9. 12. 2022

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

NIS2: Nová regulace kybernetické bezpečnosti v EU

Směrnice NIS2 nově přijatá Evropským parlamentem a Radou rozšiřuje okruh povinných osob v oblasti kybernetické bezpečnosti, zpřísňuje požadavky na hlášení bezpečnostních incidentů, zavádí odpovědnost managementu a zvyšuje sankce za nedodržení povinností.

Nové technologie a hrozby, rostoucí počet a rozsah kybernetických útoků, pandemie COVID-19, která zrychlila digitální transformaci, a závislost kritických sektorů na digitálních technologiích – to vše jsou důvody, proč byla na evropské úrovni přijata nová, přísnější regulace kybernetické bezpečnosti v podobě směrnice NIS2. Směrnice si klade za cíl harmonizovat požadavky na kybernetickou bezpečnost v rámci celé EU, zlepšit kybernetickou odolnost EU a schopnost koordinované reakce na kybernetické incidenty napříč EU.

Kybernetická bezpečnost je na evropské úrovni v současnosti regulována směrnicí 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 („**NIS**“). V Česku právní úpravu obsahuje zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů („**ZKB**“), který tuto směrnice transponuje.

Dne 28. 11. 2022 schválila Rada Evropské unie návrh nové směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii („**NIS2**“). Ta ruší stávající směrnici NIS a vyvolá také nutnost novely českého ZKB. NIS2 zejména rozšiřuje okruh povinných osob v oblasti kybernetické bezpečnosti, zpřísňuje požadavky na hlášení bezpečnostních incidentů, zavádí odpovědnost managementu a zvyšuje sankce za nedodržení povinností.

Regulovaná odvětví, základní a důležité subjekty

Z pohledu povinných osob v soukromém i veřejném sektoru NIS2 rozšiřuje okruh regulovaných odvětví, a to nejen oproti původní směrnici NIS, ale také oproti domácí právní úpravě v podobě ZKB. Nově bude mít právní úprava dopad na poskytovatele IT služeb, výrobní podniky, poštovní a kurýrní služby nebo organizace působící v oblasti výzkumu. V odvětvích, na která už stávající právní úprava dopadá, pak dojde k rozšíření okruhu povinných osob – například v energetice budou nově regulováni obchodníci s plynem a elektřinou. Odvětví i povinné subjekty v rámci těchto odvětví jsou uvedeny v přílohách I a II směrnice. Podle odhadů NÚKIB bude v ČR podle NIS2 minimálně 6 000 povinných osob ve srovnání se stávajícími cca 400 povinnými osobami dle ZKB.[1]

NIS2 také zavádí novou terminologii. Namísto stávajícího rozdělení povinných osob nově rozlišuje základní (*essential*) a důležité (*important*) subjekty, pro které zavádí dva odlišné režimy. Ačkoliv základní povinnosti dle NIS2 jako zavádění bezpečnostních opatření a hlášení bezpečnostních incidentů budou dopadat na obě kategorie povinných osob, konkrétní požadavky, dohled nad jejich dodržováním a sankce budou ve vztahu k základním subjektům přísnější.

Povinnými osobami dle směrnice budou až na výjimky pouze organizace dosahující alespoň velikosti

středního podniku ve smyslu doporučení Evropské komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků, tedy s minimálně 50 zaměstnanci a 10 miliony eur obratu (alternativně k minimálnímu obratu postačí naplnit kritérium 10 milionů eur bilanční sumy).

Základní subjekty (s přísnějšími povinnostmi) jsou vymezeny zejména v příloze I směrnice, kdy u těchto se uplatní výše zmíněné kritérium velikosti podniku. Budou mezi ně spadat například subjekty v odvětví dopravy, zdravotnictví, digitální infrastruktury, veřejné správy či v již zmiňovaných odvětvích energetiky a IT služeb. V IT se konkrétně bude vztahovat zejména na poskytovatele řízených služeb (*managed service providers*), tedy subjekty poskytující služby související s instalací, správou, provozem nebo údržbou produktů ICT. Nad rámec přílohy I pak budou do této kategorie spadat zejména poskytovatelé veřejných služeb elektronických komunikací a bez ohledu na velikost podniku také kvalifikovaní poskytovatelé služeb vytvářejících důvěru, ústřední orgány státní správy, kritické subjekty dle připravované směrnice CER[2] (obdoba subjektů kritické infrastruktury dle českého práva)[3] nebo aktuálně určení poskytovatelé základních služeb.

Důležité subjekty (s mírnějšími povinnostmi) jsou vymezeny v příloze II směrnice (definičně se jedná o všechny subjekty v příloze I a II, které nejsou základními subjekty). Mezi ně budou spadat povinné osoby například v odvětvích poštovních a kurýrních služeb, nakládání s odpady, chemického, potravinářského a vybraných oblastí zpracovatelského průmyslu. Členské státy mohou dle svého hodnocení rizik do obou kategorií zařadit další subjekty.

Při určení, zda je subjekt středním nebo větším podnikem, přitom hraje roli i začlenění do koncernu. Čl. 6 odst. 2 Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků stanoví, že pro naplnění definice středního podniku se započítají i údaje partnerských a přidružených podniků. Recitál č. 16 NIS2 však umožňuje členským státům uplatnit korekci v podobě zohlednění míry nezávislosti podniku v rámci skupiny, zejména z hlediska nezávislosti užívaných informačních systémů nebo poskytovaných služeb.

Z působnosti směrnice jsou vyloučeny orgány veřejné správy v oblasti národní a veřejné bezpečnosti, obrany, vymáhání práva (zejm. vyšetřování trestných činů), soudní moc, parlamenty a národní banky – tyto subjekty však mohou být zahrnuty, resp. zůstat v působnosti národní právní úpravy. Nedomníváme se přitom, že v souvislosti s implementací směrnice do českého práva by některé stávající povinné osoby byly zcela vyňaty z působnosti ZKB.

Podle platné právní úpravy v ZKB správce informačních a komunikačních systémů kritické informační infrastruktury a provozovatele základních služeb dle platné právní úpravy určuje v závislosti na odvětví a dopadových kritériích[4] opatřením obecné povahy, resp. rozhodnutím Národní úřad pro kybernetickou a informační bezpečnost („NÚKIB“).[5] Pod působnost nové právní úpravy budou povinné osoby spadat automaticky naplněním výše uvedených kritérií, aniž by NÚKIB vydával rozhodnutí nebo jiný správní akt. Na základě tohoto sebeurčení pak bude každá povinná osoba mít povinnost oznámit NÚKIB, případně národnímu CERT, své identifikační a kontaktní údaje a důvody, proč do působnosti spadá.[6]

Změny v povinnostech a odpovědnost managementu

Pro stávající povinné osoby podle ZKB směrnice NIS2 nepřináší zásadní změny v okruhu jejich povinností, pouze jejich zpřesnění a doplnění. Zůstává zachována povinnost přijmout bezpečnostní opatření, a to na základě analýzy rizik.[7] NIS2 přináší oproti předchozí evropské úpravě konkrétní výčet minimálního rozsahu opatření, v poměru k české právní úpravě v ZKB a vyhlášce[8] je však míra podrobnosti nižší, a v této oblasti tak neočekáváme významné změny pro stávající povinné osoby.

Oproti současné české právní úpravě je novinkou možnost Evropské komise přijímat prováděcí akty, které stanoví konkrétní bezpečnostní opatření – dosud je stanovovaly pouze členské státy.[9] Přibývá také oprávnění Evropské komise a členských států požadovat, aby povinné osoby užívaly v konkrétní oblasti pouze produkty, služby či procesy informačních či komunikačních technologií vypracované touto osobou nebo certifikované dle evropských systémů certifikace kybernetické bezpečnosti.[10]

Změní se také pravidla pro oznamování kybernetických bezpečnostních incidentů. ZKB požaduje jejich ohlášení NÚKIB, resp. národnímu CERT „bezodkladně“,[11] NIS2 stanoví pro ohlášení konkrétní lhůty. Povinné osoby budou muset po zjištění významného incidentu[12] nejpozději do 24 hodin podat tzv. včasné varování, do 72 hodin prvotní posouzení incidentu včetně závažnosti a dopadu a do 1 měsíce závěrečnou zprávu obsahující podrobný popis incidentu a další informace jako například pravděpodobnou příčinu incidentu nebo přijatá opatření ke zmírnění následků.[13] Přibývá také povinnost o kybernetickém bezpečnostním incidentu ve vhodném případě informovat i příjemce služby, která je v působnosti NIS2. Tato povinnost se týká incidentů, které by mohly negativně ovlivnit poskytování služeb.[14]

Nově pak NIS2 stanoví, že řídící orgány povinných osob pak jednotlivá opatření schvalují a dohlíží nad jejich uplatňováním, přičemž za porušení této povinnosti mohou být odpovědné.[15] S tím souvisí nová povinnost řídících orgánů absolvovat školení a tato poskytovat i svým zaměstnancům.

Dohled a sankce

NIS2 stanoví v oblasti dohledu nad dodržováním povinností dohledovým orgánům rozsáhlá oprávnění, ta se však významně neliší od stávání kompetencí NÚKIB dle kontrolního řádu[16] a ZKB. Nově směrnice požaduje, aby měl dohledový orgán oprávnění po uplynutí lhůty určené k nápravě nedostatků či splnění jiných požadavků dohledového orgánu uložit do doby splnění povinností dočasný zákaz výkonu řídicích funkcí jakékoliv vedoucí fyzické osobě,[17] případně dočasné pozastavení certifikace nebo povolení ve vztahu ke službám poskytovaným subjektem.[18]

Ke změnám dochází, i co se týče sankcí za porušení povinností, kdy zatímco dle současně platné právní úpravy lze za nesplnění povinností v oblasti kybernetické bezpečnosti uložit pokutu v maximální výši 5 milionů Kč, nově bude za porušení povinnosti zavádět bezpečnostní opatření nebo oznamovat incidenty možné uložit důležitým subjektům pokutu až 7 milionů EUR (cca 170 milionů Kč) nebo 1,4 % celosvětového ročního obratu (dle toho, která částka je vyšší) a základním subjektům až 10 milionů EUR (cca 240 milionů Kč) nebo 2 % obratu.[19] Pokuty lze ukládat vedle dalších opatření a NIS2 taktéž umožňuje uložení opakovaných penále až do okamžiku splnění příslušné povinnosti.[20] Sankce ovšem budou muset být účinné, přiměřené a odrazující.[21]

Sektorové regulace a transpozice v ČR

Směrnice NIS2 se neuplatní v případě, kdy existuje sektorová úprava, která stanoví regulovanému subjektu povinnosti ve vztahu k řízení rizik a oznamovací povinnosti alespoň v takovém rozsahu jako směrnice NIS2.[22] Takovou sektorovou regulací je především připravované nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru („**DORA**“),[23] které stanoví jednotné požadavky na bezpečnost sítí a systémů ve finančním sektoru a kritické technologie třetích stran. DORA se bude vztahovat např. na banky, pojišťovny nebo investiční společnosti.

Vydání směrnice NIS2 v úředním věstníku lze očekávat ještě v roce 2022. S ohledem na transpoziční lhůtu 21 měsíců tak lze očekávat účinnost změn v domácí právní úpravě od 1. 7. 2024. Návrh domácí právní úpravy by přitom měl být zveřejněn v lednu 2023. V rámci této domácí právní úpravy by mělo dojít k zjednodušení struktury ZKB.

Stávající samostatně definované povinné osoby budou pravděpodobně nahrazeny pojmem „poskytovatel regulované služby“ jako jediná povinná osoba. Ve vztahu k základním subjektům bude zaveden režim vyšších povinností, v rámci kterých budou povinné osoby povinny podléhat stávající vyhlášce o kybernetické bezpečnosti (v novelizované podobě) a oznamovat veškeré kybernetické bezpečnostní incidenty. Ve vztahu k důležitým subjektům bude zaveden režim nižších povinností, v rámci kterých budou povinné osoby povinny zavádět bezpečnostní opatření v minimálním rozsahu vyžadovaném NIS2 a oznamovat pouze významné kybernetické bezpečnostní incidenty (na základě posouzení přímo povinnou osobou). Bezpečnostní opatření by měl pro režim nižších povinností stanovit nový, samostatný prováděcí právní předpis,[24] který by měl obsahově vycházet z Minimálního bezpečnostního standardu publikovaného NÚKIB.[25]

Závěr

Směrnice NIS2 přináší podstatné rozšíření okruhu povinných subjektů v oblasti kybernetické bezpečnosti. Stávající povinnosti rozšiřuje a zpřísňuje sankce za jejich nedodržení. Ačkoliv tedy česká právní úprava již obsahuje rozsáhlou úpravu kybernetické bezpečnosti nad rámec požadavků předchozí směrnice NIS, transpozice nové směrnice NIS2 přinese změny jak pro nové povinné osoby, které dosud regulované nebyly, tak pro osoby již spadající do působnosti ZKB.

JUDr. Josef Donát, LL.M
Partner

Mgr. et Mgr. Ing. Jan Tomíšek
Advokát / Partner

Mgr. Michal Jeníček
Advokátní koncipient

ROWAN LEGAL, advokátní kancelář s.r.o.

GEMINI Center
Na Pankráci 1683/127

140 00 Praha 4

Tel.: +420 224 216 212
Fax: +420 224 215 823
e-mail: praha@rowan.legal

---

[1] Přednáška Martina Švédy na konferenci CyberCon 2022 „Směrnice NIS2 a hlavní plány její transpozice v ČR“, viz >>> zde.

[2] Návrh směrnice Evropského parlamentu a Rady o posílení odolnosti kritických subjektů, COM/2020/829 final, viz >>> zde.

[3] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

[4] Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

[5] Viz § 22 písm. n) a § 22a ZKB.

[6] Viz čl. 3 odst. 4 NIS2.

[7] Viz čl. 21 NIS2.

[8] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.

[9] Viz čl. 21 odst. 5.

[10] Viz čl. 24 NIS2.

[11] Viz § 8 odst. 1 ZKB.

[12] Tedy takového incidentu, který povinnému subjektu způsobil nebo může způsobit závažné provozní narušení služeb nebo finanční ztráty, příp. jiným fyzickým nebo právnickým osobám způsobil nebo může způsobit značnou hmotnou nebo nehmotnou újmu, viz čl. 23 odst. 3 NIS2.

[13] Povinné osoby budou taktéž povinny na žádost předložit průběžnou zprávu s aktualizací daného stavu.

[14] Viz čl. 23 odst. 1 NIS2.

[15] Viz čl. 20 odst. 1 NIS2.

[16] Viz § 23 odst. 2 ZKB a zákon č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů.

[17] NIS2 stanoví oprávnění uložit dočasný zákaz výkonu řídicích funkcí ve vztahu k fyzické osobě, která má odpovědnost za výkon řídicích funkcí na úrovni výkonného ředitele nebo zákonného zástupce v daném subjektu.

[18] Viz čl. 32 odst. 5 NIS2.

[19] Viz čl. 34 odst. 4 a 5 NIS2. Směrnice stanoví tyto horní hranice pokut jako minimální, tedy členské státy mohou mít tuto hranici vyšší.

[20] Viz čl. 34 odst. 6 NIS2.

[21] Viz čl. 32 odst. 1 a čl. 34 odst. 1 NIS2.

[22] Viz čl. 4 odst. 1 a 2 NIS2.

[23] Viz recitál č. 28 NIS2 a návrh nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru, COM/2020/595 final, viz >>> zde.

[24] Přednáška Martina Švédy na konferenci CyberCon 2022 „Směrnice NIS2 a hlavní plány její transpozice v ČR“, viz >>>zde.

[25] Minimální bezpečnostní standard NÚKIB, viz >>> zde.

Další články:

- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory
- Jak fungují plánovací smlouvy v reálných situacích (2. díl)
- Nejvyšší soud a forma smlouvy o smlouvě budoucí: krok zpět v ochraně právní jistoty?
- „Za každou kauzou je živý příběh“
- Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi
- Spoluvlastnictví a správa společné věci
- Doručování soudních písemností ze zahraničí do ČR