Estonsko, Lotyšsko, Litva, Řecko, Itálie, Švédsko, Francie, Německo či Velká Británie.

Přístupy jednotlivých zemí se přitom částečně liší v míře přísnosti vůči rizikovým dodavatelům. Některé státy zvolily cestu úplného zákazu určitých dodavatelů či jejich technologií (např. Polsko, Rumunsko, Estonsko, Lotyšsko, Litva, Švédsko). Jiné země se vydaly spíše směrem umožňujícím posouzení rizik jednotlivých dodavatelů a jejich následné případné vyloučení na základě provedeného bezpečnostního auditu (např. Řecko, Itálie, Francie). Další skupinu tvoří státy, které sice vysoce rizikové dodavatele nezakázaly, ale zpřísnily kontrolní mechanismy a požadavky na bezpečnost telekomunikačních sítí, což de facto vede k omezení využití některých rizikových technologií (např. Německo, Velká Británie).

Rozsah přijímaných opatření se také různí. Zatímco některé státy se soustředí primárně na 5G sítě, jiné již dnes budují komplexní rámec pro řešení rizik napříč kritickou informační infrastrukturou bez ohledu na konkrétní technologickou oblast.

4.1.2. Přístupy mimo EU

Přístupy k regulaci rizikových dodavatelů v dodavatelských řetězcích jsou nejlépe zdokumentovány na příkladu čínských společností Huawei a ZTE. Z toho důvodu se níže pracuje právě s těmito významnými dodavateli. Je však potřeba mít na paměti, že problematika regulace dodavatelského řetězce je širší než jedna společnost a pokrývá více než jeden stát.

Mezi nejvýznamnější státy, které se intenzivně zabývají riziky spojenými s využíváním produktů a služeb čínských technologických společností (zejména Huawei a ZTE) ve svých kritických informačních infrastrukturách, patří Spojené státy, Austrálie a Nový Zéland.

Spojené státy v roce 2019 zařadily společnost Huawei na tzv. "entity list" tamního Ministerstva obchodu, což jí fakticky znemožnilo obchodování s americkými firmami. USA dále zakázaly vládním institucím využívat telekomunikační vybavení Huawei a ZTE a zároveň vyvíjely tlak na soukromé mobilní operátory k vyřazení tohoto vybavení z jejich sítí. V reakci na očekávané náklady byly přijaty speciální pobídkové programy na podporu náhrady čínských technologií v mobilních sítích.

Austrálie v roce 2018 zcela zakázala, aby společnosti Huawei a ZTE dodávaly technologie pro 5G sítě budované na území Austrálie. Učinila tak s odkazem na bezpečnostní rizika spojená s produkty těchto dodavatelů a též kvůli obavám z jejich možného zneužití pro kybernetické útoky či narušení kritické infrastruktury. Podobný krok již o něco dříve učinil i telekomunikační regulátor Nového Zélandu, který hlavnímu mobilnímu operátorovi (společnosti Spark New Zealand Trading Limited) zakázal využívat 5G vybavení od společnosti Huawei v jeho mobilní síti s odůvodněním existence významného bezpečnostního rizika.

Japonsko sice samo nepřistoupilo k zákazu využívání produktů Huawei a ZTE, nicméně bylo v roce 2018 prvním státem, který vydal varování před kybernetickými bezpečnostními riziky spojenými s využíváním čínského telekomunikačního vybavení ve vládních sítích. Na základě tohoto varování bylo vládním institucím doporučeno přesunout se k využívání řešení od jiných dodavatelů.

Tchaj-wan v roce 2021 přijal opatření, na jehož základě začal platit zákaz prodeje produktů společností Huawei a ZTE subjektům, které dodávají služby pro vládní instituce a vojenské úřady Tchaj-wanu. Jedná se tedy o dílčí omezení zasahující pouze státní sféru.

4.1.3. Přístup ČR

V ČR by měl danou problematiku řešit nový zákon o kybernetické bezpečnosti, který zavede mechanismus pro prověřování bezpečnosti dodavatelských řetězců u strategicky významné infrastruktury (strategicky významných služeb). Cílem je omezit závislost na dodavatelích představujících riziko pro národní bezpečnost a vnitřní pořádek ČR.

Úřad bude pověřen identifikací a vyhodnocováním hrozeb plynoucích z dodavatelských řetězců na základě stanovených podmínek. V případě vyhodnocení dodavatele jako rizikového bude moci Úřad omezit nebo vyloučit jeho technologie z dodávek pro vybrané povinné subjekty poskytující služby strategického významu. Závažnější případy budou podléhat schválení některými dalšími ústředními orgány státní správy.

Nová právní úprava tak vytvoří komplexní systém pro omezování strategických rizik spojených s dodavateli kritických technologií pro nejdůležitější infrastrukturu, aniž by měnila stávající principy regulace kybernetické bezpečnosti.

ČR tak volí cestu umožňující flexibilní posouzení a případné vyloučení rizikových dodavatelů ze strategických odvětví na základě bezpečnostní analýzy. Zároveň ale zachovává možnost využití jejich produktů a služeb v méně kritických segmentech infrastruktury.

V rámci přípravy nového právního rámce pro posílení kybernetické bezpečnosti ČR byla provedena analýza zahraničních přístupů k řešení rizik plynoucích z využívání zboží a služeb rizikových dodavatelů v kritické informační infrastruktuře a strategických odvětvích. Cílem bylo identifikovat osvědčené postupy a inspirovat se mechanismy aplikovanými v jiných státech při tvorbě vlastní právní úpravy.

Motivací přijímaných opatření všech výše uvedených států je rostoucí obava z možného zneužití telekomunikačních a dalších informačních a komunikačních technologií pro účely kybernetických útoků, narušení kritické infrastruktury či možné špionážní aktivity ze strany rizikových dodavatelů. Zásadním faktorem je tak snaha o zvýšení kybernetické odolnosti a snížení závislosti na rizikových dodavatelích. Přístupy jednotlivých zemí se nicméně liší v rozsahu omezení, tj. zda se vztahují pouze na určitá odvětví kritické infrastruktury (např. jen na telekomunikační sítě) nebo se uplatní napříč všemi klíčovými obory. Míra přísnosti přijímaných opatření se pohybuje od úplných zákazů, přes možnost vyloučení na základě posouzení bezpečnostních rizik, až po obecnější zpřísněné kontrolní mechanismy a požadavky pro dodavatele.

Komparační kritéria

Pro účely srovnávací analýzy byly státy rozděleny do několika kategorií podle míry přísnosti jejich přístupu k bezpečnosti dodavatelského řetězce v klíčových sektorech jako jsou telekomunikace, energetika či doprava. Hlavními kritérii pro hodnocení přísnosti byly:

a) Rozsah regulace – zda se vztahuje pouze na telekomunikační sítě (5G) nebo komplexně řeší rizika napříč kritickou infrastrukturou.

b) Míra omezení vůči rizikovým dodavatelům – od úplného zákazu, přes možnost vyloučení na základě posouzení kritérií, až po obecná bezpečnostní doporučení.

c) Postup při omezování rizikových technologií – zda existuje časový rámec pro jejich postupné vyřazení nebo jsou odstraněny bez přechodného období.

d) Úroveň transparentnosti a konzultací v rozhodovacím procesu o omezování dodavatelů.

Státy s přísnějším přístupem než ČR (v EU i mimo ni)

Do této kategorie spadají země, které přistoupily k úplnému zákazu využívání produktů a služeb konkrétních rizikových dodavatelů, zejména čínských firem Huawei a ZTE. Patří sem například Polsko, Rumunsko, Estonsko, Lotyšsko, Litva, Švédsko, Austrálie, USA, Nový Zéland a další. Jejich motivací jsou převážně bezpečnostní obavy z možného zneužití technologií pro špionáž, narušení infrastruktury či kybernetické útoky. Přístup bývá nejpřísnější v oblasti 5G mobilních sítí.

Státy se stejně či podobně přísným přístupem jako ČR

Do této skupiny lze zařadit země, které neumožňují úplné zákazy, ale mají mechanismy pro individuální posuzování rizik u jednotlivých dodavatelů a případné omezení či vyloučení jejich produktů a služeb na základě stanovených kritérií a transparentního procesu. Jde například o Německo, Francii, Nizozemsko, Rakousko, Slovensko, Španělsko a některé další. Řada z nich v současnosti řeší spíše 5G sítě, avšak s výhledem rozšíření na další kritickou infrastrukturu.

ČR po vzoru těchto států volí cestu umožňující flexibilní posouzení rizik se zachováním možnosti využití produktů rizikových dodavatelů v méně kritických částech infrastruktury. Zároveň ale vytváří komplexnější systém pro klíčová odvětví.

Méně přísné přístupy

Některé státy doposud přistupují k řešení rizik spojených s dodavateli poměrně vstřícně, s minimem regulačních zásahů. Patří sem například Belgie, Itálie, Chorvatsko, ale též ČR se svým současným dílčím přístupem. Mezi v této oblasti zcela neaktivní země se v současné době řadí Bulharsko, Maďarsko, Malta, Řecko, Slovinsko a některé další.

Výhody a nevýhody jednotlivých přístupů

Přísnější úplné zákazy přinášejí vyšší míru kontroly a eliminaci rizik, ovšem za cenu možných vysokých nákladů na rychlou obměnu zařízení, narušení kontinuity služeb, ztrátu konkurenceschopnosti či vzniku bezpečnostních rizik při unáhleném přerušení dodávek. Flexibilnější, méně striktní model posuzování rizik dává větší manévrovací prostor a díky individuálnímu posouzení jednotlivých případů umožňuje přizpůsobení charakteru bezpečnostního hodnocení dodavatele a jeho produktů reálným možnostem a prioritám dané země. Na druhou stranu přináší zvýšenou administrativní zátěž a určitá rizika v případě selhání kontrolních mechanismů.

Po kritickém zhodnocení různých zahraničních přístupů byla zvolena cesta kombinující prvky nejpřísnějších, úplných zákazů se zaměřením na nejvýznamnější součásti kritické infrastruktury s flexibilnějším modelem posuzování rizik pro méně strategické oblasti. Tento vyvážený přístup by měl zajistit potřebnou úroveň kontroly nad rizikovými dodavateli při zachování přijatelné míry praktické aplikovatelnosti a minimalizaci potenciálních negativních vedlejších dopadů.

Odůvodnění výsledné podoby mechanismu řešení rizik spojených s dodavateli technologií pro kritickou infrastrukturu v ČR

Navrhovaný mechanismus řešení rizik spojených s dodavatelským řetězcem v ČR vychází z kombinace analyzovaných zahraničních přístupů a specifik českého právního prostředí. Podobně jako v řadě jiných zemí EU (např. Německo, Francie, Nizozemsko, Rakousko), je i pro účely české právní úpravy zvolen model individuálního posuzování jednotlivých dodavatelů podle stanovených kritérií s možností jejich případného omezení či vyloučení. Tato flexibilní cesta umožňuje přizpůsobení postupu reálným možnostem a minimalizaci negativních dopadů.

Na rozdíl od některých států jako Dánsko, Litva či Estonsko, kde může docházet k plošnému a neprodlenému odstranění určitých rizikových technologií bez přechodného období, počítá český přístup s vymezeným časovým rámcem pro případnou obměnu zařízení po oznámení rizika. Tím jsou jednotlivým subjektům, jichž se proces hodnocení bezpečnosti dodavatelského řetězce určitým způsobem týká, dány přiměřené lhůty pro přizpůsobení se konkrétní nastalé situaci.

Rozsahem své věcné působnosti jde český návrh nad rámec mnoha jiných přístupů zaměřených pouze na telekomunikační sítě a pokrývá komplexně kritickou informační infrastrukturu napříč klíčovými sektory (energie, doprava, zdravotnictví apod.). Tato skutečnost odráží zvýšené požadavky na odolnost i v dalších kritických odvětvích.

Při koncipování mechanismu byl rovněž zohledněn současný stav právní úpravy v ČR tak, aby touto novou regulací nebyly řešeny otázky již ošetřené jinými předpisy, a nedocházelo tím ke zbytečnému zdvojování právní úpravy. Přístup ČR vychází z nejlepších zahraničních vzorů, ale současně zohledňuje i specifické podmínky a potřeby státu při zachování legislativní

konzistence. Aplikace neadekvátního mechanismu pro naše bezpečnostní prostředí by kromě jiného měla extrémní finanční dopady především na povinné subjekty poskytující služby kritické infrastruktury. Tomu je zabráněno zvolením patřičných prvků mechanismu relevantních a aplikovatelných pro ČR.

Příklad neslučitelnosti jiného mechanismu a odůvodnění

Pro demonstraci odlišných přístupů z důvodu lišící se legislativy i bezpečnostního prostředí může posloužit vzájemná komparace mechanismů v USA a ČR. USA používají mechanismus „černé listiny" (tzv. blacklist), na který může ad hoc přidávat rizikové dodavatele. Tento přístup se liší od flexibilního modelu individuálního hodnocení jednotlivých dodavatelů zvolených v ČR. Důvodem odlišnosti přístupu používaného v USA je především charakter právního prostředí USA, které se od podmínek ČR liší.

V USA existuje větší prostor pro přímé obchodní sankce vůči zahraničním subjektům z důvodů národní bezpečnosti na úrovni federální legislativy. Seznam subjektů podléhajících obchodním omezením (tzv. Entity List) je dlouhodobě zavedeným nástrojem, který umožňuje rychlé vyloučení subjektů z obchodních vztahů.

Na druhou stranu v ČR je při omezování přístupu dodavatelů na trh nutné postupovat transparentními procesy a objektivně zkoumat naplnění kritérií vycházejících z legislativy, která současně musí být v souladu s požadavky volného pohybu zboží a služeb na jednotném trhu EU. Proto byl zvolen model hodnocení založený na stanovených kritériích, který je více v souladu s tímto unijním právním rámcem.

Dalším faktorem je rozsah, v jakém se omezený přístup uplatňuje. Zatímco americká černá listina je obecným nástrojem s přímým účinkem ve všech odvětvích ekonomiky, v ČR je mechanismus primárně zaměřen na zajištění kybernetické bezpečnosti kritické informační infrastruktury.

4.2. Stanovení pořadí variant a výběr nejvhodnějšího řešení

Jako nejvhodnější řešení byla vybrána varianta V, tedy jak transpozice směrnice, tak zohlednění mechanismu prověřování bezpečnosti dodavatelského řetězce a odstranění zjištěných nedostatků a reflexe dosavadních zkušeností. Realizace této varianty si z důvodu rozsahu změn vyžádá zrušení stávajícího zákona o kybernetické bezpečnosti a schválení nového zákona o kybernetické bezpečnosti.

Varianty II a IV by sice mohly být zvoleny s cílem realizovat co nejjednodušeji povinnost transpozice evropského právního předpisu do českého právního řádu, ale pokud nebudou v rámci transpozice směrnice provedeny dodatečné úpravy zákona o kybernetické bezpečnosti, je téměř nemožné dané změny realizovat takovým způsobem, aby zákon i nadále plnil svou funkci a distribuce nákladů byla smysluplná. Varianta III pak sice splňuje požadavky směrnice a odstraňuje nedostatky uvedené u variant II a IV, ovšem v rámci ní chybí také podstatný prvek, kterým je zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, a který přináší podstatné kroky k posílení bezpečnosti ČR. Varianta I se s ohledem na výše popsané důsledky a s nimi souvisejícími náklady nedoporučuje přijmout a zařazuje se na poslední místo v pořadí variant.

Navrhuje se přijmout variantu V. Pokud jde o jednotlivé podvarianty, platí následující:

Podvarianta Va – Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře řeší diskutovaný problém v celé jeho šíři a dosahuje zamýšleného cílového stavu. Zároveň minimalizuje dodatečné náklady dotčených subjektů spojené s extenzivnější variantou Vc, čímž zachovává proporcionalitu mezi dosažením cílového stavu a minimalizací zásahu do práv osob. Do procesu zahrnuje jako garanta

proporcionality Bezpečnostní radu státu, jakožto pracovní orgán vlády ČR, a další relevantní orgány, jako je Ministerstvo financí a další orgány zapojené do procesu, případně budou nutné přímo závazné stanovisko Ministerstva průmyslu a obchodu, Ministerstva zahraničních věcí a Ministerstva vnitra. Proces proporcionality bude zajištěn také zapojením sektorových regulátorů (Český telekomunikační úřad a Energetický regulační úřad) v případech, kdy se opatření obecné povahy bude dotýkat jejich působnosti. Na rozdíl od podvarianty Vb je proces zúžen na několik klíčových ministerstev, což může vést k nižší míře kontroly, ale k větší pružnosti a ke zkrácení lhůty nutné pro vydání OOP.

Podvarianta Vb – Mechanismus cíleného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře se zapojením vlády ČR řeší diskutovaný problém v celé jeho šíři a dosahuje zamýšleného cílového stavu. Do procesu prověřování je zapojena vláda ČR, jejíž usnesení o tom, jak má Úřad ve věci vydání konkrétního OOP postupovat, je nezbytnou podmínkou k vydání OOP, ve kterém Úřad poskytovatelům strategicky významné služby stanoví podmínky prověřování nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. Celý proces je tím prodloužen, ale o nutnosti vydat OOP rozhoduje nejvyšší kolektivní politický orgán, což značně posílí jeho legitimitu a právní sílu.

Podvarianta Vc – Mechanismus plošného prověřování bezpečnosti dodavatelského řetězce ve strategicky významné infrastruktuře navrhovaný problém řeší v celé jeho šíři a dosahuje zamýšleného cílového stavu. Na druhou stranu ovšem přináší významné, až neproporční zvýšení nákladů jak na straně státu, tak na straně ostatních dotčených subjektů.

Podvarianta Vd – Mechanismus prověřování bezpečnosti dodavatelského řetězce v sektoru elektronických komunikací řeší definovaný problém pouze částečně, a to ve vybraném sektoru elektronických komunikací. Nemá tak potenciál plně dosáhnout požadovaného cílového stavu, k jeho plnění pouze přispívá, byť za vynaložení minimálních nákladů.

S ohledem na míru naplnění požadovaného cílového stavu a minimalizaci nákladů s tím spojených došlo k vyhodnocení vhodnosti podvarianty Va nebo podvarianty Vb. Při vyhodnocování podvariant Va a Vb bylo porovnáváno zejména to, jaký model mechanismu je nejvhodnější variantou pro posuzování dodavatelů. Oba modely, tedy podvarianta Va, kdy o vydání OOP rozhoduje sám Úřad (v závažnějších situacích podléhající vydání souhlasného stanoviska od Ministerstva průmyslu a obchodu, Ministerstva zahraničních věcí a Ministerstva vnitra), tak i podvarianta Vb, ve které je vydání OOP Úřadu podmíněno usnesením vlády, v českém právním řádě existují. Podvarianta Va přináší obdobný proces jako prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné správy zavedený do české právní úpravy zákonem o informačních systémech veřejné správy.

Podvarianta Vb nabízí obdobný proces jako zákon o prověřování zahraničních investic či sankční zákon, jelikož podmiňuje vydání OOP, které stanovuje podmínky či zakazuje využití dodavatele, usnesením vlády ČR. Předkladatel vyhodnotil, že navrhuje přijmout podvariantu Va, a to především z důvodu, že podvarianta Va nabízí systematické posuzování dodavatelů podle transparentních kritérií a současně zachovává strategický dohled pracovního orgánu vlády ČR.

4.3. Zvolené řešení právní úpravy

4.3.1. Návrh zákona

Pouze varianta V je komplexní a vnitřně koherentní právní úpravou, která dosahuje cílů stanovených v podkapitole 1.5. Tato varianta je postavena na převzetí všech požadavků

směrnice NIS 2 (zejm. definování rozsahu této regulace v čl. 2 a 3, stanovení bezpečnostních opatření v čl. 20 a 21 a povinnosti hlášení kybernetických bezpečnostních incidentů v čl. 23), přizpůsobení v co největší míře dosavadnímu obsahu zákona o kybernetické bezpečnosti a zároveň nastavení takových institutů, které budou univerzální a umožní rozvíjet obsah návrhu zákona i v budoucnu, pokud by to bylo potřeba.

Zvolená varianta na rozdíl od zákona o kybernetické bezpečnosti přejímá koncept jednoho hlavního typu povinné osoby, které mají být ukládány povinnosti v oblasti kybernetické bezpečnosti (zejména týkající se zavádění bezpečnostních opatření a hlášení incidentů). Tímto typem povinné osoby je v návrhu zákona tzv. poskytovatel regulované služby. Tato úprava navazuje na obsah směrnice NIS 2, nicméně je také ovlivněna dosavadními zkušenostmi s aplikací zákona o kybernetické bezpečnosti, kdy celkový počet třinácti různých kategorií povinné osoby, které zákon o kybernetické bezpečnosti v průběhu času a novelizací ve svém § 3 postupně reguloval, způsoboval extrémní zmatení u adresátů této normy. S tím souvisí také celkové zjednodušení používaného pojmosloví.

Směrnice NIS 2 přináší rozdělení povinných osob na tzv. „*essential entity*“ a „*important entity*“. Vybraná varianta tento koncept přejímá a povinnou osobu poskytovatele regulované služby vnitřně dělí do dvou skupin, tzv. režimů. Režimy vyjadřují rozsah povinností ukládaných jednotlivým poskytovatelům regulované služby a jsou odrazem přiměřenosti regulace v rámci principu minimalizace státního donucení, na kterém je postavena jak dosavadní právní úprava, tak návrh zákona. S enormním nárůstem povinných osob, tak jak je jejich okruh stanoven ve směrnici NIS 2, je potřeba přejít na tento tzv. dvourychlostní princip.

Enormní nárůst povinných osob, zároveň však zjednodušení identifikačních kritérií vedou k tomu, že dosavadní vedení správního řízení s každou budoucí povinnou osobou (což byl dominantní způsob určení povinné osoby podle zákona o kybernetické bezpečnosti) bude nahrazeno tzv. samoidentifikací (tento princip se v souladu se zákonem o kybernetické bezpečnosti používal u tzv. významných informačních systémů) s následnou registrací u Úřadu. Tento model umožňuje pojmout v krátkém čase větší množství povinných osob, na druhou stranu klade vyšší nároky na zodpovědný přístup adresátů normy. Zkušenosti získané se samoidentifikací významných informačních systémů podle zákona o kybernetické bezpečnosti je potřeba vzít v potaz, a zahrnout do návrhu zákona pojistky a zlepšení, které umožní bezproblémové fungování samoidentifikace nových povinných osob.

Návrh zákona je potřeba postavit na zkušenostech a znalostech získaných z fungování zákona o kybernetické bezpečnosti. Na východiscích preventivního závádění bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů nebo na veřejnoprávním dohledu nad plněním těchto povinností není potřeba v zásadě nic měnit, požadavky kladené směrnicí NIS 2 jsou s těmito principy v souladu, resp. přinášejí jen zvýšenou míru detailu regulace. Varianta V tedy zachovává všechny doposud známé povinnosti povinné osoby, byť v některých případech doplněné o povinnosti nové (zajištění dostupnosti strategicky významné služby nebo informační povinnost poskytovatele regulované služby). Z velké části se jedná o povinnosti stejné pro oba režimy poskytovatelů regulovaných služeb, na druhou stranu i v tomto případě je realizován princip dvourychlostní kybernetické bezpečnosti. Ty povinnosti, které jsou spojené s vyššími náklady a jejichž uložení jedné ze skupin regulovaných osob by nebylo přiměřené, se tedy vůči jednomu z režimů (typicky nižšímu režimu) neuplatní.

S ohledem na změny povinných osob je také nutné změnit dosavadní nastavení stavu kybernetického nebezpečí. Současný stav kybernetického nebezpečí rozšiřuje okruh osob povinných k dodržování opatření Úřadu o organizace, které jsou podle návrhu zákona již standardně regulovaným subjektem. Současné geopolitické trendy nadto ukazují, že stejně jako např. v případě mechanismu prověřování bezpečnosti dodavatelského řetězce, je potřeba připravovat legislativu na možné budoucí výzvy a stanovit v rámci stavu kybernetického

nebezpečí taková opatření, která budou adekvátní k řešení nenadálých situací. Varianta V tedy přináší racionalizovaný stav kybernetického nebezpečí přizpůsobený novým výzvám v kybernetické bezpečnosti a zajišťující Úřadu účinné prostředky pro zvládání či prevenci kybernetických incidentů velkého rozsahu či obdobných krizových stavů *sui generis*.

Navrhovaná úprava stavu kybernetického nebezpečí umožňuje rychlým a zároveň proporcionálním způsobem reagovat na aktuální hrozbu nebo incident v oblasti kybernetické bezpečnosti, přičemž vybraná opatření k řešení stavu kybernetického nebezpečí budou aplikována v reakci na identifikované problémy v nezbytném rozsahu a po nezbytně dlouhou dobu. Oproti jiným podobám zvolená úprava umožňuje v nejhorším možném případě zasáhnout i v případě ohrožení subjektů, na které se běžný zákonný režim nevztahuje.

Tak jako v případě povinných osob, také institucionální pojetí navrhované regulace vychází z již existujícího reálného stavu (Úřad, Národní CERT, Vládní CERT apod.). Na druhou stranu i v souvislosti s výkonem kontroly plnění povinností se výrazně projeví nárůst počtu povinných osob. Je tedy potřeba hledat alternativní institut ke klasickému výkonu kontroly Úřadem.

Jak bylo uvedeno výše (podkapitola 2.5.1.), podvarianta Va současně i Vb (podkapitola 2.5.2) respektují v maximální možné míře stávající performativní povahu pravidel řízení dodavatelů a jiných ustanovení vyhlášky o kybernetické bezpečnosti a zaměřuje prověřování ze strany státu toliko na ty strategické aspekty důvěryhodnosti dodavatelů, jež poskytovatelé strategicky významné služby z podstaty své činnosti (a vzhledem k distribuci pravomocí mezi stát a soukromý sektor) nemohou provádět. Základní tezí zvolené podvarianty je, že případné omezení plynoucí z prověřování by mělo dopadnout pouze na dodavatele poskytující plnění do kritické součásti systému strategicky významné infrastruktury, které má zároveň vliv na bezpečnost regulovaného systému.

Při vymezování části infrastruktury, stejně jako rozsahu dodávek, jejichž dodavatelé mohou být prostřednictvím mechanismu omezeni, byl kladen důraz na vyvážený přístup, který jednak respektuje princip, kdy bezpečnost systémů má být v maximální možné míře v rukou jejich správců, a jednak stát poskytuje povinným subjektům dostatečná vodítka, aby byla aplikace mechanismu u všech povinných subjektů obdobná. Základním předpokladem pro případném omezování posouzeného dodavatele přitom je, že by se mělo jednat pouze o takové dodavatele, jejichž dodávka má či může mít vliv na bezpečnost regulované služby.

Pokud jde o kritickou součást systému strategicky významné infrastruktury, rozumí se jí soubor aktiv regulovaného systému:

i) u kterých správce regulované služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací úrovní vysoká nebo kritická, nebo

ii) které zajišťují funkce regulovaného systému, stanovené prováděcím právním předpisem.

Dodavatel, který může být omezen prostřednictvím mechanismu prověřování, pak bude takový dodavatel, který poskytuje bezpečnostně významnou dodávku do kritické součásti systému strategicky významné infrastruktury. Bezpečnostně významnou dodávkou se rozumí plnění spočívající ve vývoji, výrobě, sestavení či servisu technického vybavení s výpočetní kapacitou nebo programového vybavení, nebo ve vývoji, sestavení, poskytnutí či servisu informační či komunikační služby směřující do kritické části systému.

Kritická část systému je určená poskytovatelem regulované služby, jež má již před přijetím návrhu zákona povinnost podle zákona o kybernetické bezpečnosti, a především jeho prováděcího právního předpisu, vyhlášky o kybernetické bezpečnosti, stanovit metodiku pro identifikaci aktiv, hodnocení aktiv, identifikovat a evidovat aktiva, provádět řízení rizik,

včetně analýzy rizik a další související povinnosti. Identifikace aktiv prováděná správcem regulované služby tak již probíhá v současnosti, a návrh zákona v této souvislosti správcům strategicky významné infrastruktury neurčuje nové povinnosti a navazuje na jejich stávající povinnosti.

Obě podvarianty řešení dále umožňuje prováděcím právním předpisem stanovit funkce regulovaného systému, jež budou příslušnými správci povinně do kritické části systému zahrnuty. Důvod pro existenci takového prováděcího systému je umožnit minimalizovat rozdílnost přístupů identifikace vysokých a kritických aktiv v případech, kdy jsou aktiva dané identifikované funkce nesporně spojená s dopadem narušení bezpečnosti informací úrovní vysoká nebo kritická. Tento prováděcí předpis umožní Úřadu identifikaci takových funkcí, a tedy zamezení rozdílného přístupu k identifikaci aktiv v těch případech, kdy o míře jejich významnosti pro zajištění kybernetické bezpečnosti poskytované služby není pochyb.

Poskytovatelé strategicky významné služby budou povinni nahlašovat Úřadu dodavatele, kteří jim poskytují bezpečnostně významnou dodávku. Nahlášení dodavatele bude znamenat poskytnout Úřadu základní identifikační údaje o dodavateli, předkladatel má tak snahu minimalizovat administrativní náklady na straně poskytovatelů strategicky významné služby pro tuto novou povinnost.

Poskytovatelé strategicky významné služby jakožto povinné osoby podle návrhu zákona podléhají ze zákona také kontrole Úřadu. S ohledem na zachování principu efektivity a principu minimalizace nákladů bude kontrolní činnost související s mechanismem prověřování zařazena mezi standardní kontrolní činnost, kterou Úřad (Odbor kontroly) provádí a jejíž systém i metodika je nastavená a fungující.

Kromě nahlášení přímých dodavatelů bezpečnostně významných dodávek budou mít poskytovatelé strategicky významné služby povinnost také vynaložit přiměřené úsilí na to, aby se dozvěděli o dalších (nepřímých) dodavatelích poskytujících bezpečnostně významnou dodávku. V neposlední řadě budou mít povinnost dodržovat omezení vydaná Úřadem.

Jelikož vláda ČR rozhodla v průběhu schvalování návrhu zákona o tom, že jednoznačně preferuje podvariantu Vb, byla tato varianta vybrána. Platí tedy, že případě kratších odpisových lhůt bude vláda ČR rozhodovat o tom, jakým způsobem bude Úřad ve věci vydávání OOP postupovat. Obecně tak lze říci, že je vláda zapojena do procesu vydání opatření obecné povahy v případě, že by zjištěné riziko bylo tak velké, že by odůvodňovalo postup pro rychlejší vyřazení dodavatele, což by sebou podle očekávání přineslo také větší dopady na poskytovatele strategicky významných služeb i na poskytování strategicky významných služeb jako takových. V takovém případě lze předpokládat zvýšené riziko případné arbitráže, a tudíž se zapojení vlády do celého procesu jeví jako vhodnější a varianta. V případě standardních odpisových, ale i zmiňovaných zkrácených odpisových lhůt bude návrh OOP projednáván i s dalšími zapojenými orgány a sektorovými regulátory. Všichni uvedení tak v případě varianty Vb představují garanci zachování proporcionality celého procesu a jeho výsledku.

Dodavatelé, kteří budou omezeni či vyloučeni z poskytování dodávek do kritické části strategicky významné infrastruktury, budou pravidelně přezkoumáváni. Dojde-li k rozdílnému vyhodnocení rizikovosti u daného dodavatele, které bude mít vliv na ohrožení bezpečnosti ČR nebo vnitřního pořádku, Úřad neprodleně provede změnu, příp. zruší omezení vztahujících se k danému dodavateli. Tímto mechanismem je zaručeno, že omezeni budou skutečně pouze ti dodavatelé, kteří mohou ohrozit bezpečnosti ČR nebo vnitřního pořádku.

Podle výsledků dotazníkového šetření 74 % respondentů určuje ekonomickou životnost aktiv. Ekonomická životnost aktiv je nejčastěji (v 49 % případů) určována podle stanovené délky podpory (výrobce) daného aktiva. Dalšími faktory pro stanovení ekonomické životnosti

aktiva je v 24 % případů stanovována s přihlédnutím k technické životnosti aktiva či ekonomickou výhodnost užívání aktiva. 39 % respondentů aktiva po uplynutí doby poskytované podpory (výrobcem) dále v provozované či spravované infrastruktuře nevyužívá. Respondenti, kteří taková aktiva využívají, poté činí různorodé kroky k mitigaci rizik v podobě zneužití zranitelností, které se u takto nepodporovaných aktiv mohou objevit, a to zejména implementací vhodných technických a organizačních opatření (např. provedením segmentace sítě, omezení přístupu k nepodporovanému aktivu, zvýšený monitoring či úplná izolace takového aktiva či zajištění redundance). Úřad se dotazoval i na délku ekonomické životnosti vysokých a kritických technických aktiv tvořící informační nebo komunikační systém regulovaný zákonem o kybernetické bezpečnosti. Taková aktiva mají nejdelší ekonomickou životnost v sektoru energetiky (jedná se o průměrnou nejnižší životnost 7 let, průměrnou životnost 10 až 11 let a nejdelší životnost až 20 let, přičemž jeden z respondentů uvedl životnost aktiva až 50 let). Respondenti z ostatních sektorů v průměru uváděli délky ekonomické životnosti od minima 3 let, přes průměr 6 až 7 let, po maximální délku životnosti 10 let, přičemž pouze 3 respondenti uvedli maximální délku ekonomické životnost delší než 10 let (jednalo se o 12, 14 a 20 let).

V případě zákazu dodavatele bude stanovena přechodná lhůta, do jejíhož uplynutí musejí poskytovatelé strategicky významné služby tento zákaz reflektovat. Tato lhůta bude reflektovat životní cyklus dodávaných technologií a bude v řádech několika let. Tato lhůta ovšem nemůže být fixní, ale musí být stanovována individuálně při vydávání OOP, a to z důvodu vysoké variability délky ekonomické životnosti aktiv, jejichž dodavatelé budou regulováni a na něž se zákaz využívání jejich plnění může.

Tento postup minimalizuje dopady omezení identifikovaných rizikových dodavatelů na poskytovatele strategicky významné služby, které plnění takového dodavatele v době identifikace rizika s ním spojeného, ve vymezené části svojí infrastruktury využívají.

Dodavatelé jsou prověřováni podle stanoveného prioritizačního mechanismu. Kromě dodavatelů nahlášených poskytovateli strategicky významné služby má Úřad, stejně tak jako ostatní státní orgány zapojené do prověřování bezpečnosti dodavatelského řetězce, možnost posoudit rizikovost i dalších subjektů, které mají potenciál poskytovat bezpečnostně významné dodávky do strategicky významné infrastruktury a mechanismus tak může působit i preventivně.

Podvarianta Vb tedy cílí na omezení strategicky rizikových dodavatelů do strategicky významné infrastruktury v ČR, přičemž dbá na principy minimalizace státního donucení a proporcionalitu zajištění národní bezpečnosti a ochrany svobody podnikání. Omezováni tak budou pouze dodavatelé bezpečnostně významných dodávek do kritické části systému strategicky významné infrastruktury. Dodavatel bude omezen či zakázán do této vymezené infrastruktury na základě vyhodnocení transparentních kritérií, které může znamenat ohrožení bezpečnosti ČR nebo vnitřního pořádku. V případě vyloučení dodavatele budou mít dotčené osoby možnost k návrhu zákazu vznést připomínky, a v odůvodněných případech mohou uplatnit žádost o výjimku. Poskytovatelé strategicky významné služby, kteří zakázaného dodavatele využívají, budou mít na vyřazení dodavatele z bezpečnostně významných dodávek přechodnou lhůtu v řádu několika let.

4.3.2. Návrh změnového zákona

Konkrétní změny dle návrhu změnového zákona spočívají v následujícím:

4.3.2.1. ZoISVS

Do §6l odst. 3 ZoISVS je doplněna povinnost pro orgány veřejné správy ve znění: *„Orgán veřejné správy je povinen před uzavřením smlouvy s poskytovatelem cloud computingu*

zařadit informační systém veřejné správy nebo jeho část, k zajištění jehož provozu má být cloud computing využíván, do bezpečnostní úrovně s ohledem na povahu dotčeného informačního systému veřejné správy podle prováděcího právního předpisu a zajistit, že budou dodržována bezpečnostní pravidla pro orgány veřejné správy využívající služeb cloud computingu stanovená prováděcím právním předpisem.“ Tímto je nahrazena obdobná povinnost nyní stanovená v § 4 odst. 5 ZKB. Rovněž se do § 12 ZoISVS přidává zmocnění pro Úřad vydat prováděcí právní předpis, který stanoví bezpečnostní úrovně informačních systémů veřejné správy a bezpečnostní pravidla pro orgány veřejné správy využívající služby poskytovatelů cloud computingu. Jedná se tedy opět o nahrazení ustanovení ZKB, konkrétně § 6 písm. e).

Problematika dvoukolejnosti stanovování bezpečnostních opatření pro zajišťování kybernetické bezpečnosti ze strany správců informačních systémů veřejné správy řeší tak, že dochází ke zrušení zmocnění pro vydávání podzákonného předpisu ze strany Ministerstva vnitra v § 5a ZoISVS. Následně pak § 5b ZoISVS stanovuje ex lege povinnost pro správce informačních systémů veřejné správy nezařazené pod návrh zákona, aby vyhlášku stanovující bezpečnostní opatření pro režim nižších povinností podle návrhu zákona dodržovali přiměřeně. Jde tak o nastavení performativní normy pro uvedenou podmnožinu správců informačních systémů veřejné správy, kterou v souvislosti se zajišťováním kybernetické bezpečnosti ZoISVS dlouhodobě předpokládal, a to bez zavedení dalších povinností, které jinak plynou poskytovatelům regulovaných služeb, tedy povinným osobám podle návrhu zákona (např. povinnost se registrovat u Úřadu či hlásit incidenty). Jedná se pouze o doplnění standardu, který byl dlouhodobě ZoISVS předpokládán, a o konkretizaci povinnosti dbát u informačních systémů veřejné správy o jejich kybernetickou bezpečnost, kterou správcům těchto systémů stanovuje ZoISVS již nyní.

Neplnění určitých povinností lze postihnout peněžitou sankcí, a subjekty jsou tak motivovány k jejich dodržování. Imperfekce norem je odstraněna.

4.3.2.2. ZoPZI

V případě ZoPZI je nutno upravit obsah § 7 písm. c). Toto ustanovení odkazuje na hlavní typy povinných osob podle ZKB, tedy na ty povinné osoby, kterým je uložena základní povinnost zavádět v plném rozsahu bezpečnostní opatření podle § 4 ZKB. Tato povinnost je dána právě správcům informačního systému kritické informační infrastruktury, správcům komunikačního systému kritické informační infrastruktury a správcům informačního systému základní služby. K této množině povinných osob, zejména k poslednímu uvedenému typu povinné osoby, je ještě přidán provozovatel základní služby. Na druhou stranu provozovatel informačního nebo komunikačního systému v rámci těchto typů povinných osob vyjmenován není. Důvodová zpráva ani komentářová literatura se k důvodům tohoto stanovení blíže nevyjadřují a stanovení přesné analogie v souladu s obsahem návrhu zákona není možné. Společným identifikovaným znakem je tedy to, že pokud cílová osoba vystupuje v dosavadní právní úpravě jako správce systému, resp. poskytovatel služby, odpovídá tomuto pohledu v rámci nové právní úpravy tzv. poskytovatel regulované služby. Z tohoto pohledu je shodná také výše zmíněná povinnost zavádět bezpečnostní opatření.

Na druhou stranu lze také identifikovat, že podle dosavadní právní úpravy nebyl okruh cílových osob stanoven na všechny povinné osoby podle ZKB, ale pouze na ty adresáty normy, kteří měli největší dopad. To vede k logické úvaze, že je potřeba při hledání analogie uvažovat o okruhu užším, než je každý poskytovatel regulované služby podle návrhu zákona. Z této úvahy vyplývají dvě podvarianty – buď všichni poskytovatelé regulované služby v režimu vyšších povinností, jako skupina poskytovatelů regulované služby, u kterých je možné identifikovat větší a významnější dopady na ČR (viz Hodnocení dopadů regulace návrhu zákona), nebo množina adresátů ještě užší, a to tzv. poskytovatelé strategicky významných služeb (opět viz Hodnocení dopadů regulace návrhu zákona). Dále byl uvažován model

postavený na podvariantě poskytovatelů regulované služby v režimu vyšších povinností tak, aby se zohlednila podstatná část rizik souvisejících se zahraničními investicemi směřujícími do zmíněného typu cílových osob.

4.3.2.3. ZEK

V rámci svého čl. 43 ruší směrnice NIS 2 k datu nabytí své účinnosti čl. 40 a 41 směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (dále jen „Kodex“). Transpozičním ustanovením čl. 40 a 41 Kodexu je v českém právním prostředí § 98 zákona o elektronických komunikacích. V případě varianty II, tedy potřeby reflektovat identifikované nedostatky změnou relevantních právních předpisů, je v případě ZEK nutno upravit obsah § 98.

Posledně zmíněné ustanovení doznalo v minulosti změn a vztahuje se na *„osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací [...]“*, tedy na širší množinu, než na kterou dopadá návrh zákona. Z výše uvedených důvodů a z důvodu minimalizace zásahu do jiných právních předpisů se doplňuje aktuální znění ZEK o nový odstavec upravující vztah povinných osob podle ZEK a návrhu zákona.

4.3.2.4. Zákon o poštovních službách

Pro posílení bezpečnosti poštovní sítě, základních služeb a přístupu k poštovní infrastruktuře tak, že se nad rámec souvisejících stávajících povinností (zejména podle stávajícího odstavce 2, 3 a 8 předmětného ustanovení) doplňuje povinnost hlásit bezpečnostní incidenty, resp. ohrožení nebo narušení bezpečnosti sítě, základních služeb nebo poskytování základních služeb nebo přístupu k poštovní infrastruktuře. S ohledem na skutečnost, že poskytovatelé poštovních služeb mají nově podle směrnice NIS 2 podléhat této směrnici, respektive regulaci oblasti kybernetické bezpečnosti v ní obsažené, je rovněž potřeba jednoznačně nastavit rozdělení kompetencí mezi ČTÚ a Úřadem. Takové jednoznačné rozdělení kompetencí je důležité i z důvodu požadavku na nezvyšování administrativní zátěže jak na straně povinného, tak na straně ČTÚ, resp. Úřad, neboť by nemělo docházet k duplicitnímu plnění povinnosti hlásit bezpečnostní incidenty vůči oběma těmto orgánům, a naopak by tyto měly být oznamovány pouze jednou. Z těchto důvodů došlo k úpravě § 33, § 37a a § 41 a k přidáním nového ustanovení do § 36b zákona o poštovních službách.

4.3.2.5. Zvláštní zákony upravující povinnost mlčenlivosti a povinnost dodržet bankovní tajemství

Návrh zákona stanovuje povinnost poskytovat informace nebo nezbytnou součinnost při zjišťování nezbytných informací Úřadu v rámci mechanismu prověřování rizik spojených s dodavatelem také ve zvláštních zákonech, které mj. upravují povinnost mlčenlivosti, resp. zachování bankovního tajemství.

4.3.3. Prováděcí právní předpisy

Realizace zvolené varianty a podvarianty je nutně spojená s formulací a vydáním prováděcích právních předpisů, které budou (stejně jako právní předpisy provádějící v současné době účinný zákon o kybernetické bezpečnosti) obsahově navazovat na návrh zákona o kybernetické bezpečnosti a podrobněji specifikovat v něm obsaženou právní regulaci. Těmito prováděcími právními předpisy má být vyhláška o regulovaných službách, vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, vyhláška o Portálu Úřadu a požadavcích na vybrané úkony, vyhláška o nepominutelných funkcích stanoveného rozsahu, vyhláška o bezpečnostních úrovních informačních systémů veřejné správy a vyhláška o bezpečnostních pravidlech informačních systémů veřejné správy.

Návrh vyhlášky o regulovaných službách navazuje na návrh zákona v tom smyslu, že stanoví seznam služeb podle § 4 odst. 1 písm. a) a vymezení podmínek významnosti poskytovatele podle § 4 odst. 1 písm. b) (v souladu se zmocněním v § 4 odst. 2 návrhu zákona), rozděluje poskytovatele regulovaných služeb do vyššího a nižšího režimu povinností (v souladu se zmocněním v § 8 odst. 2 návrhu zákona) a stanoví konkrétní regulované služby v odvětvích veřejná správa, energetika, doprava a digitální infrastruktura a služby, které splňují podmínky strategicky významné služby (v souladu se zmocněním v § 25 odst. 1 návrhu zákona). Návrh vyhlášky o regulovaných službách je tedy namístě považovat za návrh prováděcího předpisu, který je klíčový pro určení, na které konkrétní subjekty navrhovaná právní úprava kybernetické bezpečnosti (tedy návrh zákona ve spojení s návrhu prováděcích právních předpisů a návrh souvisejícího změnového zákona) dopadne. Obsahově vychází návrh vyhlášky z vyhlášeného znění směrnice NIS 2, kterým je Česká republika při implementaci směrnice vázána, a to i co do jednotlivých regulovaných odvětví činnosti. Návrh vyhlášky vyhlášené znění směrnice NIS 2 překračuje pouze tam, kde je to opodstatněno výslovným odkazem směrnice na vnitrostátní právo či významem konkrétní činnosti pro bezpečnost v ČR.

U návrhu vyhlášky není předpokládán dopad na státní rozpočet, ten je spojen s návrhem zákona, k jehož provedení má být vyhláška o regulovaných službách vydána. S ohledem na obsah transponované směrnice NIS 2 a stanovení nových povinných osob a jejich povinností lze předpokládat zvýšené dopady na podnikatelské prostředí ČR a soukromý sektor celkově. Tyto dopady jsou opět primárně spojeny s návrhem zákona, k jehož provedení má být vyhláška vydána, návrh vyhlášky ovšem konkretizuje podmínky pro registraci regulovaných služeb a režim jejich poskytovatelů, tedy i vyhláška samotná má mít přeneseně na podnikatelské prostředí vliv. Zvýšení zabezpečení u organizací splňujících podmínky pro registraci podle návrhu zákona a návrhu vyhlášky bude mít finanční dopady vyčíslené v této závěrečné zprávě ve vztahu k návrhu zákona, každopádně však přispěje k budování důvěry spotřebitelů a obchodních partnerů, případně i zahraničních investorů, které může přilákat právě vysoká míra bezpečnosti českého ICT prostředí.

Návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností navazuje jak na návrh zákona (v souladu se zmocněním v § 13 odst. 3 návrhu zákona), tak také na návrh vyhlášky o regulovaných službách, která mj. rozděluje poskytovatele regulovaných služeb do vyššího a nižšího povinnostního režimu. Cílem návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností je v zásadě konkretizace bezpečnostních, tedy organizačních a technických, opatření poskytovatele regulované služby v režimu vyšších povinností, která jsou prostým výčtem uvedena v § 14 odst. 1 návrhu zákona. Návrh vyhlášky vedle toho specifikuje nezbytný rozsah dostupnosti tzv. strategicky významné služby ve smyslu § 25 návrhu zákona, který je zakotven v § 33 návrhu zákona, a stanoví přechodná ustanovení pro poskytovatele regulované služby, kteří budou ke dni předcházejícímu nabytí účinnosti vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností orgánem nebo osobou podle § 3 ZKB, kterým se ukládají povinnosti v oblasti zavádění a provádění bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti, ve znění účinném přede dnem nabytí účinnosti vyhlášky, a kteří budou ke dni nabytí účinnosti vyhlášky splňovat podmínky pro registraci alespoň jedné regulované služby.

Předpokládaný hospodářský a finanční dopad návrhu vyhlášky na veřejné rozpočty a podnikatelské prostředí ČR lze vymezit obdobně jako v případě návrhu vyhlášky o regulovaných službách. Návrh vyhlášky nemá mít dopad na státní rozpočet ani ostatní veřejné rozpočty, dopady vyvolává návrh zákona, k jehož provedení je vydávána. Při zohlednění obsahu směrnice NIS 2 a stanovení nových povinných osob a jejich povinností podle návrhu zákona lze předpokládat zvýšené dopady na podnikatelské prostředí ČR, stejně jako na soukromý sektor celkově. Tyto dopady má primárně návrh zákona, k jehož provedení má být

navrhovaná vyhláška vydávána, nicméně návrh vyhlášky zejména konkretizuje bezpečnostní opatření poskytovatele regulované služby v režimu vyšších povinností, proto i navrhovaná vyhláška má mít přeneseně na podnikatelské prostředí vliv. Je namístě zopakovat, že zvýšení zabezpečení u organizací splňujících podmínky pro registraci podle návrhu zákona, k němuž je návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, bude mít finanční dopady vyčíslené v této závěrečné zprávě ve vztahu k návrhu zákona, jistě však přispěje k budování důvěry spotřebitelů a obchodních partnerů, případně i zahraničních investorů, které může přilákat právě vysoká míra bezpečnosti českého ICT prostředí.

Podobně jako pro návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností také pro návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností platí, že navazuje na návrh zákona (v souladu se zmocněním v § 13 odst. 3 návrhu zákona), stejně jako na návrh vyhlášky o regulovaných službách, která mj. rozděluje poskytovatele regulovaných služeb do vyššího a nižšího povinnostního režimu. Dále podobně jako návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností konkretizuje zásadní bezpečnostní opatření organizačního a technického charakteru poskytovatele regulované služby v režimu nižších povinností, která jsou uvedena v § 14 odst. 2 návrhu zákona. Návrh vyhlášky rovněž stanoví přechodná ustanovení pro poskytovatele regulované služby, kteří budou ke dni předcházejícímu nabytí účinnosti o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností vyhlášky orgánem nebo osobou podle § 3 ZKB, kterým se ukládají povinnosti v oblasti zavádění a provádění bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti, ve znění účinném přede dnem nabytí účinnosti návrhu vyhlášky, a kteří budou ke dni nabytí účinnosti vyhlášky splňovat podmínky pro registraci alespoň jedné regulované služby.

K předpokládanému hospodářskému a finančnímu dopadu návrhu vyhlášky na veřejné rozpočty a podnikatelské prostředí ČR je namístě odkázat na vyčíslení tohoto dopadu u návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Návrh vyhlášky o Portálu Úřadu a požadavcích na vybrané úkony vychází ze zmocnění v § 16 odst. 5 návrhu zákona. Jak je zřejmé z formulace posledně zmíněného ustanovení návrhu zákona, návrh vyhlášky stanoví obsahové náležitosti, formát a způsob hlášení kybernetického bezpečnostního incidentu, průběžné zprávy o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu, průběžné zprávy o aktuálním stavu zvládání kybernetického bezpečnostního incidentu a závěrečné zprávy o vyřešení kybernetického bezpečnosti. Taková právní úprava odpovídá požadavkům stanoveným v nálezu Ústavního soudu ze dne 12. listopadu 2019 sp. zn. Pl. ÚS 19/17, podle kterého orgán veřejné moci nemá pravomoc libovolně aktualizovat a upravovat obsah formulářů, které požaduje k provádění určitých úkonů a podání. Návrh vyhlášky dále v souladu se zmocněním v § 45 odst. 3 návrhu zákona stanoví technické a organizační podmínky používání Portálu Úřadu, sloužícího k provádění činností podle § 45 odst. 1 návrhu zákona a obsahové náležitosti, formát, strukturu a způsob provedení úkonů podle § 45 odst. 2 návrhu zákona.

Co se týče předpokládaných dopadů návrhu vyhlášky o Portálu Úřadu a požadavcích na vybrané úkony na veřejné rozpočty a podnikatelské prostřední ČR, dopady na státní rozpočet vyplývají především ze samotného návrhu zákona, který legislativně zakotvuje vznik a fungování Portálu. Návrh vyhlášky pouze stanovuje některá související pravidla a náležitosti, sám o sobě nemá žádné dopady na státní rozpočet nebo ostatní veřejní rozpočty. S pořízením a provozem Portálu budou spojeny vstupní a následně provozní výdaje, ovšem

ze střednědobého i dlouhodobého hlediska jde o výdaje zcela nezbytné a účelně vynaložené. V případě absence obdobného řešení by velmi pravděpodobně došlo k extrémnímu administrativnímu zatížení, které by si vyžádalo zásadní zvýšení personálních kapacit. Provoz Portálu má realizován převážně z interních personálních zdrojů Úřadu. Pro samotný Úřad i všechny další regulované subjekty bude zřízení Portálu představovat zefektivnění a snížení administrativního zatížení při řešení zákonem předvídaných úkonů nebo využívání nabízených služeb.

Návrh vyhlášky o nepominutelných funkcích stanoveného rozsahu navazuje na návrh zákona v tom smyslu, že v souladu se zmocněním v § 27 odst. 4 návrhu zákona stanoví seznam nepominutelných funkcí strategicky významných služeb, které jsou v § 27 odst. 3 návrhu zákona obecně vymezeny jako činnosti nebo vlastnosti aktiva zajišťující provoz strategicky významné služby, jejichž narušení by mohlo mít závažný dopad na poskytování strategicky významné služby. Takto nahlíženo je konkrétní seznam nepominutelných funkcí strategicky významných služeb klíčový pro řádné fungování mechanismu prověřování bezpečnosti dodavatelského řetězce, neboť pokrývá minimální nutný rozsah aktiv stanoveného rozsahu strategicky významné služby.

Pokud jde o případné dopady návrhu vyhlášky na veřejné rozpočty a podnikatelské prostředí ČR, tyto jsou stejně jako u návrhů ostatních prováděcích předpisů spojeny především se samotným návrhem zákona. Lze připustit, že přímo v souvislosti s navrhovanou vyhláškou dojde k rozšíření kritické části stanoveného rozsahu povinných osob mechanismu v sektoru elektronických komunikací, z čehož plyne možné rozšíření počtu dodavatelů, kteří budou moci mechanismu posuzování dodavatelů podléhat a kteří budou moci být omezeni. V případě vydání varování podle zákona o kybernetické bezpečnosti se bude jednat o povinnost povinné osoby mechanismu reflektovat identifikovanou hrozbu v analýze rizik, což je proces, který je v současnosti u povinných osob mechanismu již nastavený a fungující. Vymezením nepominutelných funkcí by mělo dojít k zefektivnění určování a udržování kritických částí systémů regulovaných subjektů. Dále dojde k aplikaci povinností plynoucích z mechanismu posuzování dodavatelů napříč povinnými osobami mechanismu obdobným způsobem, a to zejména tím, že funkce, jejichž významnost je nezpochybnitelná, tedy takové funkce, které jsou zajištěny aktivy, která by měla být vždy ohodnocena jako vysoká či kritická, protože na nich bude poskytování regulované služby vždy vysoce závislé, budou pevně stanoveny. Dojde tak k nutnému zamezení negativních dopadů možného rozdílného přístupu i kvality provedení identifikace vysokých a kritických aktiv jednotlivými poskytovateli regulovaných služeb v režimu vyšších povinností, na něž dopadá mechanismus posuzování dodavatelů.

Návrh vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy je založen na zmocnění obsaženém v § 12 odst. 2 písm. g) ZoISVS ve znění návrhu změnového zákona. Podle navrhovaného znění § 6l odst. 3 zákona o informačních systémech veřejné správy využívá orgán veřejné správy cloud computing poskytovaný na základě písemné smlouvy o poskytování cloud computingu orgánu veřejné správy, přičemž před uzavřením smlouvy s poskytovatelem cloud computingu je povinen zařadit informační systém veřejné správy nebo jeho část, k zajištění jehož provozu má být cloud computing využíván, do bezpečnostní úrovně s ohledem na povahu dotčeného informačního systému veřejné správy podle prováděcího právního předpisu a dále je orgán veřejné správy povinen zajišťovat, že budou dodržována bezpečnostní pravidla stanovená prováděcím právním předpisem. Návrh vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy do značné míry přejímá obsah z účinné vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, neboť vlastní potřeba vydat vyhlášku o bezpečnostních úrovních informačních systémů veřejné správy vychází ze skutečnosti, že dochází k přesunu zmocnění obsaženého v § 28 odst. 2 písm. a) ZKB do ZoISVS ve znění návrhu změnového zákona, jmenovitě do výše uvedeného § 12 odst. 2 písm. g).

Návrh vyhlášky sám o sobě nebude mít vliv na státní nebo ostatní veřejné rozpočty. Ze zařazení poptávaného cloud computingu do bezpečnostní úrovně nevznikají pro orgán veřejné správy bez dalšího žádné dodatečné výdaje. V případě, že by se orgán veřejné správy rozhodl přesunout určitý systém či jeho část do cloudového řešení, lze předpokládat určitý dopad na veřejné rozpočty, takový dopad nicméně bezprostředně nesouvisí se stanovením bezpečnostní úrovně daného systému nebo jeho části, nýbrž s procesem přechodu na cloudové řešení. U méně významných systémů může být přesun do cloudu finančně výhodnější z dlouhodobého hlediska s minimálními vstupními výdaji. U důležitějších informačních systémů orgánu veřejné správy si přesun do cloudu může vyžádat významnější počáteční investice i náklady na následný provoz a údržbu, ty by přímo ovšem nesouvisely s návrhem vyhlášky, ale s rozhodnutím subjektu o využití služeb cloud computingu. Proces samotného posouzení poptávaného cloud computingu, respektive jeho zařazení do relevantní bezpečnostní úrovně podle tohoto návrhu vyhlášky, s sebou nese zcela marginální provozní výdaje. Návrh vyhlášky současně nemá dopad na podnikatelské prostředí.

Podobně jako návrh vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy také návrh vyhlášky o bezpečnostních pravidlech informačních systémů veřejné správy vychází ze zmocnění obsaženém v ZoISVS ve znění návrhu změnového zákona. V případě návrhu vyhlášky o bezpečnostních pravidlech informačních systémů veřejné správy má být v novelizované verzi ZoISVS dotčené zmocnění obsaženo v § 12 odst. 2 písm. h). Také návrh vyhlášky o bezpečnostních pravidlech informačních systémů veřejné správy obsahově navazuje na již vydanou vyhlášku (č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu) a její vydání má reflektovat skutečnost, že dochází k přesunu zmocnění obsaženého v § 28 odst. 2 písm. a) ZKB, do ZoISVS ve znění změnového zákona, konkrétně do výše uvedeného § 12 odst. 2 písm. h), který byl zmíněn výše.

U návrhu vyhlášky nejsou předpokládány žádné hospodářské a finanční dopady na státní rozpočet, ostatní veřejné rozpočty či podnikatelské prostředí ČR.

5. Implementace doporučené varianty a vynucování

S ohledem na požadavky stanovené především potřebou transpozice směrnice, ale i mechanismem prověřování bezpečnosti dodavatelského řetězce, a s obojím spojené nutné zásadní úpravy, dosahuje zvolená varianta V takové míry zásahu do znění zákona o kybernetické bezpečnosti, že se jako nejvhodnější jeví forma nového zákona o kybernetické bezpečnosti s novými prováděcími právními předpisy. S ohledem na smysl a účel regulace je nutno zachovat veřejnoprávní regulaci kybernetické bezpečnosti v rámci jednoho speciálního právního předpisu.

V rámci návrhu zákona je nutné zachovat východiska a zásady, stejně tak jako základní instituty systému zajištění kybernetické bezpečnosti podle zákona o kybernetické bezpečnosti. Struktura povinností se v navrhované právní úpravě i nadále vztahuje k osobám soukromého práva i orgánům veřejné moci.

Návrh zákona pak musí zavést nový pojmový aparát a novým způsobem upravit povinnosti pro nově definovanou kategorii povinných osob, resp. přizpůsobit tyto povinnosti režimům povinných osob. Vybraná ustanovení zákona o kybernetické bezpečnosti je třeba modifikovat, aby byla zajištěna jejich aplikovatelnost i v rámci budoucí úpravy (např. protiopatření, stav kybernetického nebezpečí, sankce apod.). Proces prověřování rizikovosti dodavatelů do strategicky významné infrastruktury bude Úřad řídit ve spolupráci se spolupracujícími státními orgány, jakož i omezovat či vylučovat tyto rizikové dodavatele v rámci svých nově nabytých zákonných povinností.

Je také nutno zachovat a rozšířit dosavadní pravomoci a kompetence Úřadu a stanovit nová pravidla pro spolupráci mezi orgány veřejné moci v oblasti kybernetické bezpečnosti.

Návrh zákona pracuje s roční přechodnou lhůtou pro zahájení plnění některých povinností stanovených poskytovatelům regulovaných služeb. Kontrola a vynucování jejich plnění tedy ve vztahu ke každému poskytovateli regulované služby započne až po uplynutí této lhůty. Pro vymáhání plnění uložených povinností návrh zákona poskytuje množství nápravných a sankčních mechanismů, kromě pokut i speciální sankce donucovacího charakteru.

Orgány a osoby do nabytí účinnosti návrhu zákona sice nejsou povinny činit významné kroky pro uvedení stavu jejich organizace do souladu s budoucími požadavky návrhu zákona, nicméně minimálně v případě orgánů a osob spadajících podle návrhu zákona do režimu vyšších povinností, které dosud do působnosti zákona o kybernetické bezpečnosti nespadaly, je zahájení určitých přípravných prací (minimálně v rozsahu analýzy současného stavu kybernetické bezpečnosti v organizaci) doporučeno.

Úřad je jediným orgánem odpovědným za implementaci nově přijaté regulace a orgánem příslušným k dozoru nad dodržováním pravidel stanovených v návrhu zákona. Za tím účelem je třeba zabezpečit Úřadu odpovídající prostředky a předpoklady.

Náklady na implementaci doporučené varianty jsou uvedeny v příslušné kapitole.

6. Přezkum účinnosti

V návaznosti na principy přezkumu účinnosti uvedené v rámci zákona o kybernetické bezpečnosti lze konstatovat, že k tomu, aby mohla navrhovaná právní úprava plnit svůj základní účel, je potřeba průběžně sledovat, do jaké míry odpovídají zákonné povinnosti aktuálním potřebám informační společnosti – vzhledem k tomu, že návrh zákona se týká zabezpečení skutečného fungování regulovaných služeb, nelze připustit situaci, kdy budou zákonné povinnosti formálně definovány a formálně plněny, to však bez skutečného praktického efektu.

Přezkum účinnosti regulace lze u navrhované právní úpravy rozdělit do tří základních fází:

1. Sledování technického vývoje a okamžitý přezkum implementace bezpečnostních opatření a protiopatření

Stejně jako doposud bude Úřad prostřednictvím činností vládního CERT, spolupráce s národním CERT a mezinárodní spolupráce permanentně sledovat a vyhodnocovat situaci v oblasti kybernetické bezpečnosti a reagovat na zjištěné nedostatky a bezpečnostní hrozby. Dojde-li k situaci vyžadující okamžité přehodnocení kvality bezpečnostních opatření, bude k jejímu řešení užito buďto protiopatření, nebo následné změny prováděcích právních předpisů.

2. Hodnocení efektivity právní úpravy a přezkum struktury jednotlivých konkrétních parametrů zákonných povinností

Úřad bude pravidelně vyhodnocovat strukturu parametrů bezpečnostních opatření, a to zejména v návaznosti na vývoj průmyslových standardů a akceptovaných doporučených postupů (best practices), a v souvislosti s úpravou uvedenou ve směrnici NIS 2 také na příslušné prováděcí akty směrnice. V případě identifikace potřeby upravit parametry bezpečnostních opatření bude jako nástroje použito změny prováděcího právního předpisu.

3. Hodnocení efektivity zákonných povinností

Úřad bude jako doposud provádět ve spolupráci s dotčenými resorty, akademickými pracovišti a soukromým sektorem pravidelné hodnocení efektivity právní úpravy jako takové. Ukáže-li se, že některé zákonné povinnosti neplní dostatečně účel navrhované právní úpravy, bude iniciována příslušná změna právní úpravy.

Konkrétní ukazatele, které budou shromažďovány pro vyhodnocení naplňování cílů návrhu zákona, se budou lišit v závislosti na konkrétních požadavcích a oblastech, které návrh zákona pokrývá. Mezi relevantní ukazatele budou patřit například:

- Počet a druh kybernetických bezpečnostních incidentů, které byly detekovány a nahlášeny Úřadu.
- Úroveň kybernetické bezpečnosti informačních systémů hodnocená na základě výsledku kontrol zavádění a provádění bezpečnostních opatření a protiopatření Úřadu.
- Procento orgánů a osob, které jsou v souladu se zákonnými požadavky.
- Úroveň osvěty a povědomí veřejnosti a dotčených osob v regulovaných organizacích v oblasti kybernetické bezpečnosti.
- Sledování indukovaných nákladů na povinné subjekty, což zahrnuje přímé náklady spojené s implementací bezpečnostních opatření, náklady na školení a osvětu, náklady na monitorování a audity, a další administrativní náklady.

Podrobnější popis sledovaných ukazatelů:

- **Počet a druh kybernetických bezpečnostních incidentů**: Sleduje se celkový počet incidentů, jejich závažnost, zdroj (interní/externí), typ útoku (phishing, malware, DDoS, apod.) a rychlost reakce na tyto incidenty.
- **Úroveň kybernetické bezpečnosti informačních systémů**: Hodnocení zahrnuje audit bezpečnostních opatření, jako jsou firewall ochrana, antivirové systémy, šifrování dat, systémová aktualizace a patch management.
- **Procento orgánů a osob v souladu se zákonnými požadavky**: Měří se úroveň shody s předpisy prostřednictvím pravidelných kontrol a inspekcí. Hodnotí se počet organizací, které úspěšně prošly bezpečnostními audity.
- **Úroveň osvěty a povědomí**: Měří se počet a kvalita školení, seminářů a informačních kampaní provedených pro zvyšování povědomí o kybernetické bezpečnosti mezi zaměstnanci a veřejností. Hodnotí se také úroveň znalostí zaměstnanců před a po školeních.
- **Indukované náklady na povinné subjekty**: Sledují se náklady na implementaci bezpečnostních opatření (např. nákup hardwaru a softwaru), náklady na školení zaměstnanců, náklady na pravidelné audity a monitorování bezpečnosti, a další provozní a administrativní náklady spojené s dodržováním zákonných povinností.

Přezkum účinnosti regulace bude probíhat i v návaznosti na činnost Evropské Komise za účelem vyhodnocení plnění cílů stanovených směrnicí NIS 2.

Co se týče mechanismu prověřování bezpečnosti dodavatelského řetězce, vyhodnocení a přezkum účinnosti právní úpravy budou prováděny průběžně ve spolupráci s ostatními orgány veřejné moci a na základě přijatých dotazů veřejnosti a orgánů veřejné moci. Hodnotit se bude, zdali zavedením mechanismu prověřování bezpečnosti dodavatelského řetězce došlo ke snížení hrozeb, a zdali má mechanismus vliv na výskyt dodavatelů, s nimiž se pojí možné významné ohrožení bezpečnosti ČR nebo vnitřního pořádku v důsledku vyhodnocení kritérií rizikovosti dodavatele.

7. Konzultace a zdroje dat

Při přípravě návrhu právního předpisu byly s žádostí o konzultace a vyjádření osloveny tyto subjekty:

Ministerstvo financí, Ministerstvo práce a sociálních věcí, Ministerstvo průmyslu a obchodu, Ministerstvo zemědělství, Ministerstvo vnitra, Ministerstvo dopravy, Ministerstvo životního prostředí, Ministerstvo zdravotnictví, Ministerstvo školství, mládeže a tělovýchovy, Energetický regulační úřad, Český statistický úřad, Český telekomunikační úřad, Úřad

pro ochranu osobních údajů, Česká správa sociálního zabezpečení, Úřad pro civilní letectví, Státní ústav pro kontrolu léčiv, Ústav zdravotnických informací a statistiky ČR, CENIA, Česká informační agentura životního prostředí, Státní veterinární správa, Státní zemědělská a potravinářská inspekce, Námořní úřad, Státní plavební správa, Česká asociace petrolejářského průmyslu a obchodu, Česká vodíková technologická platforma, Hospodářská komora ČR, Svaz průmyslu a dopravy ČR, Brno Space Cluster a sdružení právnických osob CZ.NIC.

Výše uvedeným gestorům byly zaslány informace o pro ně relevantních službách uvedených v přílohách I a II směrnice a s nimi dotazy směřující na správné použití pojmů odpovídajících české právní úpravě. Osloveným gestorům byla dána možnost vyjádřit se k budoucí regulaci, případně navrhnout nové regulované služby nad rámec požadavků směrnice. Některé z výše uvedených organizací této možnosti využily.

Vedle uvedených gestorů oslovil Úřad s nabídkou konzultací také zájmové svazy, komory a další sdružení. Tato nabídka byla zaslána následujícím subjektům:

Asociace krajů, Asociace kritické infrastruktury, Asociace poskytovatelů mobilních sítí, Asociace českých a moravských nemocnic, ČAPPO, Česká asociace odpadového hospodářství, Česká bankovní asociace, Česká konference rektorů, Česká vodíková technologická platforma, Český plynárenský svaz, ČSRES, Hospodářská komora ČR, hSOC, ICT unie, konsorcium CRP-KYBER, Potravinářská komora ČR, SOVAK, Svaz vodního hospodářství ČR, Svaz chemického průmyslu, Svaz dopravy, Svaz měst a obcí, Svaz průmyslu a dopravy, Svaz českých a moravských výrobních družstev, Teplárenské sdružení, Výbor nezávislého ICT průmyslu a Zemědělský svaz ČR.

Organizacím, které na nabídku reagovaly, byl představen základ budoucí regulace podle aktuálního stavu, a také jim byla dána možnost se k problematice vyjádřit.

Informace shromážděné v průběhu konzultací a vyjádření oslovených subjektů byly podkladem pro formulaci návrhu zákona a jeho prováděcích předpisů. Zejména byly využity informace o zkušenostech s praktickou aplikací institutů obsažených v zákoně o kybernetické bezpečnosti, návrhy na zjednodušení a zefektivnění aktuálního stavu, informace o subjektech působících v jednotlivých regulovaných odvětvích a o právních předpisech, které tato odvětví regulují, a z nichž bylo možné vycházet při formulaci kritérií pro identifikaci a určení poskytovatelů regulovaných služeb.

Co se týče mechanismu prověřování bezpečnosti dodavatelského řetězce, v rámci příprav návrhu zákona byly s žádostí o konzultace, vyjádření a následnou spolupráci s podílením se na procesu prověřování bezpečnosti dodavatelského řetězce osloveny tyto státní orgány:

Finanční analytický úřad, Ministerstvo průmyslu a obchodu, Ministerstvo vnitra, Ministerstvo zahraničních věcí, Nejvyšší státní zastupitelství, Policie ČR, Úřad pro ochranu hospodářské soutěže a zpravodajské služby ČR.

S vybranými organizačním složkami státu byl konzultován mechanismus prověřování bezpečnosti dodavatelského řetězce v několika fázích přípravy, přičemž došlo na vzájemné sdílení informací a připomínek jak k dílčím částem mechanismu – tzn. k právní, strategické i technické stránce – tak k jeho funkčnímu celku. Vybrané státní orgány dále poskytly cenné podklady v podobě informací z hlediska pracovních kapacit a celkových nákladů souvisejících s fungováním a podílením se na mechanismu prověřování bezpečnosti dodavatelského řetězce, a to formou vyplňování relevantních dotazníků Úřadu.

Problematika právních, strategických, politických a dalších aspektů mechanismu prověřování bezpečnosti dodavatelského řetězce, včetně návrhů možných řešení, byla také v rámci otevřených diskuzí konzultována s akademickou obcí (například Masarykova

univerzita), zájmovými svazy, komorami a soukromým sektorem (například výše uvedené sdružení právnických osob CZ.NIC). Pro potřeby dopadů regulace a mechanismu jako takového na regulované subjekty Úřad dále oslovil zástupce širokého spektra subjektů[75] s žádostí o poskytnutí informací do dotazníků k dopadům připravované regulace. Pro potřeby identifikace těchto dopadů se vyjádřili zástupci odvětví, jako jsou odvětví energetické, odvětví dopravní, bankovnictví včetně infrastruktury finančních trhů, zdravotnictví, vodohospodářství, digitální infrastruktura, chemický průmysl, potravinářství a zemědělství, komunikační a informační systémy, nouzové služby a veřejná správa.

Problematika mechanismu prověřování bezpečnosti dodavatelského řetězce byla rovněž konzultována a diskutována na mezinárodním poli s relevantními úřady (analogie Národního úřadu pro kybernetickou a informační bezpečnost) převážně Německa, Spojeného království či Spojených států amerických, které vzhledem ke své expertíze a svým mechanismům ochrany dodavatelských řetězců poskytly významné informace a zkušenosti s nastavováním mechanismu prověřování bezpečnosti dodavatelského řetězce.

Jako relevantní zdroje použitelných dat posloužily zejména strategické dokumenty a dokumenty politik, zákonné či podzákonné předpisy a jiné koncepční dokumenty nebo zkušenosti relevantních států EU a NATO související s tamními obdobami mechanismů prověřování bezpečnosti dodavatelského řetězce, jak v rozsahu telekomunikačního sektoru, tak i napříč bezpečnostně relevantními sektory obsahujícími kritickou informační infrastrukturu. Jako další písemné podklady využitelné k tvorbě mechanismu prověřování bezpečnosti dodavatelského řetězce posloužily Soubor opatření EU pro kybernetickou bezpečnost sítí 5G (tzv. EU 5G Toolbox), Zvláštní zpráva Evropského účetního dvora č. 3/2022: Spouštění sítí 5G v EU a data Úřadu a spolupracujících organizačních složek státu.

Celková podoba budoucího právního rámce mechanismu, a spolu s tím i budoucí rozsah úpravy, byla také představena a konzultována skrz odborné semináře a konference, jakými byly:

Konference v Poslanecké sněmovně Parlamentu ČR na téma *„Bezpečnost dodavatelského řetězce v sítích elektronických komunikací a další strategické infrastruktuře České republiky“* ze dne 13. července 2022, konference *„CyberCon 2022“* ze dnů 13. – 15. září 2022, konference CEVRO institutu k bezpečnosti dodavatelského řetězce v sítích elektronických komunikací v ČR ze dne 20. září 2022, konference v Poslanecké sněmovně Parlamentu ČR k budování 5G sítí ze dne 19. října 2022, konference EU Secure and Innovative Digital Future ze dnů 3. - 4. listopadu 2022 či Seminář k bezpečnosti dodavatelského řetězce ze dne 7. prosince 2022.

Úřad rovněž opakovaně vyzýval odbornou i širokou veřejnost k zasílání podnětů týkajících se mechanismu prověřování bezpečnosti dodavatelského řetězce, ať už formou připomínek v rámci dotazníků, možnosti účastnit se a diskutovat na konferencích či odborných seminářích k mechanismu prověřování bezpečnosti dodavatelského řetězce, tak prostřednictvím plošné konzultace s širokou veřejností, na jejímž základě vzniklo mnoho podkladů pro konečné úpravy mechanismu.

Celková podoba budoucího právního rámce transpozice směrnice do českého právního řádu, a spolu s tím i budoucí rozsah úpravy, byly konzultovány také se zahraničními organizacemi. V rámci příprav návrhu zákona a prováděcích právních předpisů bylo toto téma také diskutováno s relevantními úřady (analogiemi Úřadu) Slovenska, Polska, Rakouska, Německa, Slovinska, Francie a Estonska. Jejich zkušenosti byly zohledněny při formulaci finálního znění návrhu zákona.

[75] Podle § 3 zákona o kybernetické bezpečnosti z těch odvětví, ve kterých je určený regulovaný systém podle vyhlášky č. 437/2017 Sb. a nařízení vlády č. 432/2010 Sb.

Úřad také opakovaně vyzýval odbornou i širokou veřejnost k zasílání podnětů týkajících se budoucí regulace – ať už formou obecné výzvy na svých internetových stránkách, tak zřízením speciální internetové stránky zaměřené na transpozici směrnice do českého právního řádu.

Při přípravě návrhu změnového zákona byly s žádostí o konzultace a vyjádření osloveny Ministerstvo vnitra (gestor problematiky upravené ZoISVS), Ministerstvo průmyslu a obchodu (gestor problematiky upravené ZoPZI) a ČTÚ (gestor problematiky upravené ZEK a zákonem o poštovních službách).