SMĚRNICE NIS 2

Východiska, cíle a vybrané klíčové aspekty návrhu směrnice NIS 2, včetně rozsahu povinných subjektů a hodnocení dodavatelů.

I. Úvod

Dne 16. prosince 2020 přijala Evropská komise **návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v celé Unii, kterou se ruší směrnice (EU) 2016/1148** (dále také "*návrh směrnice NIS 2*" nebo "*směrnice NIS 2")*. Cílem tohoto návrhu je rozšířit oblast působnosti 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 celé Unii (dále jen "*směrnice NIS")* a přizpůsobit ji potřebám současnosti i budoucnosti, neboť, jak odhalila pandemie koronaviru, v současnosti účinná právní úprava se z pohledu Evropské komise jeví jako nedostatečná a nekonzistentní, a to zejména s ohledem na požadavek zvýšené a stále se rozvíjející digitalizace ve všech možných oblastech (včetně těch kritických).

Směrnice NIS 2 by měla být jedním z opatření stanovených s cílem dále zlepšit odolnost a schopnost reakce na incidenty veřejných a soukromých subjektů, příslušných orgánů, jakož i Evropské unie jako celku v oblasti kybernetické bezpečnosti a ochrany kritické infrastruktury. Návrh směrnice NIS 2 přímo souvisí a zároveň má nahradit směrnici NIS z roku 2016, která byla prvním celoevropským právním předpisem v oblasti kybernetické bezpečnosti.

Směrnice o bezpečnosti sítí a informací dosáhla mnoha významných úspěchů a položila základy institucionálního a regulačního přístupu ke kybernetické bezpečnosti v mnoha zemích EU - přispěla ke zlepšení schopností v oblasti kybernetické bezpečnosti na vnitrostátní úrovni tím, že členským státům uložila povinnost přijmout vnitrostátní strategie kybernetické bezpečnosti a jmenovat orgány pro kybernetickou bezpečnost, zvýšila spolupráci mezi členskými státy na úrovni EU zřízením různých fór usnadňujících výměnu strategických a operativních informací a zlepšila kybernetickou odolnost veřejných a soukromých subjektů v sedmi konkrétních odvětvích[1] a ve třech digitálních službách[2] tím, že od členských států požadovala, aby zajistily, že provozovatelé

[1] Energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, dodávky a distribuce pitné vody a digitální infrastruktura.
[2] Online tržiště, online vyhledávače a služby cloud computingu.

základních služeb a poskytovatelé digitálních služeb zavedou požadavky na kybernetickou bezpečnost a budou hlásit incidenty.

Vzhledem k rychle se rozvíjející digitální transformaci celé společnosti a stále rostoucímu počtu (stále sofistikovanějších) kybernetických útoků přicházejících z EU i oblastí mimo EU se však současná regulace, kterou představuje směrnice o bezpečnosti sítí a informací, již nezdá být dostatečná. Evropská komise považuje za největší problémy současné regulace následující: nízkou úroveň kybernetické odolnosti podniků působících v EU, nejednotnou úroveň odolnosti napříč členskými státy a odvětvími a nízkou úroveň společného situačního povědomí a nedostatečnou společnou reakci na krize. [3]

Pokud jde o vztah k jiným předpisům Evropské unie, návrh směrnice NIS 2 se týká zejména směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví Evropský kodex elektronických komunikací (dále jen "***Evropský kodex elektronických komunikací"*** nebo "*EECC"),* který se považuje za *lex specialis* pro směrnici NIS 2 (jakmile bude přijata). Směrnice NIS 2 rovněž doplní návrh směrnice Evropského parlamentu a Rady o odolnosti kritických subjektů (dále jen "***návrh směrnice CER"),*** který je rovněž stále v legislativním procesu - v podstatě na stejné úrovni jako návrh směrnice NIS 2.[4] Směrnice NIS 2 je tedy ve skutečnosti úzce spojena s návrhem směrnice CER, jejímž cílem je posílit odolnost kritických subjektů vůči fyzickým hrozbám v mnoha odvětvích. Tento návrh má zajistit, aby příslušné orgány přijímaly doplňující se opatření podle obou právních aktů a aby si podle potřeby vyměňovaly informace jak o kybernetické, tak o nekybernetické odolnosti a aby zejména klíčové subjekty v odvětvích považovaných za zásadní podle tohoto návrhu podléhaly také obecnějším povinnostem zaměřeným na posílení odolnosti s důrazem na nekybernetická rizika[5].

Pro úplnost je třeba uvést, že ve finančním sektoru[6] bude pro směrnici NIS 2 relevantní také návrh nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014 (dále jen "***návrh DORA")***. Toto nařízení stanoví jednotné požadavky týkající se bezpečnosti sítí a informačních systémů podporujících obchodní procesy finančních subjektů, které jsou potřebné k dosažení vysoké společné úrovně digitální provozní odolnosti. Návrh DORA by měl zajistit právní

[3] Viz pracovní dokument útvarů Komise - Shrnutí zprávy o posouzení dopadů připojené k návrhu směrnice NIS 2 ze dne 16. prosince 2020, strana1 .
[4] Obecný přístup Rady k návrhu směrnice Evropského parlamentu a Rady o odolnosti kritických subjektů č. 14594/21 byl přijat 7. prosince 2021.
[5] Obecný přístup Rady navrhuje následující definici **"rizika":** "*potenciální ztráta nebo narušení způsobené událostí a vyjadřuje se jako kombinace velikosti takové ztráty nebo narušení a pravděpodobnosti výskytu uvedené události*".
[6] Má podobu nařízení, tj. bude právně závazné a bude platit v celé EU.

jasnost v tom, zda a jak se ustanovení o digitální provozní odolnosti vztahují zejména na přeshraniční finanční subjekty, a měl by odstranit potřebu členských států individuálně zdokonalovat pravidla, standardy a očekávání týkající se provozní odolnosti a kybernetické bezpečnosti jako reakci na současný omezený rozsah právní úpravy EU a poměrně obecnou povahu směrnice NIS.[7]

Níže uvedený text vychází především z návrhu směrnice NIS 2 a zohledňuje také nejnovější navrhované změny směrnice NIS 2 - především obecný přístup Rady k návrhu směrnice NIS 2 ze dne 3. prosince 2021[8] a také předběžnou kompromisní změnu Evropského parlamentu ze dne 28. října 2021.[9]

II. Současná fáze legislativního procesu směrnice NIS 2

Záměr Evropské komise revidovat stávající směrnici o bezpečnosti sítí a informací byl oznámen již 29. ledna 2020 v novém pracovním programu Evropské komise - revize směrnice o bezpečnosti sítí a informací měla proběhnout v posledním čtvrtletí roku 2020.

Dne **7. července 2020** zahájila Evropská komise veřejnou konzultaci o revizi směrnice o bezpečnosti sítí a informací, jejímž cílem bylo shromáždit názory na její provádění a na dopad případných budoucích změn. Konzultace byla ukončena **2. října 2020**.

Evropská komise a vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku představily **16. prosince 2020** novou strategii kybernetické bezpečnosti EU, jejímž cílem je posílit odolnost vůči kybernetickým hrozbám na evropské úrovni. V návaznosti na to Evropská komise přijala dva nové návrhy:

- návrh směrnice NIS 2,
- návrh směrnice CER.

[7] Viz Briefing, Průběžná legislativa EU ke směrnici NIS2 - Vysoká společná úroveň kybernetické bezpečnosti v EU z prosince 2021, strana 8.
[8] Více na: https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf
[9] Více informací naleznete na adrese: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2021/10-28/NIS2_COMPROMISE_amendment_EN.pdf.

Dne **3. února 2021** se Výbor stálých zástupců rozhodl konzultovat návrh s Evropským výborem regionů. Evropský výbor regionů dosud nezaujal žádné stanovisko.[10]

Evropský inspektor ochrany údajů přijal své stanovisko **11. března 2021**.[11]

Dne **13. dubna 2021** předložila Evropská komise svůj návrh Evropskému parlamentu, v tomto případě příslušnému Výboru pro průmysl, výzkum a energetiku (ITRE).[12] Výbory pro stanovisko jsou: Výbor pro Zahraniční věci, Vnitřní trh a ochrana spotřebitele, Doprava a cestovní ruch a Občanské svobody, spravedlnost a vnitřní věci.

Dne **26. května 2021** zpravodaj předložil návrh zprávy. Lhůta pro předložení pozměňovacích návrhů k navrhované směrnici NIS 2 byla stanovena do 2. června 2021.

Dne **14. července 2021** zveřejnily svá stanoviska výbory pro ochranu spotřebitele a pro dopravu a 15. července 2021 výbor pro zahraniční věci zveřejnil své stanovisko k návrhu zprávy výboru pro průmysl.

Výbor ITRE přijal zprávu zpravodaje dne **28. října 2021**. Zpráva vyzvala ke zpřísnění povinností v oblasti kybernetické bezpečnosti, pokud jde o řízení rizik, oznamovací povinnosti a sdílení informací, a zaměřila se na snížení administrativní zátěže a zlepšení hlášení kybernetických bezpečnostních incidentů. Kromě toho zpráva uvádí, že země EU by měly splňovat přísnější opatření v oblasti dohledu a vymáhání a harmonizovat své sankční režimy. Zpráva má rovněž v úmyslu rozšířit odvětvovou působnost tak, aby zahrnovala i akademické, znalostní a výzkumné instituce[13], které Komise ponechala mimo oblast působnosti návrhu směrnice NIS 2, zatímco řada vnitrostátních strategií kybernetické bezpečnosti se jich týká.

Dne **22. listopadu 2021 zprávu přijal Evropský parlament na svém plenárním zasedání** spolu s **rozhodnutím zahájit interinstitucionální jednání**.

V Radě Evropské unie (dále jen "*Rada*") se návrhem

[10] Viz obecný přístup Rady Evropské unie k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v celé Unii, kterou se zrušuje směrnice (EU) 2016/1148, č. j. 14337/21, strana 2.
[11] Stanovisko 5/2021 ke strategii kybernetické bezpečnosti a směrnici NIS 2.0 ze dne 11. března 2021.
[12] Zpravodaj: Bart Groothuis, Renew, Nizozemsko.
[13] Viz příloha II bod 6a kompromisního pozměňovacího návrhu Evropského parlamentu.

NIS 2 zabývala horizontální pracovní skupina pro kybernetické otázky. První kompromisní návrh předsednictví ke znění návrhu směrnice NIS 2 byl vydán dne **21. září 2021**.[14] Poslední revize tohoto kompromisního návrhu předsednictví byla projednána na úrovni pracovní skupiny dne **22. listopadu 2021**.[15]

Dne 3. prosince 2021 přijala Rada svůj vyjednávací postoj a dosáhla **obecného přístupu Rady k návrhu směrnice NIS 2** (dále jen "*obecný přístup Rady")*. Oproti původnímu návrhu směrnice NIS 2 Rada zavedla řadu významných změn. Například - další kritéria pro určení subjektů, na které se má směrnice NIS 2 vztahovat, přičemž z oblasti působnosti byly vyloučeny subjekty působící v oblasti obrany nebo národní bezpečnosti, veřejné bezpečnosti, vymáhání práva a soudnictví, jakož i parlamenty a centrální banky. Obecný přístup Rady sladil znění s dalšími souvisejícími navrhovanými právními předpisy, jako je návrh směrnice CER a návrh směrnice DORA. Rada rovněž zjednodušila povinnosti týkající se hlášení incidentů, aby se zabránilo nadměrnému hlášení, a prodloužila lhůtu, kterou mají členské státy na provedení směrnice NIS 2 do vnitrostátního práva, na dva roky namísto původně navrhovaných 18 měsíců.

Přijetí směrnice NIS 2 probíhá řádným legislativním postupem (COD). V současné době se **čeká na stanovisko Evropského parlamentu v 1. čtení návrhu směrnice NIS 2**.

Očekává se také, že v **roce 2022 budou brzy** zahájena **interinstitucionální jednání v rámci trialogu**. Trialogy jsou neformální třístranná jednání o legislativních návrzích mezi zástupci Evropského parlamentu, Rady a Evropské komise. Jejich cílem je dosáhnout předběžné dohody o znění přijatelném pro Radu i Evropský parlament. Mohou být uspořádány v kterékoli fázi legislativního postupu a mohou vést k takzvaným dohodám v prvním čtení, v předčasném druhém čtení nebo ve druhém čtení, případně ke společnému textu během dohodovacího řízení.[16]

Pro úplnost je třeba uvést, že směrnice NIS 2 vstupuje v platnost dvacátým dnem po vyhlášení v Úředním věstníku Evropské unie, přičemž **členské státy jsou povinny směrnici NIS 2 provést do 18 měsíců (resp. 24 měsíců podle obecného přístupu Rady) od jejího vstupu v platnost**.[17]

[14] Viz kompromisní návrh předsednictví k návrhu směrnice Evropského parlamentu a Rady o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v celé Unii, kterou se zrušuje směrnice (EU) 2016/1148, č. 12019/21.
[15] Viz kompromisní návrh předsednictví č. 12019/5/21 REV 5.
[16] Další podrobnosti naleznete na adrese: https://www.europarl.europa.eu/olp/en/interinstitutional-negotiations.
[17] Viz články 42 a 38 návrhu směrnice NIS 2.

III. Klíčové aspekty návrhu směrnice NIS 2

Návrh směrnice NIS 2 se snaží řešit neuspokojivou situaci v oblasti kybernetické bezpečnosti a usiluje o její nápravu, zejména v následujících klíčových aspektech:

1) Změna (rozšíření) rozsahu působnosti subjektů, na které se vztahuje směrnice NIS 2, na

Návrh směrnice NIS 2 rozšiřuje oblast působnosti stávající směrnice NIS o nová odvětví na základě jejich ekonomické a společenské kritičnosti a zároveň spojuje oblast působnosti s velikostí subjektu, což znamená, že směrnice NIS 2 se vztahuje na všechny střední a velké společnosti ve vybraných odvětvích nebo poskytující služby.

Ačkoli směrnice NIS 2 uvádí, že se nebude primárně vztahovat na malé podniky a mikropodniky, ve skutečnosti se má vztahovat i na malé subjekty nebo mikropodniky, které splňují určitá zde stanovená kritéria. V souladu s ustanoveními článku 2 odst. 2 písm. a) návrhu směrnice NIS 2 ve spojení s bodem 8 přílohy č. I návrhu směrnice NIS 2 se tak oblast působnosti směrnice NIS 2 rozšiřuje například na poskytovatele veřejných sítí elektronických komunikací nebo poskytovatele veřejně dostupných služeb elektronických komunikací (operátory) bez ohledu na jejich velikost.

Podle návrhu směrnice NIS 2 by měla být odvětví, na něž se vztahuje , rozšířena tak, aby bylo zajištěno komplexní pokrytí odvětví a služeb, které jsou nezbytné pro klíčové sociální a hospodářské činnosti na vnitřním trhu, a pravidla by se neměla lišit podle toho, zda jsou subjekty poskytovateli základních služeb nebo poskytovateli digitálních služeb.[18]

Subjekty by měly být klasifikovány podle odvětví, v němž působí (nebo podle druhu služeb, které poskytují), a na tomto základě rozděleny do dvou kategorií - **základní a důležité**[19]. Režimy dohledu a sankcí by se měly v jednotlivých kategoriích lišit, ale jak základní, tak důležité subjekty by měly podléhat stejným požadavkům na řízení rizik a oznamovací povinnosti.[20] Další podrobnosti viz oddíl IV. níže.

2) Nová bezpečnostní opatření a hodnocení rizik

[18] Viz 7. bod odůvodnění návrhu směrnice NIS 2.
[19] Jednotlivé subjekty spadající do těchto kategorií jsou uvedeny v přílohách I a II návrhu směrnice NIS 2.
[20] Viz 11. bod odůvodnění návrhu směrnice NIS 2.

Za prvé směrnice NIS 2 zavádí nová bezpečnostní opatření, jako je povinnost základních subjektů, včetně poskytovatelů elektronických komunikací, **posuzovat a řídit bezpečnostní rizika** vyplývající z jejich dodavatelských řetězců a dodavatelských vztahů. [21]

Opatření pro řízení rizik kybernetické bezpečnosti by měla zahrnovat alespoň:

- analýzu rizik a bezpečnostní politiku informačních systémů;
- řízení incidentů (prevence, detekce a reakce na incidenty);
- kontinuitu podnikání a krizové řízení;
- bezpečnost dodavatelského řetězce, včetně bezpečnostních aspektů souvisejících se vztahem mezi jednotlivými subjekty a jejich dodavateli nebo poskytovateli služeb, jako jsou poskytovatelé služeb ukládání a zpracování dat nebo spravovaných bezpečnostních služeb;
- bezpečnost při pořizování, vývoji a údržbě sítí a informačních systémů, včetně řešení a odhalování zranitelností;
- zásady a postupy (testování a audit) k posouzení účinnosti opatření k řízení rizik kybernetické bezpečnosti;
- používání kryptografie a šifrování.

Obecný přístup Rady k výše uvedeným kritériím přidává další, a to bezpečnost lidských zdrojů, zásady kontroly přístupu a správu aktiv.

Kompromisní pozměňovací návrh Evropského parlamentu rovněž navrhuje přidat další kritéria, a to

- základní postupy počítačové hygieny a školení o kybernetické bezpečnosti;
- používání vícefaktorového ověřování nebo řešení průběžného ověřování, zabezpečené hlasové, video a textové komunikace a případně zabezpečených systémů nouzové komunikace v rámci subjektu;
- v případě potřeby se použije také kryptografie, například šifrování.

Za druhémají členské státy možnost ve spolupráci s Evropskou komisí a Agenturou Evropské unie pro kybernetickou bezpečnost (dále jen "*ENISA")* provádět **koordinované posouzení rizik v dodavatelském řetězci** konkrétních kritických služeb, systémů nebo produktů IKT, přičemž se zohlední technické nebo netechnické rizikové faktory.[22]

Výše uvedená posouzení rizik by měla vycházet z přístupu přijatého v souvislosti s doporučením Komise (EU) 2019/534 ze dne 26. března 2019 Kybernetická bezpečnost sítí 5G (dále jen

[21] Viz článek 18 návrhu směrnice NIS 2.
[22] Viz článek 19 návrhu směrnice NIS 2.

"*doporučení o kybernetické bezpečnosti sítí 5G*") a uplatňovat kritéria stanovená v souboru nástrojů EU.[23] Směrnice NIS 2 rovněž v zásadě rozšiřuje uplatňování kritérií pro posuzování rizik dodavatelů obsažených v EU Toolboxu na kritickou infrastrukturu obecně (nejen na sítě 5G, na které byl EU Toolbox původně zaměřen). Další podrobnosti viz oddíl V. níže.

3) Přesnější ustanovení o postupu oznamování, obsahu oznámení a časových plánech[24]

Návrh směrnice NIS 2 uvádí, že zásadní a důležité subjekty se často ocitají v situaci, kdy je třeba určitou událost oznámit různým orgánům v důsledku oznamovací povinnosti obsažené v různých právních nástrojích. Takové případy vytvářejí pro povinné subjekty další zátěž. Aby se předešlo nejasnostem, pokud jde o formát a postupy takových oznámení, musí členské státy zřídit jednotné vstupní místo[25] pro všechna oznámení vyžadovaná podle směrnice o bezpečnosti sítí a informací (a také podle návrhu směrnice NIS 2) a také podle jiných právních předpisů EU, jako je nařízení (EU) 2016/679 (obecné nařízení o ochraně osobních údajů) a směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích). Návrh směrnice NIS 2 předpokládá, že agentura ENISA by měla ve spolupráci se skupinou[26] pro spolupráci vypracovat společné šablony pro oznamování prostřednictvím pokynů, které by zjednodušily a zefektivnily oznamování informací požadovaných právními předpisy EU a snížily zátěž pro společnosti. Pokud existuje podezření, že incident souvisí se závažnou trestnou činností podle práva EU nebo vnitrostátního práva, měly by členské státy rovněž vybízet zásadní a důležité subjekty, aby na základě platných pravidel trestního řízení v souladu s právem EU oznamovaly incidenty, u nichž existuje podezření na závažnou trestnou činnost, příslušným orgánům činným v trestním řízení.[27]

Návrh směrnice NIS 2 navrhuje dvoustupňový přístup k hlášení incidentů. Cílem tohoto přístupu je nalézt rovnováhu mezi rychlým hlášením (které pomáhá zmírnit potenciální šíření incidentů a umožňuje subjektům vyhledat podporu) a hloubkovým hlášením, které umožňuje využít zkušenosti z jednotlivých incidentů a pomáhá zvýšit odolnost jednotlivých subjektů i celých odvětví vůči hrozbám v oblasti kybernetické bezpečnosti. Navrhuje se, aby v případě, že se subjekty o incidentu dozvědí, byly povinny do 24 hodin podat prvotní oznámení (včetně informací nezbytných k tomu, aby se o incidentu dozvěděly příslušné orgány), po němž by nejpozději do

[23] Viz 46. a 47. bod odůvodnění návrhu směrnice NIS 2.
[24] Viz čl. 11 odst. 2, článek 20 a 55. a 56. bod odůvodnění návrhu směrnice NIS 2.
[25] V rámci České republiky je v současné době jednotným kontaktním místem Národní úřad pro kybernetickou a informační bezpečnost podle § 22 zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Lze předpokládat, že se tato skutečnost nezmění ani po přijetí směrnice NIS 2.
[26] Viz článek 12 návrhu směrnice NIS 2.
[27] Je žádoucí, aby koordinaci mezi příslušnými orgány a donucovacími orgány různých členských států případně usnadňovalo Evropské centrum pro boj proti kyberkriminalitě (EC3) a agentura ENISA.

jednoho měsíce od incidentu následovala závěrečná zpráva. Členské státy by měly zajistit, aby požadavek na předložení tohoto počátečního oznámení neodváděl zdroje ohlašujícího subjektu od činností souvisejících s řešením incidentů, které by měly být upřednostněny, a zároveň by mělo být také stanoveno, že v řádně odůvodněných případech a po dohodě s příslušnými orgány nebo CSIRT[28] se může dotčený subjekt odchýlit od lhůty 24 hodin pro počáteční oznámení a jednoho měsíce pro závěrečnou zprávu. Další podrobnosti viz oddíl VI. níže.

4) **Přísnější dohledová opatření pro vnitrostátní orgány, přísnější požadavky na vymáhání a snaha o harmonizaci sankčních režimů ve všech členských státech.[29]**

Ustanovení článků 28 až 34 návrhu směrnice NIS 2 obsahují omezené podmínky pro dohled, vymáhání a sankcionování základních a významných subjektů. Podrobnosti viz oddíl VII. níže.

5) **Posílení úlohy skupiny[30] pro spolupráci**

Skupina pro spolupráci je složena ze zástupců členských států, Evropské komise a agentury ENISA a hraje důležitou roli při utváření strategických politických rozhodnutí o nových technologiích, nových trendech a zvyšuje sdílení informací a spolupráci mezi orgány členských států.[31] Posiluje rovněž operativní spolupráci, mimo jiné v oblasti kybernetického krizového řízení. Základní rámec pro koordinované zveřejňování zranitelností a vytvoření evropského registru zranitelností, který bude zřízen a spravován agenturou ENISA.[32]

IV. Kategorie regulovaných subjektů

Směrnice NIS se původně vztahovala na dvě specifické kategorie subjektů - provozovatele základních služeb a poskytovatele digitálních služeb - přičemž v příloze směrnice NIS jsou uvedeny

[28] CSIRT = Computer Security Incident Response Team (tým pro řešení incidentů v oblasti počítačové bezpečnosti).
[29] Viz články 28 až 34 návrhu směrnice NIS 2.
[30] Viz článek 12, a zejména body odůvodnění 32-34 a 46-47 návrhu směrnice NIS 2.
[31] Evropská služba pro vnější činnost se účastní činnosti skupiny pro spolupráci jako pozorovatel. Evropské orgány dohledu se mohou v souladu s čl. 17 odst. 5 písm. c) nařízení DORA účastnit činností skupiny pro spolupráci. - Viz čl. 12 odst. 3 návrhu směrnice NIS 2.
[32] Viz článek 6 návrhu směrnice NIS 2.

typy subjektů, které do těchto dvou skupin spadají. Cílem navrhované směrnice NIS 2, jak je podrobně popsáno v jejích přílohách I a II, je tyto kategorie přejmenovat (nově se rozlišují skupiny základních a významných subjektů), rozšířit počet regulovaných subjektů a výrazně rozšířit typy subjektů, které do těchto skupin spadají. Rozdělení do kategorií má velký význam i pro způsob, jakým budou pravidla obsažená v návrhu směrnice NIS 2 prosazována (další podrobnosti viz níže v oddíle VII.).

Jak bylo uvedeno výše, oblast působnosti byla v návrhu směrnice NIS 2 rozšířena o další typy subjektů. Kromě odvětví, na která se již směrnice NIS 2 vztahuje, jsou nyní zahrnuta i základní zařízení v odvětví kanalizace, veřejné správy a vesmíru. Rozlišování mezi provozovateli základních služeb a poskytovateli digitálních služeb bylo v návrhu směrnice NIS 2 opuštěno - místo toho **se nyní rozlišuje mezi tzv. základními a důležitými subjekty na základě stupně kritičnosti odvětví**[33]. Kromě nově přidaných odvětví kanalizace, veřejné správy a vesmíru lze **zásadní subjekty** nalézt i ve známých odvětvích, jako je energetika, doprava, zdravotnictví nebo zásobování vodou. Úplný seznam základních subjektů je uveden v příloze I návrhu směrnice NIS 2.

Podle přílohy II směrnice NIS 2 patří mezi odvětví, v nichž působí **významné subjekty,** nejen poskytovatelé digitálních služeb, kteří jsou již známí ze směrnice NIS, ale také poštovní a kurýrní služby a výroba určitého zboží (včetně zdravotnických prostředků a motorových vozidel).

Není třeba zdůrazňovat, že oblast působnosti se nyní vztahuje na všechny střední a velké podniky v kritických odvětvích[34]. Mikropodniky a malé podniky se zdají být z oblasti působnosti v zásadě vyloučeny. **V článku 2 odst. 1 směrnice NIS 2 však směrnice stanoví pro tyto podniky v určitých případech protivýjimku.** Velikost subjektů se posuzuje podle doporučení Komise ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků (dále jen "*doporučení")*.[35] Podle daného doporučení jsou jednotlivé velikosti podniků definovány následovně:

- **mikropodnik**: méně než 10 zaměstnanců a roční obrat (objem peněz přijatých za určité období) nebo rozvaha (výkaz aktiv a pasiv společnosti) nižší než 2 miliony EUR;
- **malý podnik:** méně než 50 zaměstnanců a roční obrat nebo rozvaha nižší než 10 milionů EUR;
- **střední podnik:** méně než 250 zaměstnanců a roční obrat nižší než 50 milionů EUR nebo rozvaha nižší než 43 milionů EUR.

[33] Viz 11. bod odůvodnění návrhu směrnice NIS 2.
[34] Viz článek 2 návrhu směrnice NIS 2.
[35] Dokument je k dispozici na adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32003H0361

Podle v současnosti platné směrnice NIS členské státy určily konkrétní organizace, které mají být regulovány na základě toho, jak strategicky důležité jsou tyto subjekty pro stát (tj. podíl na trhu, národní bezpečnost, hospodářský dopad atd.).[36] Aby se předešlo výrazným rozdílům mezi členskými státy, nebudou již přesné prahové hodnoty pro základní (a nově i významné) služby určovány členskými státy, ale přímo směrnicí NIS 2. Pokud jde o poskytovatele služeb DNS, registry názvů TLD, poskytovatele služeb cloud computingu, poskytovatele služeb datových center a poskytovatele sítí pro doručování obsahu uvedené v bodě 8 přílohy I, jakož i poskytovatele digitálních služeb uvedené v bodě 6 přílohy II návrhu směrnice NIS 2, museli by být registrováni u agentury ENISA a agentura ENISA by tyto subjekty oznámila členským státům v jejich jurisdikci. [37]

Rozšíření okruhu subjektů, které budou podléhat úpravě předpokládané v návrhu směrnice NIS 2, je patrné i z níže uvedené tabulky:

Kategorie činností, na které se vztahuje směrnice NIS	
Provozovatelé základních služeb	**Poskytovatelé digitálních služeb**
Poskytovatelé zdravotní péče	Online tržiště
Digitální infrastruktura - IXP, služby DNS, registry TLD	Online vyhledávací služby
Pitná voda	Cloudové služby
Doprava	
Infrastruktura finančního trhu	
Energie	
Bankovnictví	
Kategorie činností, na které se vztahuje návrh směrnice NIS 2	
Základní subjekty	**Důležité subjekty**
Prakticky všechny oblasti uvedené výše pro směrnici NIS provozovateli základních služeb.	Online tržiště
Další služby související se zdravotnictvím - včetně farmaceutických firem, některých výrobců zdravotnických prostředků, výzkumných pracovníků.	Online vyhledávací služby

[36] Viz článek 6 směrnice obezpečnosti sítí a informací.
[37] Viz článek 25 návrhu směrnice NIS 2.

Další služby digitální infrastruktury - služby cloud computingu, datová centra, CDN, poskytovatelé sítí.	Služby sociálních sítí
Odpadní voda	Výroba a distribuce potravin
Prostor	Poštovní služby
Veřejná správa	Nakládání s odpady
	Výrobci chemikálií
	Zpracovatelský průmysl - zdravotnické prostředky, elektronické výrobky a zařízení, stroje, vozidla a dopravní prostředky.
+ případně řízení[38] ICT služeb (B2B) - *podle obecného přístupu Rady*	**+** případně vzdělávání a výzkum - *podle kompromisního pozměňovacího návrhu Evropského parlamentu*

Vzhledem k tomu, že otázka rozsahu subjektů, na které se má nová směrnice NIS 2 vztahovat, byla největším problémem, který se v procesu přijímání směrnice objevil (a stále se řeší), není překvapivé, že do původního návrhu silně zasahují (a v některých případech jej přímo přepracovávají) pozměňovací návrhy Rady a Evropského parlamentu.

Návrh směrnice NIS 2:

Návrh směrnice NIS 2 představil následující legislativní návrh, podle něhož by se směrnice NIS 2 měla vztahovat na [39]veřejné a soukromé subjekty, které jsou v příloze I označeny jako základní subjekty a v příloze II jako významné subjekty. Tato směrnice se nevztahuje na subjekty, které se kvalifikují jako mikropodniky a malé podniky ve smyslu doporučení. Bez ohledu na jejich velikost by se však směrnice NIS 2 měla vztahovat i na základní a významné subjekty, jak jsou uvedeny v přílohách I a II směrnice NIS 2, které splňují zvláštní podmínky:

a) služby poskytuje jeden z následujících subjektů:

[38] Včetně těchto subjektů (podle čl. 4 odst. 26ac) 26ad) obecného přístupu Rady):
Poskytovatelé spravovaných služeb - tj. jakýkoli subjekt, který poskytuje služby, jako jsou sítě, aplikace, infrastruktura a zabezpečení, prostřednictvím průběžné a pravidelné správy, podpory a aktivní administrace v prostorách zákazníka, v jeho datovém centru (hosting) nebo v datovém centru třetí strany.
Poskytovatelé spravovaných bezpečnostních služeb - tj. jakýkoli subjekt, který zajišťuje externí monitorování a správu bezpečnostních zařízení a systémů. Mezi běžné služby patří spravované firewally, detekce narušení, virtuální privátní sítě, skenování zranitelností a antivirové služby.
[39] Viz článek 2 návrhu směrnice NIS 2.

- veřejné sítě elektronických komunikací nebo veřejně dostupné služby elektronických komunikací uvedené v bodě 8 přílohy I směrnice NIS 2;
- poskytovatelé služeb vytvářejících důvěru podle bodu 8 přílohy I směrnice NIS 2;
- registry doménových jmen nejvyšší úrovně a poskytovatele služeb systému doménových jmen (DNS) uvedené v bodě 8 přílohy I směrnice NIS 2;

b) subjekt je subjektem[40] veřejné správy;
c) subjekt je jediným poskytovatelem služby v členském státě;
d) případné narušení služby poskytované subjektem by mohlo mít dopad na veřejnou bezpečnost, veřejnou bezpečnost nebo veřejné zdraví;
e) případné narušení služby poskytované subjektem by mohlo vyvolat systémová rizika, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad;
f) subjekt je kritický z důvodu svého specifického významu na regionální nebo celostátní úrovni pro dané odvětví nebo druh služby nebo pro jiná vzájemně závislá odvětví v členském státě;
g) subjekt je označen jako kritický subjekt podle návrhu směrnice o CER nebo jako subjekt rovnocenný kritickému subjektu podle článku 7 uvedené směrnice.

Návrh směrnice zároveň požaduje, aby členské státy sestavily seznam subjektů určených podle výše uvedených písmen b) až f) a předložily jej Evropské komisi do šesti měsíců po uplynutí lhůty pro provedení směrnice. Členské státy tento seznam pravidelně, a poté alespoň každé dva roky, přezkoumají a případně aktualizují.

Obecný přístup Rady:

S ohledem na četná obvinění týkající se přílišného rozsahu subjektů, na které se vztahuje návrh směrnice NIS 2, přišla Rada v rámci obecného přístupu s vlastní upravenou klasifikací subjektů. Obecný přístup Rady především upřesňuje, že směrnice NIS 2 se má vztahovat na subjekty vymezené v přílohách I a II, které splňují nebo překračují stropy pro střední podniky.

Oproti původnímu návrhu směrnice NIS 2 rozšiřuje obecný přístup Rady okruh subjektů, na které se má směrnice vztahovat, bez ohledu na jejich velikost. Kromě subjektů uvedených pod písmeny a) až g) výše přidává také kvalifikované poskytovatele svěřenských služeb a nekvalifikované poskytovatele svěřenských služeb. Pokud jde o subjekty, které jsou jediným poskytovatelem služby v členském státě, upřesňuje se, že se musí jednat o službu, která je zásadní pro zachování kritických společenských nebo hospodářských činností (a zároveň se navrhuje vyjmout subjekt uvedený v písmenu f) výše). Potenciální narušení podle písmen d) a e) výše souvisí s významností

[40] Jak je definováno v čl. 4 bodu 23 návrhu směrnice NIS 2.

dopadu a riziky. Mezi subjekty, na které se vztahuje směrnice NIS 2, jsou výslovně zahrnuty i subjekty veřejné správy, a to bez ohledu na jejich velikost.[41]

Obecný přístup Rady ve svém článku 2a jasně stanoví, které subjekty mají být považovány za zásadní a které za důležité.

Mezi subjekty, na které by se měla směrnice NIS 2 vztahovat, je **třeba za zásadní považovat**:

a) subjekty typu uvedeného v bodech 1 až 8a a 10 přílohy I směrnice NIS 2, které překračují stropy pro střední podniky;
b) střední subjekty uvedené v čl. 2 odst. 2 písm. a) bodě i) směrnice NIS 2.
   - tj. **poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací.**
c) subjekty uvedené v čl. 2 odst. 2 písm. a) bodech ii) a iv) směrnice NIS 2, bez ohledu na jejich velikost.
   - tj. kvalifikovaní poskytovatelé služeb vytvářejících důvěru, registry doménových jmen nejvyšší úrovně.
d) subjekty uvedené v čl. 2 odst. 2 písm. g) a čl. 2 odst. 2a směrnice NIS 2, bez ohledu na jejich velikost.
   - tj. kritické subjekty
e) subjekty, které členské státy určily před vstupem této směrnice v platnost jako provozovatele základních služeb v souladu se směrnicí o bezpečnosti sítí a informací nebo vnitrostátními právními předpisy.[42]
f) subjekty, které překračují stropy pro střední podniky typu uvedeného v příloze II, které členské státy určí jako nezbytné na základě kritérií uvedených v čl. 2 odst. 2 písm. c) až e) směrnice NIS 2;
g) středně velké subjekty, které členské státy určí jako zásadní na základě kritérií uvedených v čl. 2 odst. 2 písm. c) až e) směrnice NIS 2;
h) mikro nebo malé subjekty[43], které členské státy určí jako nezbytné na základě vnitrostátního posouzení rizik.

Mezi subjekty, na které by se měla směrnice NIS 2 vztahovat, je **třeba považovat za důležité tyto**:

a) subjekty typu uvedeného v příloze I směrnice NIS 2, které se kvalifikují jako střední podniky, a subjekty typu uvedeného v příloze II, které splňují nebo překračují stropy pro střední podniky;

[41] Viz čl. 2 odst. 2a obecného přístupu Rady.
[42] Pokud je zřízen členskými státy.
[43] stanovené v odst. 2 písm. a) bodě i) nebo určené podle odst. 2 písm. c) až e) tohoto článku.

b) subjekty uvedené v čl. 2 odst. 2 bodě iii) směrnice NIS 2 bez ohledu na velikost - tj. nekvalifikovaní poskytovatelé služeb vytvářejících důvěru;
c) malé subjekty a mikropodniky uvedené v čl. 2 odst. 2 písm. a) bodě i) - tj. **poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací;**
d) malé subjekty a mikrosubjekty, které členské státy určí jako důležité subjekty na základě čl. 2 odst. 2 písm. c) až e) směrnice NIS 2 - tj. jediní poskytovatelé v členském státě, kteří jsou nezbytní pro zachování kritických společenských nebo hospodářských činností atd.

Z výše uvedeného je zřejmé, že pokud jde o poskytovatele elektronických komunikací, vztahuje se na ně návrh směrnice NIS 2 bez ohledu na jejich velikost.

Obecný přístup Rady rovněž výslovně uvádí, na které subjekty a činnosti se návrh směrnice NIS 2 nevztahuje:

- **subjekty,** které nespadají do oblasti působnosti práva EU, a v každém případě všechny subjekty, které vykonávají zejména činnosti v oblasti obrany, národní bezpečnosti, veřejné bezpečnosti nebo vymáhání práva, bez ohledu na to, který subjekt tyto činnosti vykonává a zda se jedná o veřejný nebo soukromý subjekt;[44]
- subjekty, které vykonávají činnosti v oblasti soudnictví, parlamentů nebo centrálních bank;
- **činnosti subjektů, které** nespadají do oblasti působnosti práva EU, a v každém případě všechny činnosti týkající se národní bezpečnosti nebo obrany, bez ohledu na to, který subjekt tyto činnosti vykonává a zda se jedná o veřejný nebo soukromý subjekt;
- činnost subjektů v oblasti soudnictví, parlamentů, centrálních bank a v oblasti veřejné bezpečnosti, včetně subjektů veřejné správy, které vykonávají činnosti v oblasti prosazování práva za účelem předcházení, vyšetřování, odhalování nebo stíhání trestných činů nebo výkonu trestů;
- subjekty, na které se nařízení DORA nevztahuje.[45]

Pro úplnost není třeba dodávat, že směrnicí NIS 2 nejsou dotčeny právní předpisy EU o ochraně osobních údajů (konkrétně GDPR a směrnice o ochraně soukromí a elektronických komunikacích).

[44] V případech, kdy subjekty veřejné správy vykonávají činnosti ve dvou výše uvedených oblastech pouze jako součást své celkové činnosti, měly by být z oblasti působnosti směrnice NIS 2 vyloučeny v celém rozsahu. - Viz článek 3a obecného přístupu Rady.
[45] Viz čl. 2 odst. 3a a 3aa obecného přístupu Rady.

Ačkoli obecný přístup Rady poněkud zužuje původní velmi obecný návrh směrnice NIS 2, rozsah působnosti subjektů (za předpokladu, že návrh bude přijat v podobě předložené Radou) je vzhledem k současnému stavu založenému na směrnici NIS stále velmi rozsáhlý.

Kompromisní pozměňovací návrh Evropského parlamentu:

Kompromisní pozměňovací návrh Evropského parlamentu nemění navrhovaný systém klasifikace právnických osob, ale ve velké míře se zaměřuje na povinnost členských států vytvořit seznam základních a významných subjektů a jejich oznamovací povinnost.

Kompromisní pozměňovací návrh Evropského parlamentu dále rozvíjí ustanovení návrhu směrnice NIS 2, která stanoví, že členské státy budou povinny vypracovat seznam všech základních a důležitých subjektů. Podle kompromisního pozměňovacího návrhu by tento seznam měl zahrnovat subjekty, které splňují obecně platná kritéria týkající se velikosti, a také malé podniky a mikropodniky, které splňují určitá kritéria, jež naznačují klíčovou roli pro ekonomiku nebo společnost členských států. Aby příslušné orgány a CSIRT mohly poskytovat pomoc a varovat subjekty před kybernetickými incidenty, které by je mohly ovlivnit, je důležité, aby tyto orgány měly správné kontaktní údaje subjektů. Subjekty by proto měly předložit (a také informovat o jakékoli změně) alespoň tyto informace: název subjektu, adresu a aktuální kontaktní údaje[46] a příslušné odvětví (odvětví) a pododvětví (pododvětví) uvedené (uvedená) v přílohách I a II směrnice NIS2. Agentura ENISA a skupina pro spolupráci vydají pokyny a šablony týkající se této povinnosti.

Členské státy mají rovněž povinnost oznámit Komisi a skupině pro spolupráci počet základních a významných subjektů. To zahrnuje i oznámení názvů malých podniků a mikrosubjektů označených za zásadní a významné, aby Komise mohla posoudit soulad mezi přístupy členských států. S těmito informacemi by mělo být nakládáno jako s přísně důvěrnými.

V souladu s kompromisním pozměňovacím návrhem Evropského parlamentu by Evropská komise měla rovněž vydat pokyny na podporu členských států při správném provádění ustanovení o oblasti působnosti a při posuzování přiměřenosti povinností stanovených směrnicí NIS 2, zejména s ohledem na komplikované případy (subjekty se složitými obchodními modely nebo provozními prostředími, kdy subjekt může současně splňovat kritéria přiřazená jak základním, tak významným subjektům, nebo může současně vykonávat činnosti, které zčásti spadají do oblasti působnosti směrnice NIS 2 a zčásti mimo ni). Malé podniky a mikropodniky, na které se vztahuje směrnice NIS 2, by měly být rovněž podporovány pokyny Komise.

[46] Včetně: e-mailových adres, IP rozsahů, telefonních čísel.

V. Vliv směrnice NIS 2 na hodnocení dodavatelů

Vzhledem k rostoucímu počtu kybernetických útoků a narušení kybernetické bezpečnosti, kdy se záškodníkům podařilo narušit bezpečnost sítě a informačních systémů subjektu zneužitím zranitelností produktů a služeb třetích stran, by subjekty měly posuzovat a zohledňovat celkovou kvalitu produktů a postupy kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje.[47]

Evropská komise proto považuje za nutné lépe regulovat hodnocení rizik, včetně koordinovaného hodnocení na úrovni EU. Návrh směrnice NIS 2 a obecný přístup Rady jsou plně v souladu s tím, jak by mělo být koordinované hodnocení rizik prováděno. Kompromisní pozměňovací návrh Evropského parlamentu však k tomuto tématu přidává několik dalších úprav.

S cílem dále řešit klíčová rizika dodavatelského řetězce a pomoci subjektům působícím v odvětvích, na něž se vztahuje směrnice NIS 2, vhodně řídit rizika související s kybernetickou bezpečností dodavatelského řetězce a dodavatelů by skupina pro spolupráci ve spolupráci s Evropskou komisí a agenturou ENISA měla provádět **koordinovaná posouzení rizik dodavatelského řetězce pro jednotlivá odvětví,** a to v podobě, jaká již byla provedena pro sítě 5G v návaznosti na doporučení o kybernetické bezpečnosti sítí 5G, s cílem určit pro každé odvětví, které [48]služby, systémy nebo produkty IKT a ICS jsou kritické, příslušné hrozby a zranitelná místa. Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA rovněž určí konkrétní kritické služby, systémy nebo produkty IKT, které mohou být předmětem koordinovaného posouzení rizik.[49]

Kompromisní pozměňovací návrh Evropského parlamentu k tomu dodává, že **posouzení rizik by mělo identifikovat**: opatření, plány na zmírnění a osvědčené postupy proti kritickým závislostem, potenciálním jediným místům selhání, hrozbám, zranitelným místům a dalším rizikům spojeným s dodavatelským řetězcem a mělo by zkoumat způsoby, jak dále podporovat jejich širší přijetí subjekty. Současně upozorňuje, že je třeba posoudit i **potenciální netechnické rizikové faktory, jako je nepatřičný vliv třetí země na dodavatele a poskytovatele služeb, zejména v případě alternativních modelů řízení,** neboť mohou zahrnovat skryté zranitelnosti nebo zadní vrátka a

[47] Viz 43. bod odůvodnění a čl. 18 odst. 3 návrhu směrnice NIS 2.
[48] ICS se uvádí v souladu s kompromisní změnou Evropského parlamentu.
[49] Viz čl. 19 odst. 2 návrhu směrnice NIS 2.

potenciální systémové narušení dodávek, zejména v případě technologického uzamčení nebo závislosti na poskytovateli.[50]

Posouzení rizik v dodavatelském řetězci by mělo (s ohledem na vlastnosti dotčeného odvětví) zohlednit **jak technické, tak případně netechnické faktory,** [51]včetně těch, které jsou definovány v doporučení o kybernetické bezpečnosti sítí 5G, v celoevropském koordinovaném posouzení rizik v oblasti bezpečnosti sítí 5G a v souboru nástrojů EU pro kybernetickou bezpečnost sítí 5G schváleném skupinou pro spolupráci.

Pro **určení dodavatelských řetězců, které by měly být předmětem koordinovaného posouzení rizik, je třeba vzít v úvahu** následující kritéria:

(i) rozsah, v jakém zásadní a důležité subjekty využívají konkrétní kritické služby, systémy nebo produkty IKT a spoléhají se na ně;

(ii) význam konkrétních kritických služeb, systémů nebo produktů IKT pro plnění kritických nebo citlivých funkcí, včetně zpracování osobních údajů;

(iii) dostupnost alternativních služeb, systémů nebo produktů ICT;

(iv) odolnost celého dodavatelského řetězce služeb, systémů nebo produktů IKT (*po celou dobu jejich životního cyklu*) vůči rušivým událostem a

(v) u nově vznikajících služeb, systémů nebo produktů IKT jejich potenciální budoucí význam pro činnost subjektů.[52]

Kompromisní pozměňovací návrh Evropského parlamentu v této souvislosti opakuje, že **zvláštní důraz by měl být kladen na služby, systémy nebo produkty IKT, které podléhají zvláštním požadavkům ze strany třetích zemí**.

Podle kompromisního pozměňovacího návrhu Evropského parlamentu by také skupina zúčastněných stran pro certifikaci kybernetické bezpečnosti zřízená podle článku 22 nařízení (EU) 2019/881[53] měla vydat stanovisko k posouzení bezpečnostních rizik konkrétních kritických služeb, systémů nebo dodavatelských řetězců IKT a ICS. Skupina pro spolupráci a agentura ENISA by měly toto stanovisko zohlednit.[54]

---

[50] Viz 46. bod odůvodnění kompromisního pozměňovacího návrhu Evropského parlamentu.
[51] Viz článek 19 návrhu směrnice NIS 2.
[52] Viz 47. bod odůvodnění návrhu směrnice NIS 2.
[53] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (Agentura Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 (zákon o kybernetické bezpečnosti).
[54] Viz 47a. bod odůvodnění kompromisního pozměňovacího návrhu Evropského parlamentu.

VI. Spolupráce na vnitrostátní úrovni a oznamovací povinnost

Spolupráce mezi vnitrostátními a nadnárodními orgány je jedním ze základních kamenů nově připravovaného návrhu směrnice NIS 2. Podle článku 8 návrhu směrnice NIS 2 každý členský stát určí jeden nebo více příslušných orgánů odpovědných za kybernetickou bezpečnost a za úkoly v oblasti dohledu uvedené v kapitole VI návrhu směrnice NIS 2.[55]

Návrh směrnice NIS 2 vyžaduje, aby členské státy zajistily, že jejich příslušné orgány na vnitrostátní úrovni nebo jejich CSIRT obdržely zprávy o incidentech a významných kybernetických hrozbách, jakož i o téměř nezaznamenaných incidentech, které byly předloženy podle směrnice NIS 2. Pokud se členský stát rozhodne, že jeho týmy CSIRT tato hlášení nedostanou, bude týmům CSIRT v rozsahu nezbytném pro plnění jejich úkolů umožněn přístup k údajům o incidentech oznámených základními nebo významnými subjekty podle článku 20 návrhu směrnice NIS 2. Současně každý členský stát zajistí, aby jeho příslušné orgány nebo týmy CSIRT informovaly své jednotné kontaktní místo o oznámeních o incidentech, významných kybernetických hrozbách a skoronehodách předložených podle směrnice NIS 2.[56]

Členské státy (v rozsahu nezbytném pro účinné plnění úkolů a povinností stanovených ve směrnici NIS 2) rovněž **zajistí vhodnou spolupráci** mezi příslušnými orgány a jednotnými kontaktními místy a orgány činnými v trestním řízení, orgány pro ochranu údajů, orgány odpovědnými za kritickou infrastrukturu podle návrhu směrnice CER a vnitrostátními finančními orgány určenými v souladu s návrhem směrnice DORA v daném členském státě.[57] V obecném přístupu Rady se dále navrhuje, aby mezi spolupracující subjekty podle čl. 11 odst. 4 směrnice NIS 2 byly zařazeny následující subjekty: příslušné orgány podle prováděcího nařízení Komise 2019/1583[58], vnitrostátní regulační orgány určené v souladu s EECC[59] , vnitrostátní orgány určené podle článku 17 nařízení (EU) č. 910/2014[60], jakož i příslušné orgány určené jinými odvětvovými právními akty EU.

---

[55] Členské státy mohou za tímto účelem rovněž určit stávající orgán nebo stávající orgány.
[56] Viz čl. 11 odst. 3 návrhu směrnice NIS 2.
[57] Viz čl. 11 odst. 4 návrhu směrnice NIS 2.
[58] Prováděcí nařízení Komise (EU) 2019/1583 ze dne 25. září 2019, kterým se mění prováděcí nařízení (EU) 2015/1998, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti, pokud jde o opatření v oblasti kybernetické bezpečnosti.
[59] Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví Evropský kodex elektronických komunikací. Tato směrnice je rovněž doplněna do kompromisní novely Evropského parlamentu.
[60] 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.

Členské státy rovněž zajistí, aby jejich příslušné orgány **pravidelně poskytovaly příslušným orgánům** určeným podle návrhu směrnice CER **informace o** kybernetických bezpečnostních rizicích, kybernetických hrozbách a incidentech, které mají vliv na základní subjekty označené podle návrhu směrnice CER za kritické nebo za subjekty rovnocenné kritickým subjektům, jakož i o opatřeních přijatých příslušnými orgány v reakci na tato rizika a incidenty.[61] Obecný přístup Rady rovněž doplňuje vyměňované informace o identifikaci kritických subjektů a kybernetických hrozeb a incidentů, jakož i o nekybernetických rizicích, hrozbách a incidentech, které mají vliv na základní subjekty. Zároveň mezi subjekty vyměňující si informace podle tohoto ustanovení řadí i subjekty podle návrhu směrnice NIS 2, návrhu DORA, jakož i subjekty podle EECC a nařízení (EU) č. 910/2014.

Jak bylo popsáno výše, návrh směrnice NIS 2 zavádí **dvoustupňový systém hlášení incidentů**. Tento systém je konkrétně popsán v článku 20 návrhu směrnice NIS 2. Obecný přístup Rady v zásadě souhlasí s návrhem směrnice NIS 2 a příliš jej nemění, kompromisní pozměňovací návrh Evropského parlamentu však navrhuje poměrně dalekosáhlé změny v této oblasti.

Kromě výše uvedeného dvoustupňového systému stanoví kompromisní návrh Evropského parlamentu o kompromitaci další rozdělení incidentů a hovoří o **významném incidentu,** který může mít dopad na důvěrnost, integritu nebo dostupnost služby. Pokud má tento významný incident dopad na dostupnost jejich služeb, měly by zásadní a důležité subjekty informovat CSIRT do 24 hodin od okamžiku, kdy se o incidentu dozvěděly, zatímco významné incidenty, které narušují důvěrnost a integritu jejich služeb, by měly být oznámeny do 72 hodin od okamžiku, kdy se o incidentu dozvěděly. Není třeba dodávat, že rozlišení mezi typy incidentů není založeno na závažnosti incidentu, ale na obtížnosti pro ohlašující subjekt incident vyhodnotit, na jeho důležitosti a na schopnosti ohlásit informace, které mohou být pro CSIRT užitečné.[62]

Pokud jde o oznamovací povinnost, členské státy musí především zajistit, aby základní a důležité subjekty bez zbytečného odkladu oznámily (v souladu s podmínkami stanovenými ve směrnici) **každou událost, která má významný dopad na poskytování jejich služeb**. Musí především informovat příslušné orgány, týmy CSIRT[63], jakož i své příjemce (kde je to vhodné, zejména v případech incidentů, které mohou mít nepříznivý vliv na poskytování služby příjemci). Zásadní a důležité subjekty musí rovněž bez zbytečného odkladu hlásit veškeré významné kybernetické hrozby, které zjistí a které by mohly vyústit ve významný incident.

[61] Viz čl. 11 odst. 5 návrhu směrnice NIS 2.
[62] Viz 55a. bod odůvodnění kompromisní novely Evropského parlamentu.
[63] Zpráva musí mimo jiné obsahovat veškeré informace, které příslušnému orgánu nebo CSIRT umožní určit případný přeshraniční dopad incidentu.

Pokud je událost považována za významnou, stanoví návrh směrnice NIS 2 v čl. 20 odst. 3 následující:

a) incident způsobil nebo má potenciál způsobit dotčenému subjektu podstatné narušení provozu nebo finanční ztráty;
b) událost ovlivnila nebo může ovlivnit jiné fyzické nebo právnické osoby tím, že způsobí značné hmotné nebo nehmotné škody.

Kompromisní pozměňovací návrh Evropského parlamentu uvádí další **kritéria pro určení významné události** a spojuje je s posouzením následujících kritérií, která je třeba zohlednit:

a) počet příjemců služeb, kterých se incident týká;
b) dobu trvání incidentu;
c) zeměpisné rozložení oblasti zasažené událostí;
d) do jaké míry je ovlivněno fungování a kontinuita služby;
e) rozsah dopadu na hospodářské a společenské činnosti.

Podle návrhu směrnice NIS 2[64] by členské státy měly zajistit, aby dotčené subjekty za účelem splnění **oznamovací povinnosti** předložily příslušným orgánům nebo CSIRT:

a) prvotní oznámení - bez zbytečného odkladu a v každém případě do 24 hodin poté, co se o incidentu dozvěděly; v prvotním oznámení se uvede, zda je incident pravděpodobně způsoben protiprávním nebo zákeřným jednáním;
b) průběžnou zprávu o aktuálním stavu (na žádost příslušného orgánu nebo CSIRT);
c) závěrečnou zprávu - nejpozději do jednoho měsíce od podání prvního oznámení; závěrečná zpráva musí obsahovat alespoň:
    - podrobný popis incidentu, jeho závažnosti a dopadu;
    - typ hrozby nebo hlavní příčinu, která incident pravděpodobně vyvolala;
    - uplatňovaná a průběžná zmírňující opatření.

Jak již bylo stručně uvedeno výše, pokud jde o počáteční oznámení, kompromisní pozměňovací návrh Evropského parlamentu navrhuje poněkud odlišné stanovení lhůt pro oznámení[65] o jejich provedení:

a) incidenty, které významně narušují dostupnost služeb poskytovaných subjektem - bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy se o incidentu dozví;

[64] Viz čl. 20 odst. 4 návrhu směrnice NIS 2.
[65] Podle čl. 20 odst. 4 písm. a) kompromisního pozměňovacího návrhu Evropského parlamentu by se daná oznámení měla zasílat CSIRT.

b) incidenty, které mají významný dopad na subjekt jiný než na dostupnost služeb poskytovaných tímto subjektem - bez zbytečného odkladu a v každém případě do 72 hodin od okamžiku, kdy se o incidentu dozví;
c) incidenty, které mají významný dopad na služby poskytovatele[66] služeb vytvářejících důvěru nebo na osobní údaje uchovávané tímto poskytovatelem služeb vytvářejících důvěru - bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy se o incidentu dozví.

Zároveň musí členské státy zajistit, aby se dotčené subjekty mohly v řádně odůvodněných případech a po dohodě s příslušnými orgány nebo CSIRT odchýlit od lhůt stanovených ve výše uvedených bodech. Kompromisní pozměňovací návrh Evropského parlamentu navrhuje doplnit povinnost zajistit důvěrnost a náležitou ochranu citlivých informací o incidentech sdílených s CSIRT, jakož i přijmout opatření a postupy pro sdílení a opakované použití informací o incidentech.[67] Tento kompromisní pozměňovací návrh rovněž vyžaduje, aby agentura ENISA ve spolupráci se skupinou pro spolupráci vypracovala a průběžně zdokonalovala společné šablony pro oznamování prostřednictvím pokynů s cílem zjednodušit a zefektivnit oznamování informací vyžadovaných právními předpisy EU a snížit zátěž pro oznamující subjekty.[68]

Příslušné vnitrostátní orgány nebo CSIRT[69] poskytnou oznamujícímu subjektu do 24 hodin od obdržení prvního oznámení odpověď, včetně prvotní zpětné vazby k incidentu a na žádost subjektu pokyny k provedení možných opatření ke zmírnění následků (+ případně také pokyny k oznámení incidentu orgánům činným v trestním řízení - pokud je podezření, že incident má trestněprávní povahu).

V případě potřeby, a zejména pokud se incident týká dvou nebo více členských států, informuje příslušný orgán nebo CSIRT o incidentu ostatní dotčené členské státy a agenturu ENISA.[70] Pokud je informovanost veřejnosti nezbytná k prevenci incidentu nebo k řešení probíhajícího incidentu

[66] "**Poskytovatelem služeb vytvářejících důvěru**" se rozumí fyzická nebo právnická osoba, která poskytuje jednu nebo více služeb vytvářejících důvěru buď jako kvalifikovaný, nebo jako nekvalifikovaný poskytovatel služeb vytvářejících důvěru - viz čl. 3 bod 19 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.
[67] Viz čl. 20 odst. 4 kompromisní novely Evropského parlamentu.
[68] Viz čl. 20 odst. 4a kompromisní novely Evropského parlamentu.
[69] 2. Pokud CSIRT neobdržel oznámení uvedené v odstavci 1 , poskytne příslušný orgán ve spolupráci s CSIRT pokyny. 3. CSIRT poskytne další technickou podporu, pokud o to dotčený subjekt požádá - viz čl. 20 odst. 5 návrhu směrnice NIS 2.
[70] Všechny zúčastněné orgány musí zachovávat bezpečnostní a obchodní zájmy subjektu a důvěrnost poskytnutých informací.

nebo pokud je zveřejnění incidentu jinak ve veřejném zájmu, může příslušný orgán nebo CSIRT[71] po konzultaci s dotčeným subjektem o incidentu informovat veřejnost nebo to po subjektu požadovat.

Návrh směrnice NIS 2 rovněž stanoví povinnost jednotného kontaktního místa každého členského státu předkládat agentuře ENISA každý měsíc souhrnnou zprávu obsahující anonymizované a agregované údaje o oznámených incidentech, významných kybernetických hrozbách[72] a téměř nehodách[73]. S cílem přispět k poskytování srovnatelných informací může agentura ENISA vydat technické pokyny k parametrům informací obsažených v souhrnné zprávě. Příslušné orgány rovněž poskytnou informace o incidentech a kybernetických hrozbách oznámených základními subjekty, které jsou podle návrhu směrnice CER označeny za kritické subjekty nebo za subjekty rovnocenné kritickým subjektům.[74]

Návrh směrnice NIS 2 předpokládá, že Evropská komise může přijmout prováděcí akty, které blíže určí druh informací, formát a postup oznámení. Komise může rovněž přijmout prováděcí akty, kterými blíže určí případy, kdy se událost považuje za významnou. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 37 odst. 2 návrhu směrnice NIS 2 (tj. postupem ve výboru v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí).

VII. Prosazování směrnice NIS 2 a sankce

Návrh směrnice NIS 2 zavádí úpravy v oblasti dohledu a prosazování pravidel obsažených ve směrnici s cílem jejího většího sjednocení a vyjasnění. Je na členských státech, aby zajistily, že

[71] jakož i orgány nebo CSIRT jiných dotčených členských států (v případě potřeby) - viz čl. 20 odst. 2 návrhu směrnice NIS 2.

[72] "**Významná kybernetická hrozba**" je pojem, který byl do definic směrnice NIS 2 doplněn v obecném přístupu Rady a znamená: "*kybernetickou hrozbu, u níž lze na základě jejích technických vlastností předpokládat, že může mít závažný dopad na síť a informační systémy subjektu nebo jeho uživatelů tím, že způsobí značné materiální nebo nemateriální ztráty.*"

[73] "**Téměř chybějící**" nebo "téměř **chybějící**" je termín, který byl do směrnice NIS 2 přidán v kompromisní novele Evropského parlamentu a také v obecném přístupu Rady.
Podle novely o kompromitaci se jí rozumí "*událost, která mohla ohrozit dostupnost, pravost, integritu nebo důvěrnost údajů nebo mohla způsobit škodu, ale podařilo se jí zabránit v tom, aby měla negativní dopad*". "
Podle obecného přístupu: "*událost, která mohla potenciálně způsobit škodu na síti a informačních systémech subjektu nebo jeho uživatelů, ale které se podařilo zabránit, aby se plně projevila.*"

[74] Viz čl. 20 odst. 9 a 10 návrhu směrnice NIS 2.

příslušné orgány budou sledovat dodržování směrnice NIS 2, a aby zajistily, že přijmou opatření nezbytná k jejímu dodržování.[75]

S cílem posílit pravomoci a činnosti v oblasti dohledu by směrnice NIS 2 měla stanovit **minimální seznam opatření** a prostředků **dohledu**, jejichž prostřednictvím mohou příslušné orgány vykonávat dohled nad základními a významnými subjekty. Návrh směrnice NIS 2 rozlišuje **dva režimy dohledu podle toho**, zda jsou určeny pro základní nebo významné subjekty, s ohledem na zajištění spravedlivé rovnováhy povinností jak pro subjekty, tak pro příslušné orgány. Podstatné subjekty by měly podléhat **plnohodnotnému režimu dohledu** (*ex ante* i *ex post),* zatímco významné subjekty by měly podléhat **mírnému režimu dohledu,** pouze *ex post*. Lehký režim dohledu ve skutečnosti znamená, že důležité subjekty by neměly systematicky dokumentovat dodržování požadavků na řízení rizik kybernetické bezpečnosti, zatímco příslušné orgány by měly uplatňovat reaktivní přístup k dohledu *ex-post* a nemají obecnou povinnost vykonávat dohled nad těmito subjekty. [76]

Formy opatření dohledu pro oba režimy dohledu jsou uvedeny v následující tabulce. Není třeba dodávat, že obecný přístup Rady navrhuje doplnit tato kritéria o to, že se na ně vztahují "**alespoň**" tato kritéria - to z nich činí demonstrativní částku, kterou mohou členské státy rozšířit.[77]

Základní subjekty (plnohodnotný režim dohledu)[78]	**Důležité subjekty (mírný režim dohledu)[79]**
kontroly na místě a dohled mimo místo, včetně namátkových kontrol.	kontroly na místě a *následný* dohled mimo místo.
pravidelné audity	-
cílené bezpečnostní audity na základě posouzení rizik nebo dostupných informací souvisejících s riziky.	cílené bezpečnostní audity na základě posouzení rizik nebo dostupných informací souvisejících s riziky.
bezpečnostní prověrky na základě objektivních, nediskriminačních, spravedlivých a transparentních kritérií hodnocení rizik.	bezpečnostní prověrky na základě objektivních, spravedlivých a transparentních kritérií hodnocení rizik.

[75] Viz čl. 28 odst. 1 návrhu směrnice NIS 2.
[76] Viz 70. bod odůvodnění návrhu směrnice NIS 2.
[77] Viz čl. 29 odst. 2 a čl. 30 odst. 2 obecného přístupu Rady.
[78] Viz čl. 29 odst. 2 návrhu směrnice NIS 2 a kompromisní pozměňovací návrh Evropského parlamentu.
[79] Viz čl. 30 odst. 2 návrhu směrnice NIS 2 a kompromisní pozměňovací návrh Evropského parlamentu.

žádosti o informace nezbytné k posouzení opatření kybernetické bezpečnosti přijatých subjektem, včetně zdokumentovaných politik kybernetické bezpečnosti, jakož i plnění oznamovací povinnosti vůči agentuře ENISA.	žádosti o veškeré informace nezbytné k následnému posouzení opatření kybernetické bezpečnosti, včetně zdokumentovaných politik kybernetické bezpečnosti, jakož i splnění oznamovací povinnosti vůči agentuře ENISA.
žádosti o přístup k údajům, dokumentům nebo jakýmkoli informacím, které jsou nezbytné pro plnění jejich úkolů v oblasti dohledu.	žádosti o přístup k údajům, dokumentům a/nebo informacím nezbytným pro plnění úkolů dohledu.
žádosti o důkazy o provádění implementace zásad kybernetické bezpečnosti, jako jsou výsledky bezpečnostních auditů provedených kvalifikovaným auditorem a příslušné podklady.	*+ požaduje důkazy o provádění implementace zásad kybernetické bezpečnosti, jako jsou výsledky bezpečnostních auditů provedených kvalifikovaným auditorem a příslušné podklady (doplnění tohoto kritéria na základě požadavku obecného přístupu Rady).*
+ vyšetřování případů nedodržování předpisů a jejich dopadů na bezpečnost služeb (podle kompromisního pozměňovacího návrhu Evropského parlamentu).	*+ vyšetřování případů nedodržování předpisů a jejich dopadů na bezpečnost služeb (podle kompromisního pozměňovacího návrhu Evropského parlamentu).*
+ cílené bezpečnostní audity prováděné kvalifikovaným nezávislým subjektem nebo příslušným orgánem (namísto pravidelného auditu - podle kompromisní novely Evropského parlamentu).	*+ cílené bezpečnostní audity prováděné kvalifikovaným nezávislým subjektem nebo příslušným orgánem (namísto pravidelného auditu - podle kompromisní novely Evropského parlamentu).*
+ ad hoc audity v případech odůvodněných závažným incidentem nebo nedodržením předpisů ze strany základního subjektu (namísto výše definovaného cíleného bezpečnostního auditu - podle kompromisního pozměňovacího návrhu Evropského parlamentu).	*+ doplnění kritéria nediskriminace do bezpečnostního skenu (podle kompromisního pozměňovacího návrhu Evropského parlamentu).*

Aby se zlepšilo prosazování pravidel obsažených ve směrnici, stanoví návrh směrnice NIS 2 **minimální seznam správních sankcí za** porušení povinností v oblasti řízení rizik kybernetické bezpečnosti a podávání zpráv. To by mělo poskytnout jasný a konzistentní rámec pro možné sankce v celé Evropské unii. Při **posuzování přiměřenosti donucovacích pravomocí a ukládání sankcí by měla být zohledněna zejména** povaha, závažnost[80] a doba trvání protiprávního jednání, skutečně způsobená škoda nebo vzniklé ztráty nebo potenciální škoda či ztráty, které mohly být vyvolány, úmyslná nebo nedbalostní povaha protiprávního jednání, opatření přijatá k zabránění nebo zmírnění vzniklé škody a/nebo ztrát, míra odpovědnosti nebo případná předchozí relevantní porušení, míra spolupráce s příslušným orgánem a jakékoli další přitěžující nebo polehčující okolnosti.[81] Uložení sankcí včetně správních pokut podléhá vhodným procesním zárukám v souladu s obecnými zásadami práva EU a Listinou základních práv Evropské unie, včetně účinné soudní ochrany a spravedlivého procesu.[82] Členské státy stanoví pravidla pro sankce za porušení vnitrostátních předpisů přijatých podle směrnice NIS 2 a přijmou veškerá opatření nezbytná k zajištění jejich provádění. Členské státy zároveň zajistí, aby ukládání pokut bylo v každém jednotlivém případě účinné, přiměřené a odrazující.[83]

Donucovací opatření, která mají být poskytnuta příslušným orgánům, jsou uvedena v následující tabulce. Stejně jako v případě režimů dohledu navrhuje obecný přístup Rady doplnit tato kritéria o to, že se použijí "alespoň" tato kritéria - tím se z nich stane demonstrativní částka, kterou mohou členské státy rozšířit.

Základní subjekty[84]	**Důležité subjekty[85]**
vydávat upozornění na nedodržování povinností stanovených ve směrnici ze strany subjektů.	vydávat upozornění na nedodržování povinností stanovených ve směrnici ze strany subjektů.
vydávat závazné pokyny (podle kompromisního pozměňovacího návrhu Evropského parlamentu také: *včetně*	vydat závazný pokyn nebo příkaz, kterým se těmto subjektům uloží povinnost odstranit

[80] Mezi **porušení, která by měla být považována za závažná,** patří: opakovaná porušení, neoznámení nebo nenapravení incidentů s významným rušivým účinkem, nenapravení nedostatků na základě závazných pokynů příslušných orgánů bránění auditům nebo monitorovacím činnostem nařízeným příslušným orgánem po zjištění porušení, poskytování nepravdivých nebo hrubě nepřesných informací v souvislosti s požadavky na řízení rizik nebo oznamovacími povinnostmi stanovenými v článcích 18 a 20 směrnice NIS 2.
[81] Viz čl. 29 odst. 7 návrhu směrnice NIS 2.
[82] Viz 71. bod odůvodnění návrhu směrnice NIS 2.
[83] Viz články 31 a 32 návrhu směrnice NIS 2.
[84] Viz čl. 29 odst. 4 návrhu směrnice NIS 2.
[85] Viz čl. 30 odst. 4 návrhu směrnice NIS 2.

opatření nezbytných k prevenci nebo nápravě události, jakož i lhůt pro provedení těchto opatření a pro podávání zpráv o jejich provádění) nebo příkaz, kterým se těmto subjektům ukládá, aby odstranily zjištěné nedostatky nebo porušení povinností stanovených ve směrnici.	zjištěné nedostatky nebo porušení povinností stanovených ve směrnici.
nařídit těmto subjektům, aby ukončily jednání, které není v souladu s povinnostmi stanovenými směrnicí, a aby se zdržely opakování tohoto jednání	nařídit těmto subjektům, aby ukončily jednání, které není v souladu s povinnostmi stanovenými směrnicí, a aby se zdržely opakování tohoto jednání
nařídit těmto subjektům, aby uvedly svá opatření k řízení rizik nebo oznamovací povinnosti do souladu s povinnostmi stanovenými směrnicí, a to stanoveným způsobem a ve stanovené lhůtě	nařídit těmto subjektům, aby uvedly svá opatření k řízení rizik nebo oznamovací povinnosti do souladu s povinnostmi stanovenými směrnicí, a to stanoveným způsobem a ve stanovené lhůtě
nařídit těmto subjektům, aby informovaly fyzické nebo právnické osoby, kterým poskytují služby nebo činnosti, jež jsou potenciálně ovlivněny významnou kybernetickou hrozbou, o všech možných ochranných nebo nápravných opatřeních, která mohou tyto fyzické nebo právnické osoby v reakci na tuto hrozbu přijmout.	nařídit těmto subjektům, aby informovaly fyzické nebo právnické osoby, kterým poskytují služby nebo činnosti, jež jsou potenciálně ovlivněny významnou kybernetickou hrozbou, o všech možných ochranných nebo nápravných opatřeních, která mohou tyto fyzické nebo právnické osoby v reakci na tuto hrozbu přijmout.
nařídit těmto subjektům, aby v přiměřené lhůtě provedly doporučení vyplývající z bezpečnostního auditu.	nařídit těmto subjektům, aby v přiměřené lhůtě provedly doporučení vyplývající z bezpečnostního auditu.
jmenovat kontrolního úředníka s přesně vymezenými úkoly, který bude po stanovenou dobu dohlížet na dodržování jejich povinností stanovených v článcích 18 a 20 směrnice *(podle obecného přístupu Rady se toto opatření ruší).*	-
nařídit těmto subjektům, aby určitým způsobem zveřejnily aspekty nedodržení povinností stanovených ve směrnici.	nařídit těmto subjektům, aby určitým způsobem zveřejnily aspekty nedodržení povinností stanovených ve směrnici.

učinit veřejné prohlášení, které identifikuje právnickou a fyzickou osobu (osoby) odpovědnou (odpovědné) za porušení povinnosti stanovené směrnicí a povahu tohoto porušení (*podle kompromisního pozměňovacího návrhu Evropského parlamentu a obecného přístupu Rady se toto opatření odstraní*).	učinit veřejné prohlášení, které identifikuje právnickou a fyzickou osobu (osoby) odpovědnou (odpovědné) za porušení povinnosti stanovené směrnicí a povahu tohoto porušení (*podle kompromisního pozměňovacího návrhu Evropského parlamentu a obecného přístupu Rady se toto opatření odstraní*).
uložit nebo požádat příslušné orgány nebo soudy o uložení správní pokuty v souladu s vnitrostátními právními předpisy, a to vedle výše uvedených opatření nebo místo nich, v závislosti na okolnostech každého jednotlivého případu.	uložit nebo požádat příslušné orgány nebo soudy o uložení správní pokuty v souladu s vnitrostátními právními předpisy, a to vedle výše uvedených opatření nebo místo nich, v závislosti na okolnostech každého jednotlivého případu.

Pokud výše uvedená donucovací opatření - vhodná pro základní subjekty - nejsou dostatečná, členské státy zajistí, aby příslušné orgány měly také **tyto pravomoci**:[86]

- pozastavit nebo požádat certifikační nebo autorizační orgán, aby pozastavil certifikaci nebo autorizaci týkající se části nebo všech služeb nebo činností poskytovaných základním subjektem;
- uložit nebo požádat příslušné orgány nebo soudy podle vnitrostátních právních předpisů o uložení dočasného zákazu výkonu řídících funkcí v tomto základním subjektu všem osobám vykonávajícím řídící funkce na úrovni výkonného ředitele nebo zákonného zástupce a všem dalším fyzickým osobám, které jsou odpovědné za porušení, vykonávat řídící funkce v tomto subjektu.

Tyto sankce se však uplatňují pouze do doby, než subjekt přijme nezbytná opatření k nápravě nedostatků nebo splní požadavky příslušného orgánu, pro které byly tyto sankce uplatněny. Kompromisní pozměňovací návrh Evropského parlamentu považuje zákaz vůči všem osobám vykonávajícím řídící funkce za prostředek ultima ratio a navrhuje, aby pozastavení certifikace bylo pouze dočasné. Podle obecného přístupu Rady se tyto sankce nevztahují na subjekty veřejné správy, na které se vztahuje směrnice NIS 2.

Pokud jde o **výši možných správních pokut za** porušení povinností stanovených ve směrnici NIS 2 (konkrétně článek 18 nebo článek 20), které mají být uloženy podle návrhu směrnice NIS 2,

[86] Viz čl. 29 odst. 5 návrhu směrnice NIS 2, kompromisní pozměňovací návrh Evropského parlamentu a obecný přístup Rady.

členské státy by měly zajistit, aby za porušení povinností byly ukládány správní pokuty v **maximální výši nejméně 10 000 000 EUR nebo až do výše 2 % celkového celosvětového ročního obratu** podniku, k němuž patří základní nebo významný subjekt, za předchozí účetní období, podle toho, která částka je vyšší.[87]

Rada v obecném přístupu navrhuje rozlišovat režim pokut zvlášť pro zásadní a důležité subjekty a navrhuje snížení maximálních částek:

- základními subjekty, správní pokuty v **maximální výši nejméně 4 000 000 EUR nebo v případě právnické osoby 2 % celkového celosvětového ročního obratu** (podle toho, která částka je vyšší);
- významnými subjekty, správní pokuty činí **maximálně 2 000 000 EUR nebo v případě právnické osoby 1 % celkového celosvětového ročního obratu** (podle toho, která částka je vyšší).

Obecný přístup Rady dospěl k závěru, že pokud právní systém členského státu nestanoví správní pokuty, členské státy zajistí, aby článek 31 směrnice NIS 2 mohl být uplatňován tak, že pokutu iniciuje příslušný orgán a ukládá příslušný vnitrostátní soud, přičemž zajistí, aby tyto opravné prostředky byly účinné a měly rovnocenný účinek jako správní pokuty ukládané příslušnými orgány. V každém případě musí být uložené pokuty účinné, přiměřené a odrazující.

VIII. Shrnutí hlavních problematických otázek návrhu směrnice NIS 2

Výše uvedené změny zavedené návrhem směrnice NIS 2 mohou v důsledku toho způsobit značné problémy a v některých případech i potenciální rozpor s právními zásadami.

1) Rozšíření působnosti dotčených subjektů podle návrhu směrnice NIS 2 a povinnosti těchto subjektů

Návrh směrnice NIS 2 představuje pro všechny právnické osoby spadající do oblasti působnosti směrnice NIS 2 velké zvýšení administrativní i finanční zátěže.

Skutečnost, že okruh subjektů, na které se má směrnice NIS 2 vztahovat, má být podstatně rozšířen, představuje především větší administrativní zátěž pro všechny subjekty. Rovněž rozšíření uplatňování kritérií pro posuzování rizik dodavatelů obsažených v souboru nástrojů EU

[87] Viz čl. 31 odst. 4 návrhu směrnice NIS 2.

na mnoho subjektů, které v současné době nespadají do oblasti působnosti směrnice NIS (nejsou považovány za provozovatele základních služeb nebo poskytovatele digitálních služeb), se jeví jako nadměrné vzhledem k jejich (ne)kritičnosti nebo nižšímu hospodářskému významu.

Návrh směrnice NIS 2 předpokládá, že její zavedení povede k následujícímu zvýšení nákladů povinných subjektů:[88]

- Orgány členských států (dopad na vnitrostátní rozpočty a správní orgány) - celkové **navýšení zdrojů o přibližně 20-30 %;**
- Subjekty (společnosti), které by spadaly do oblasti působnosti návrhu směrnice NIS 2 - zvýšení maximálně o **22 % jejich současných výdajů na bezpečnost ICT v** prvních letech po zavedení nového rámce NIS (12 % pro společnosti, které již spadají do oblasti působnosti stávající směrnice NIS).

Zvýšení nákladů pro členské státy má být kompenzováno lepším přehledem a interakcí s klíčovými podniky, posílenou přeshraniční operativní spoluprací, jakož i mechanismy vzájemné pomoci a vzájemného hodnocení (tj. celkovým zvýšením schopností v oblasti kybernetické bezpečnosti ve všech členských státech). Pro podniky vidí návrh směrnice NIS 2 výhodu v poměrném přínosu těchto investic díky snížení nákladů na kybernetické bezpečnostní incidenty (pravděpodobně až 118 miliard EUR za 10 let).

2) Možné porušení zákazu diskriminace a práva na rovné zacházení

Přímý odkaz na EU Toolbox[89] podporuje interpretaci hodnocení rizik dodavatelů a dodavatelského řetězce nejen na základě objektivních technických kritérií či norem nebo předchozích zkušeností s kybernetickými bezpečnostními incidenty, ale také na základě netechnických rozhodnutí. Ve spojení se souborem nástrojů EU Toolbox se místo objektivních kritérií používají subjektivní a vágní kritéria, která se účinně zaměřují na dodavatele ze zemí mimo EU. Potenciálně je tedy dáno riziko nepřímé diskriminace zahraničních dodavatelů na základě země jejich původu.

Neexistence přesných pokynů, které by bylo možné použít při posuzování rizik, může vést ke svévolným rozhodnutím dotčených subjektů (např. poskytovatelů elektronických komunikací) a členských států. Existuje riziko svévolných, diskriminačních a nekonzistentních rozhodnutí.

[88] Viz příloha 7 ROZHODNUTÍ KOMISE o vnitřních pravidlech pro plnění souhrnného rozpočtu Evropské unie (oddíl Evropská komise), která je určena útvarům Komise - LEGISLATIVNÍ FINANČNÍ VÝKAZ "AGENTURY", strana 18.
[89] Viz články 18 a 19 návrhu směrnice NIS 2 ve spojení s 46. a 47. bodem odůvodnění návrhu směrnice NIS 2).

3) Další potenciálně problematické aspekty v souvislosti se souborem nástrojů EU

Systém hodnocení rizik dodavatele podle EU Toolboxu může porušovat následující zásady vycházející z evropského i vnitrostátního práva:

- zásada volného pohybu zboží a služeb (články 34 a 56 Smlouvy o fungování Evropské unie);
- právo na vlastnictví (článek 17 *Listiny základních práv Evropské unie* ("*LZPS*") + článek 11 české Listiny základních práv a svobod ("*LZPS")*).
    - pokud je na základě kritérií podle EU Toolboxu zakázáno/nepovoleno použití určitého zařízení od dodavatelů mimo EU, může to vést k riziku nutnosti odstranění tohoto zařízení;
- právo (svoboda) podnikat (článek 16 CFR EU + článek 26 LZPS).
    - na základě hodnotících kritérií podle souboru nástrojů EU může být smluvní volnost subjektů omezena;
- zásada nediskriminace a právo na rovné zacházení (články 20-21 CFR EU + článek 3 LZPS);
- zásada technologické neutrality
    - existuje riziko diskriminace mezi technologiemi s rovnocenným účinkem.

4) Možný rozpor se zásadou proporcionality

Není jasné, zda změna předložená návrhem směrnice NIS 2 splňuje test proporcionality, podle kterého musí být prostředky použity ve vztahu ke sledovanému cíli:

a) vhodné (umožňuje institut dosáhnout stanoveného cíle?);

b) nezbytné (lze cíle dosáhnout jinými opatřeními, která umožňují dosáhnout stejného cíle, ale která se nedotýkají základních práv a svobod?);

c) přiměřené (měření základních práv).

Navrhovaná opatření jsou pravděpodobně nepřiměřená, neboť zavádějí nový regulační rámec pro řízení a posuzování rizik dodavatelů, který se potenciálně vztahuje na veškerou infrastrukturu IKT a elektronických komunikací, včetně např. pevných sítí, aniž by konkrétně zohledňovala fungování a relativní význam jednotlivých typů dotčených subjektů.

IX. Dopad směrnice NIS 2 na českou legislativu, zejména s ohledem na koncept kritické informační infrastruktury

V současné době není zcela jasná konkrétní podoba transpozice směrnice NIS 2 do českého právního řádu (i vzhledem k tomu, že dosud nebylo dáno její konečné znění). Je však zřejmé, že **se** zcela jistě **promítne do českého zákona č. 181/2014 Sb. o kybernetické bezpečnosti** (dále jen "*ZKB*"), stejně jako v současnosti platná a účinná směrnice NIS.

Na tomto místě lze s největší pravděpodobností konstatovat, že okruh subjektů, na které se bude směrnice NIS 2 vztahovat, bude podstatně širší než v současnosti platná a účinná směrnice NIS, která byla transponována zejména do ZKB.

Návrh směrnice NIS 2 předpokládá, že do oblasti působnosti směrnice budou zahrnuty všechny střední a velké společnosti ve vybraných odvětvích nebo poskytující služby (které jsou uvedeny v přílohách I a II návrhu směrnice NIS 2). Subjekty mají být klasifikovány podle odvětví, v němž působí (nebo podle druhu služeb, které poskytují), a na tomto základě rozděleny do dvou kategorií - základní a významné, přičemž všechny kategorie základních subjektů budou podle v současnosti platné a účinné směrnice NIS.

Pokud jde o kategorii tzv. **kritických subjektů -** směrnice NIS 2 se o těchto subjektech výslovně zmiňuje pouze okrajově, s odkazem na návrh směrnice CER, který zavádí zvláštní úpravu pro tyto subjekty a úzce souvisí s návrhem směrnice NIS 2 a doplňuje jej. Rozsah kritických subjektů uvedený v návrhu směrnice CER je v zásadě totožný se seznamem zásadních subjektů podle návrhu směrnice NIS 2 (viz příloha I návrhu směrnice NIS 2). V této souvislosti je však třeba poznamenat, že samotný návrh směrnice CER ve 14. bodě odůvodnění uvádí, že:

"*Subjekty spadající do **odvětví digitální infrastruktury jsou v podstatě založeny na síťových a informačních systémech a spadají do oblasti působnosti směrnice NIS 2, která se zabývá fyzickou bezpečností těchto systémů v rámci jejich povinností v oblasti řízení rizik kybernetické bezpečnosti a podávání zpráv**. Vzhledem k tomu, že se na tyto záležitosti vztahuje směrnice NIS 2, povinnosti stanovené touto směrnicí se na tyto subjekty nevztahují. Vzhledem k významu služeb poskytovaných subjekty v odvětví digitální infrastruktury pro poskytování jiných základních služeb by však členské státy měly na základě kritérií a za použití postupu stanoveného v této směrnici obdobně určit subjekty týkající se odvětví digitální infrastruktury, které by měly být považovány za rovnocenné kritickým subjektům pouze pro účely kapitoly II, včetně ustanovení o podpoře členských států při zvyšování odolnosti těchto subjektů*."

Právě výrazný nárůst počtu subjektů, na které se návrh směrnice NIS 2 vztahuje, a zejména zavedení kritéria velikosti podniku, podle něhož do jeho působnosti spadají všechny střední a velké subjekty působící v odvětvích nebo službách, na které se návrh směrnice NIS 2 vztahuje, byly od počátku hlavním důvodem k obavám členských států a dalších příslušných subjektů. Z tohoto důvodu Rada předložila kompromisní návrh dále rozpracovaný ve svém obecném přístupu k návrhu směrnice NIS 2, který sice toto pravidlo zachovává, ale obsahuje dodatečná ustanovení k zajištění proporcionality, vyšší úrovně řízení rizik a jasnějších pravidel pro posuzování kritičnosti při určování subjektů spadajících do oblasti působnosti směrnice NIS 2. Evropský parlament rovněž vydal předběžné znění svých pozměňovacích návrhů k návrhu[90] směrnice NIS 2, které však rozsah povinných subjektů nijak zásadně nesnižuje (spíše naopak - navrhuje zahrnout i akademické, znalostní a výzkumné instituce).

Obecný přístup Rady doplňuje další kategorii základních služeb (bod 8a - řízení služeb ICT). Poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací uvedení v bodě 8 přílohy I v každém případě spadají do oblasti působnosti směrnice NIS 2, ale měli by být rozděleni do dvou kategorií podle velikosti - střední a velcí poskytovatelé by měli spadat do kategorie základních subjektů, zatímco malí poskytovatelé a mikroposkytovatelé do kategorie významných subjektů. Obecně by subjekty uvedené v příloze I návrhu směrnice NIS 2, které jsou větší než střední subjekty, měly spadat do kategorie základních subjektů a střední subjekty uvedené v příloze I by měly být zařazeny mezi významné subjekty ve smyslu návrhu směrnice NIS 2.

V této souvislosti je třeba zmínit 14a. bod odůvodnění obecného přístupu Rady:

"*Subjekty patřící do odvětví digitální infrastruktury jsou v podstatě založeny na síťových a informačních systémech, a proto by se povinnosti uložené těmto subjektům touto směrnicí měly komplexně zabývat fyzickou bezpečností těchto systémů v rámci jejich povinností v oblasti řízení rizik kybernetické bezpečnosti a podávání zpráv. Vzhledem k tomu, že se na tyto záležitosti vztahuje tato směrnice, povinnosti stanovené v kapitolách III až VI směrnice (EU) XXX/XXX [CER] se na tyto subjekty nevztahují.* "

Z výše uvedeného je zřejmé, že směrnice NIS 2 bude mít na ZKB významný dopad - okruh povinných subjektů se jednoznačně rozšíří, otázkou však je, do jaké míry a zda a jakým způsobem směrnice NIS 2 ovlivní definici kritické informační infrastruktury ve smyslu ZBK. Lze předpokládat, že výše uvedené kategorie (základní a významné) se promítnou do rozšíření § 2 písm. i) ZKB a doplnění dalšího pojmu "významné služby" v tomto ustanovení § 2 a následně do povinností

[90] Viz https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2021/10-28/NIS2_COMPROMISE_amendment_EN.pdf.

stanovených v ZKB. Samotná definice kritické informační infrastruktury nemusí být nutně dotčena směrnicí NIS 2, ale je pravděpodobné, že bude dotčena směrnicí CER.

X. Závěr

Z návrhu směrnice NIS 2 je zřejmé, že hlavní snahou Evropské komise (resp. také Evropského parlamentu a Rady) je výrazně zlepšit kybernetickou bezpečnost v Evropské unii a sjednotit ji napříč EU, neboť v současné době existují mezi členskými státy značné rozdíly v přístupu k této problematice.

Jak vyplývá z přístupu všech zúčastněných orgánů EU, jsou toho názoru, že incidenty a krize v oblasti kybernetické bezpečnosti (zejména velkého rozsahu) na úrovni EU vyžadují koordinovaný postup, aby byla zajištěna bezodkladná a účinná reakce, a to z důvodu vysoké míry vzájemné závislosti mezi odvětvími a zeměmi. Není pochyb o tom, že dostupnost kyberneticky odolných sítí a informačních systémů a dostupnost, důvěrnost a integrita dat jsou pro bezpečnost EU zásadní jak uvnitř, tak i za jejími hranicemi, neboť kybernetické hrozby mohou pocházet i z oblastí mimo EU (jak opět zdůrazňuje kompromisní pozměňovací návrh Evropského parlamentu).

Návrh směrnice NIS 2 však vyvolává mnoho sporných otázek. Zejména je otázkou, zda je návrh směrnice NIS 2 schopen projít testem proporcionality vzhledem k podstatnému rozšíření působnosti subjektů, na které se má směrnice NIS 2 vztahovat. Zdá se, že ve své současné podobě se směrnice NIS 2 dotýká široké škály subjektů, jejichž nedostatečný společenský, kritický nebo hospodářský význam nenaznačuje, že by měly být zatíženy dodatečnými požadavky, které na ně návrh směrnice NIS 2 klade.

Vyvstává také otázka výslovného zakotvení požadavku na posuzování netechnických kritérií při hodnocení rizik dodavatelů, když zejména z kompromisního pozměňovacího návrhu Evropského parlamentu je zřejmé, že toto opatření je zaměřeno na konkrétní země mimo Evropskou unii. A zde se situace dostává mimo jiné do potenciálního rozporu se zásadou nediskriminace, zásadou volného pohybu zboží a služeb i svobodou podnikání.