20. 8. 2025

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

Koncernové řízení kybernetické bezpečnosti – I. část

Zákon o kybernetické bezpečnosti (dále jen „ZKB“), který nijak nezohledňuje koncernové řízení kybernetické bezpečnosti přináší pro poskytovatele regulované služby nejen celou řadu novinek, ale i palčivé problémy, které zpravidla vyplývají až z praxe. Může se jednat např. o problematické zabezpečování kybernetické bezpečnosti pro společnosti v odlišném režimu plnění povinností (vyšší nebo nižší režim), hořký střet s realitou při zavádění bezpečnostních požadavků do smluv s neochotnými dodavateli, nebo i o formalistický přístup NÚKIBU spojený s hlášením kybernetických bezpečnostních incidentů. V článku se čtenář dozví, jak by měl postupovat při řešení těchto problematických situací.

Koncernové řízení společností v odlišném režimu povinností

ZKB počítá s tím, že společnosti mohou být zařazeny do dvou režimů plnění povinností, a to vyššího a nižšího režimu, kdy společnosti samotné nemohou bez dalšího změnit samovolně svůj režim povinností. Oba režimy mají svá specifika (zejména odlišné místo hlášení incidentů a mírně odlišné bezpečnostní požadavky). Koncernu, který je tvořen společnostmi v odlišném režimu povinností, tak vznikají další náklady a administrativní zátěž spojená s řízením společností v odlišných režimech.

Pro řadu koncernů by bylo nejjednodušší plnit zákonné požadavky v jednom režimu povinností (vyšší režim), poskytovatel regulované služby v režimu nižších povinností však může toliko zabezpečovat dobrovolně své systémy podle požadavků kladených na poskytovatele regulované služby v režimu vyšších povinností, ke změně režimu povinností (z nižšího režimu na vyšší) však nedochází.[1]

Seznam bezpečnostních opatření dle ust. § 14 ZKB kladených na poskytovatele regulované služby v režimu vyšších povinností sice v zásadě obsahuje povinnosti, které jsou kladeny na poskytovatele regulované služby v režimu nižších povinností, ten však nemůže slepě plnit dle bezpečnostních požadavků pro vyšší režim. Poskytovateli regulované služby v nižším režimu povinností, který chce plnit povinnosti pro poskytovatele regulované služby ve vyšším režimu povinností tak lze doporučit, aby prověřil, zda na něj ZKB zároveň neklade v rámci režimu nižších povinností povinnost, kterou již poskytovatel ve vyšším režimu nemusí plnit. Pokud by totiž NÚKIB ke kontrolám přistupoval striktně formalisticky, tak se může stát, že poskytovatel regulované služby v režimu nižších povinností bude plnit veškeré povinnosti v režimu vyšších povinností a NÚKIB mu následně formalisticky udělí pokutu za nesplnění povinnosti, která je určena pouze pro poskytovatele regulované služby v režimu nižších povinností.[2]

Společnosti jsou rovněž omezeny místem hlášení incidentů, jestliže by totiž poskytovatel regulované služby v nižším režimu hlásil incident NÚKIBU namísto Národnímu CERTU, tak opět riskuje udělení pokuty až do výše 175 000 000 Kč nebo až do výše 1,4 % čistého celosvětového ročního obratu dosaženého podnikem podle čl. 101 a 102 SFEU.[3]

Pro určení, zda se vyplatí zavést u všech společností jednotný režim, navzdory tomu, že zde stále budou existovat určité odlišnosti (např. místo hlášení incidentu) je vhodné vyhodnotit, kolik společností v koncernu bude vedeno jako poskytovatel regulované služby v režimu vyšších povinností

a kolik zase naopak v nižším režimu povinností. Stejně tak je vhodné zvážit potenciální náklady u zavádění obou režimů.

Prověřování dodavatelů

Jedním z hlavních bezpečnostních opatření dle ust. § 14 odst. 1 písm. a) bodu č. 7 je pro poskytovatele regulované služby v režimu vyšších povinností rovněž řízení dodavatelů. Ust. § 31 ZKB dále ukládá poskytovatelům strategicky významné služby povinnost zjišťovat informace o dodavatelském řetězci. Ke zjištění informací o dodavatelském řetězci je dle důvodové zprávy ZKB nezbytné vyvinout přiměřené úsilí, a to například skrze dotazování přímého dodavatele, s nímž poskytovatel vstoupil do smluvního vztahu, případně skrze dohledání informací o poddodavatelích dodavatele v otevřených zdrojích. Samotný pojem přiměřené úsilí je navíc neurčitým právním pojmem, kterému v návrhu zákona neodpovídá přesná definice, neboť zákonodárce si chtěl ponechat volný prostor pro posuzování jednotlivých případů.

Hodnocení, zda poskytovatel strategicky významné služby v daném případě přiměřené úsilí vyvinul, či nikoli se bude dle důvodové zprávy tedy odvíjet vždy od konkrétních skutkových okolností. Vzhledem k výše uvedenému je nepochybně vhodné, aby úprava informování o dodavatelském řetězci byla zahrnuta do smluv s dodavateli. Stejně tak je vhodné zavést funkční compliance procesy, které budou dokumentovat míru vynaloženého úsilí pro potřeby kontroly plnění uvedených povinností NÚKIBEM.

Útěchou může být to, že důvodová zpráva také uvádí, že je vždy nutné postupovat proporcionálně. Nelze tedy ani předpokládat nutnost zjišťovat informace o dodavatelích všech komponent až na zcela základní výrobní úroveň, a to zejména v případě, že proces zjišťování nebude opodstatněn bezpečnostními riziky, která jednotlivé komponenty či programové vybavení představují pro kybernetickou bezpečnost strategicky významné služby.[4]

Poskytovateli strategicky významné služby tedy lze doporučit:

1. v každém případě detailně prověřit své významné dodavatele a subdodavatele;
2. vést a uchovávat dokumentaci o prověřování významných dodavatelů.

Smlouvy s významnými dodavateli

Poskytoval regulované služby v režimu vyšších povinností má také povinnost zanášet bezpečnostní požadavky do smluv s dodavateli. Tato povinnost se vztahuje nejen na nově uzavírané smlouvy, ale i na ty již uzavřené. Pokud se tedy osoba stane poskytovatelem regulované služby v průběhu plnění smlouvy, je potřeba uzavřenou smlouvu revidovat tak, aby obsahovala skutečně všechny relevantní požadavky vyplývající z bezpečnostních opatření, která musí poskytovatel regulované služby nově plnit, resp. k jejichž plnění zavazuje své dodavatele. Pokud smlouva všechny takové požadavky neobsahuje, je nutné zahájit proces změny smlouvy. V případě, kdy změna není možná (typicky např. ve chvíli, kdy by uzavřením dodatku došlo k porušení pravidel zákona o zadávání veřejných zakázek a jiný postup by nepřicházel v úvahu), je potřeba provést změnu smlouvy ihned, jakmile to bude možné.[5]

Doporučený obsah smlouvy uzavírané s významnými dodavateli má dle Přílohy č. 6 k Vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby tvořit např.:

a) ustanovení o bezpečnosti informací z pohledu důvěrnosti (včetně ustanovení o mlčenlivosti), integrity a dostupnosti;

b) ustanovení o oprávnění užívat data;

c) ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zavazují dodržovat v plném rozsahu ujednání mezi povinnou osobou a do davatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele;

d) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele (nebo odsouhlasení pro dodavatelský vztah relevantních částí bezpečnostních politik) povinnou osobou,

e) ustanovení o povinnosti dodavatele informovat povinnou osobu o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy, způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy, dále také o významných změnách.[6]

To, že ZKB počítá s tím, že poskytovatelé strategicky významné služby budou bezproblémově aktualizovat smluvní dokumentaci s dodavateli je jedna věc, to, že dodavatelé často odmítají plnit požadavky stanovené ZKB je zcela odlišným problémem. Poskytovatel strategicky významné služby musí u všech svých významných dodavatelů pod pohrůžkou vysokých pokut zajistit, aby plnili povinnosti dle ZKB, pokud však dodavatelé odmítají uzavřít dodatky ke smlouvám, tak je k řešení problémů nutné přistoupit kreativnějším způsobem (např. odkazováním na vnitřní normu, která bude přílohou smluvní dokumentace).

Formalistická komunikace s NÚKIBEM

Poskytovatelé regulované služby musí dbát na to, že ust. § 45 ZKB stanovuje, že vybrané úkony (např. ohlášení regulované služby, hlášení kontaktních údajů, incidentů nebo provedení protiopatření) musí být provedeny výlučně prostřednictvím formulářových podání na Portálu NÚKIBU. Pokud nebudou úkony provedeny stanoveným způsobem, tak budou považovány za neúčinné, za neúčinné provedení úkonu může být přitom poskytovatelům regulované služby opět udělena poměrně vysoká pokuta.[7] Poskytovatelé regulované služby by tedy měli vždy dbát na to, aby všechny prováděné úkony byly učiněny prostřednictvím formulářových podání a splnily náležitosti, které vyžadují prováděcí vyhlášky k ZKB.

Závěr

Je patrné, že správné nastavení systému jednotného řízení kybernetické bezpečnosti může koncernu zajistit konkurenční výhodu. Koncerny by se již teď měly snažit zmapovat do jakého režimu budou zařazeny jejich společnosti, stejně tak je důležité neprodleně provést audit smluvní dokumentace s významnými dodavateli. S ohledem na složitost problematiky je řízení kybernetické bezpečnosti také vždy vhodné konzultovat s odborníky na právo kybernetické bezpečnosti.

Mgr. Ondřej Rada,
advokátní koncipient

VKS LEGAL
ADVOKÁTNÍ KANCELÁŘ

VKS Legal advokátní kancelář, s. r. o.

dům u Nováků, Vodičkova 30
110 00 Praha 1 - Nové Město, 3. schodiště, 5. patro

tel.: +420 224 947 158
e-mail: office@akvks.cz

---

[1] Viz ust. § 13 důvodové zprávy sněmovního tisku č. 759/0, vládní návrh zákona o kybernetické bezpečnosti

[2] Viz ust. § 14 důvodové zprávy sněmovního tisku č. 759/0, vládní návrh zákona o kybernetické bezpečnosti

[3] Viz st. § 59 odst. 2 písm. h) sněmovního tisku č. 759/0, vládní návrh zákona o kybernetické bezpečnosti

[4] Viz ust. § 31 důvodové zprávy sněmovního tisku č. 759/0, vládní návrh zákona o kybernetické bezpečnosti

[5] Viz ust. § 13 důvodové zprávy sněmovního tisku č. 759/0, vládní návrh zákona o kybernetické bezpečnosti

[6] Viz příloha č. 6 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (sněmovní tisk č. 759/0)

[7] Viz ust. § 45 důvodové zprávy sněmovního tisku č. 759/0, vládní návrh zákona o kybernetické bezpečnosti

Další články:

- Rozdělení společného jmění manželů v případech výdělečné činnosti pouze jednoho z manželů
- Oběť znásilnění má nárok na peněžitou satisfakci
- Digitalizace AML povinností: jak technologie mění plnění povinností pro tisíce povinných osob
- (Ne)vypořádání předmětu řízení u soudního smíru
- Nové limity opatrovnického rozhodování v judikatuře ESLP a Ústavního soudu
- Mimosmluvní odměna při společném zastupování více osob
- Nepřiznané koalice
- Společnost s podíly 50:50 – právní rizika patových situací a jejich smluvní řešení
- Byznys a paragrafy, díl 34: Jednání za společnost – prokura
- Jak nastavit smlouvy s dodavateli podle nové právní úpravy kybernetické bezpečnosti?
- Vada koupené věci – kdy zjištěné nedostatky zakládají kupujícímu práva z vadného plnění a kdy nikoliv?