19. 9. 2024

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

Stav regulace kybernetické bezpečnosti v České republice ve světle probíhající transpozice NIS 2 - 1. část

V úvodním článku této série jsme představili Směrnici NIS2[1]a její zásadní dopady na evropskou regulaci v oblasti kybernetické bezpečnosti, a rovněž uvedli nový český implementační zákon o kybernetické bezpečnosti (dále jen "Zákon")[2]. V tomto článku již přistupujeme ke specifickým pravidlům Zákona – konkrétně představíme, jak Zákon přistupuje k určení základních a důležitých subjektů, na které mají dopadat povinnosti k zajištění vysoké úrovně kybernetické bezpečnosti podle NIS2 (poskytovatelé regulované služby podle dikce Zákona), a jak mají takové subjekty postupovat pro vyhodnocení dopadu Zákona na jejich služby.

Regulovaná služba, režimy povinností, registrace povinného subjektu

Pojem regulovaná služba

Zákon dopadá na osoby, které jsou usazeny v České republice, tedy především zde musí fakticky vykonávat činnosti prostřednictvím tzv. stálých struktur.[3] Tyto osoby musí posoudit, zda poskytují regulovanou službu podle Zákona, přičemž o určení, zda se jedná o regulovanou službu a o její registraci rozhoduje Úřad. Ten tak rozhodne na základě oznámení daného subjektu, nebo v některých případech z moci úřední.

Základní podmínky pro určení regulované služby, **jejichž naplnění by měl každý subjekt posoudit sám**, jsou naplněny pokud:

a. se jedná o službu, která je významná pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v České republice v rámci konkrétních odvětví (mj. energetika, výrobní a potravinářský průmysl, zdravotnictví, digitální infrastruktura, doprava či finanční trhy); a zároveň

b. poskytovatel této služby spadá pod definici středního nebo velkého podniku[4], případně se jedná o poskytovatele významného pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v České republice.

Konkrétní seznam služeb a vymezení podmínek významnosti poskytovatele stanoví Úřad vyhláškou, přičemž její rozsah (vzhledem k počtu služeb a odvětví) jde významně nad rozsah internetového článku.

Vyjma výše uvedeného *standardního* režimu, který se uplatní zejména u procese sebeidentifikace Zákon rovněž v souladu se směrnicí NIS2 vymezuje okruh dalších *alternativních* kritérií, podle kterých jde určit regulovanou službu.

Bez splnění podmínek velikosti podniku podle bodu b) Zákon dopadá **alternativně** též na subjekty, u nichž tak **rozhodne Úřad z moci úřední** z důvodu jejich **důležitosti pro celou společnost nebo**

určité odvětví, přičemž tak bude zkoumat v rámci správního řízení – například pokud se jedná o jediného poskytovatele služby zásadní pro zabezpečení důležitých společenských nebo ekonomických činností v České republice, či by mohlo mít narušení této služby významný dopad na bezpečnost České republiky, vnitřní pořádek nebo život a zdraví.

U některých služeb Zákon dokonce **nevyžaduje naplnění bodů a) ani b)**. Zákon, respektive jeho důvodová zpráva přitom předpokládá, že ani sami dotčené subjekty přitom nemusí mít nezbytné informace, zda příslušné parametry naplňují, a tak i zde bude **Úřad rozhodovat z moci úřední**. Do této kategorie budou spadat služby:

a. jejíž narušení může způsobit závažný zásah do života více než 125 000 osob, a to prostřednictvím ohrožení bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkové hodnoty nebo životního prostředí; a

b. jejíž narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu poskytovatele v režimu vyšších povinností.

Kritéria pro určení režimu povinností

Zákon dále v souladu se směrnicí NIS2 stanoví tzv. **režim poskytovatele regulované služby**, a to režim **vyšších** a režim **nižších povinností**. Jazykem směrnice se pak v případě vyššího režimu povinností jedná o základní subjekty (*essential entities*), u režimu nižších povinností pak o subjekty důležité (*important entities*). Poskytovatelé regulované služby budou do těchto režimů spadat mj. na základě své velikosti, druhu regulované služby, počtu uživatelů, rizikovosti provozu či jiných kritérií podle prováděcí vyhlášky.

Obecně lze říci, že do režimu vyšších povinností spadají takové subjekty, které jsou poskytovateli služeb v rámci tzv. vysoce kritických odvětví a současně jsou velkými podniky. Ve zbytku se pak uplatní režim povinností nižších. Mezi zmíněná vysoce kritická odvětví patří zejména energetika, doprava, bankovnictví a infrastruktura finančních trhů, zdravotnictví či digitální infrastruktura. Do režimu vyšších povinností budou rovněž spadat ty subjekty, které splní výše uvedené alternativní podmínky pro registraci regulované služby, a které budou registrovány na základě rozhodnutí Úřadu *ex-offo*.

Příslušný režim má samozřejmě poměrně zásadní dopad na povinnosti daného subjektu, kdy v případě režimu vyššího je těchto povinností přirozeně více, a nároky na řízení kybernetické bezpečnosti jsou obecně o něco vyšší. Mezi základní aspekty, které odlišují režim vyšších povinností od režimu povinností nižších, patří:

a. rozdělení povinných opatření na organizační a technická (v případě nižšího režimu se aplikuje jen jedna obecná kategorie opatření);

b. rozdělení funkcí významných pro řízení kybernetické bezpečnosti (v případě nižšího režimu stačí určení pouze jedné odpovědné osoby); a

c. provádění auditu kybernetické bezpečnosti.

Registrace u Úřadu

Subjekty, které výše zmíněné regulované služby poskytují, je budou muset sami identifikovat podle naplnění kritérií uvedených výše (tzv. sebeidentifikace) a **do 60 dnů ode dne, kdy ke splnění**

podmínek došlo, ohlásit Úřadu. V tomto směru se pak jedná o dvoufázový proces – nejdříve subjekt po provedené sebeidentifikaci regulovanou službu ohlásí Úřadu, posléze pak Úřad provede registraci této služby.

Pokud dojde k registraci ohlášené regulované služby, bude mít příslušný subjekt **30 dnů ode dne doručení rozhodnutí o registraci regulované služby** na to, aby Úřadu poskytl další nezbytné údaje, konkrétně (i) kontaktní údaje (údaje o fyzické osobě oprávněné jednat za poskytovatele regulované služby) a (ii) doplňující údaje, mezi které patří mj. doménová jména, čísla autonomních systémů (ASN) a rozsahy IP adres, které jsou využívány k poskytování regulované služby.

Samotné ohlášení regulované služby a hlášení výše zmíněných údajů bude probíhat prostřednictvím formulářů vypracovaných a zveřejněných ze strany Úřadu. Pro obdobné účely budou rovněž dostupné i další formuláře, mj. pro hlášení jakýchkoliv změn regulovaných služeb či pro žádost o zrušení registrace.

Závěrem

Vzhledem k povinnosti sebeidentifikace je na místě, aby subjekty pravidelně evaluovaly rozsah jimi poskytovaných služeb a kritéria určení velikosti jejich podniku, neboť s neoznámením regulované služby Úřadu Zákon spojuje nejpřísnější sankce, které podle aktuálního znění mohou dosahovat až do výše 250 000 000 Kč, nebo 2 % čistého celosvětového obratu. Registrace regulované služby je přitom prvním krokem pro určení dalších specifických povinností, které bude muset subjekt dodržovat, a které si blíže představíme v dalších článcích této série.

Sebastian Špeta

Martin Svoboda

schönherr
ADVOKÁTNÍ KANCELÁŘ

Schönherr Rechtsanwälte GmbH, organizační složka
Jindřišská 937/16
110 00 Praha 1

Tel.: +420 225 996 500
Fax: +420 225 996 555
e-mail: se.speta@schoenherr.eu
e-mail: ma.svoboda@schoenherr.eu

[1] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii.

[2] Ke dni publikace tohoto článku byl návrh zákona připravený Národním úřadem pro kybernetickou a informační bezpečnost (dále jen "Úřad") schválen Vládou k předložení do Poslanecké sněmovny Parlamentu České republiky.

[3] Pokud se nejedná o osoby, které na území České republiky zajišťují sítě nebo poskytují služby elektronických komunikací, na které se Zákon vztahuje bez ohledu na usazení vždy.

[4] Pro určení, zdali se jedná o velký či střední podnik, se uplatní doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků. Zákon současně vymezuje určité výjimky z tohoto pravidla, dle kterých se vybraná ustanovení tohoto doporučení neuplatní a/nebo se uplatní v odchylné podobě. Pro úplnost uvádíme, že v obecné rovině se bude regulace v souladu s definicí středních a velkých podniků týkat podniků, které zaměstnávají 50 a více zaměstnanců a dosahují ročního obratu (či bilanční sumy roční rozvahy) min. 10 milionů EUR.

Další články:

- Novelizace nařízení EU o odlesňování (EUDR)
- Zneužití práva na přístup podle GDPR
- Doručování soudních písemností ze zahraničí do ČR
- Novinky z české a evropské regulace finančních institucí za měsíc únor 2026
- Digital Fairness Act a influencer marketing – cesta ke konci roztříštěnosti regulace?
- Novinky z české a evropské regulace finančních institucí za měsíc leden 2026
- IATA Travel & Cargo akreditace v letectví – v čem spočívají její výhody?
- Digital Omnibus o AI: návrh nařízení o zjednodušení pravidel pro umělou inteligenci
- Rozhodčí nálezy vydané ruskými rozhodčími soudy a jejich uznání a výkon na území EU
- Environmentální tvrzení společností v hledáčku EU: Jak se vyhnout greenwashingu a obstát v nové regulaci?
- AIFMD II v České republice: Schvalovací proces a co čeká investiční společnosti