Jak promítnout požadavky plynoucí ze směrnice NIS2

do smluv s dodavateli

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.
Policejní akademie České republiky v Praze
Císař, Češka, Smutný, advokátní kancelář

30 1993-2023 CÍSAŘ ČEŠKA SMUTNÝ

Současná právní úprava

- **Směrnice NIS -** 2016/1148, z 6. 7. 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
- **Zákon ZKB** - 181/2014 Sb. o kybernetické bezpečnosti
- **Vyhláška VKB** – vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti
- **Oblast řízení dodavatelů zejména:**
  - Příloha č. 7 VKB
  - § 4 odst. 4 ZKB

Směrnice NIS 2 a její implementace

- **Směrnice NIS 2 -** 2022/2555, z 14. 12. 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii

  Očekávaná implementace směrnice v ČR – polovina roku 2024

- Zákon kybernetické bezpečnosti + prováděcí předpisy – mělo by být zahájeno mezirezortní připomínkové řízení

- Součástí nového zákona je i **mechanismus posuzování rizik** spojených s dodavatelem, který byl původně plánován jako samostatný zákon – mimo rámec Směrnice NIS 2

Regulace smluv s dodavateli dle NIS 2

- Čl. 85 recitálu NIS 2: *Základní a důležité subjekty by měly být zejména vybízeny,* ***aby začlenily opatření k řízení kybernetických bezpečnostních rizik do smluvních ujednání se svými přímými dodavateli a poskytovateli služeb.***
- Čl. 21 NIS 2: základní a důležité subjekty by měly přijmout přiměřená technická, provozní a organizační opatření k řízení bezpečnostních rizik, které zahrnují i:
  - *bezpečnost dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;*
- Čl. 22 NIS 2: Koordinované posouzení bezpečnostních rizik kritických dodavatelských řetězců na unijní úrovni (Komise + ENISA)

Řízení dodavatelů v návrhu zákona o kybernetické bezpečnosti

- Návrh zákona plně přebírá princip dosavadního § 4 odst. 4 ZKB
- Návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností plně přebírá dosavadní principy řízení dodavatelů dle ZKB a VKB

X

Návrh zákona ruší dosavadní kategorii „provozovatelů“, ponechává však kategorii významných dodavatelů

X

Nově je zaveden Mechanismus prověřování bezpečnosti dodavatelského řetězce

Řízení dodavatelů v současné právní úpravě

- § 8 VKB musí povinná osoba řídit rizika spojená s dodavateli
- Při výběru dodavatele nutné zohlednit stanovená bezpečnostní opatření dle výsledku analýzy rizik
- U významných dodavatelů je nezbytné zohlednit oblasti uvedené v příloze č. 7 VKB + vést evidenci významných dodavatelů
- **veškerá rizika** spojená s dodavateli **posuzují samotné povinné osoby**
- povinné osoby **musí** varování či doporučení NÚKIB **pouze zohlednit** v analýze rizik a následně výsledky promítnout do zadávacích podmínek
- aplikace § 4 odst. 4 ZKB

Požadavky na smlouvy s významnými dodavateli

- ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity)
- ustanovení o oprávnění užívat data,
- ustanovení o autorství programového kódu, popřípadě o programových licencích,
- ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),
- ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem
- ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,
- ustanovení o řízení změn,
- ustanovení o souladu smluv s obecně závaznými právními předpisy,

Požadavky na smlouvy s významnými dodavateli II

- 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,
  - významné změně ovládání tohoto dodavatele podle ZOK
- specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),
- specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),
- specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,
- pravidla pro likvidaci dat,

Požadavky na smlouvy s významnými dodavateli III

- ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy a
- ustanovení o sankcích za porušení povinností

Vysvětlení požadavků na smlouvy s dodavateli obsahuje podpůrný materiál NÚKIB: „Požadavky na smlouvy s dodavateli“ – dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/pozadavky_na_smlouvy_s_dodavateli_v1.4.pdf

Mechanismus prověřování bezpečnosti dodavatelského řetězce

- prověřování bude provádět NÚKIB ve spolupráci s dalšími subjekty
- Mechanismus by měl přinést možnost vyloučit z dodávek do strategicky významné infrastruktury vysoce rizikové dodavatele
- prověřování dodavatelů se bude týkat pouze dodávek do stanovených částí strategicky významné infrastruktury, která je kritická pro fungování státu
- NÚKIB vydá opatření obecné povahy, ve kterém stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky, zjistí-li možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku x možnost individuální výjimky

Plnění povinností dle přílohy č. 7 VKB v praxi

- Často snaha o zapracování požadavků do obchodních podmínek, nebo smluvních vzorů
- Skutečnost, že je určitý dodavatel významným dodavatelem, je nutné určit ve smlouvě, případně je nutné takového dodavatele prokazatelně písemně informovat o tom, že je významným dodavatelem a o jeho konkrétních povinnostech
- Úprava v obchodních podmínkách, nebo smluvních vzorech, však **neznamená, že povinná osoba měla rezignovat na určování smluvních podmínek pro dodavatele individuálně u každé smlouvy**
- některé povinnosti dle vyhlášky zobecnit nejdou (např. otázka exit plánu, součinnosti př ukončení smlouvy, zahrnutí do havarijních plánů apod.)
    - X Je vhodné rozhodnout, zda nebudou vyloučeny některá nerelevantní ustanovení VKB
    - X Je nutné s ohledem na předmět plnění rozhodnout, jaká konkrétní opatření by měl dodavatel dodržovat
- Není vhodné jít cestou „maximální přísnosti“
- **nutné určovat jednotlivé požadavky individuálně, nelze odkázat na „plnění všech povinností dle ZKB“**

Dopady na povinné osoby Mechanismu

- Nově povinnost zjišťovat a dokumentovat informace o dodavatelích (i poddodavatelích!) bezpečnostně významných dodávek - tyto hlásit NÚKIB, včetně změn
- Zvýšená nejistota v této oblasti – k zákazu může dojít kdykoliv v době trvání závazku
- Vhodná úprava smluvních vztahů s dodavateli kvůli možnosti vydání OOP
- Veřejný zadavatel může závazek ze smlouvy na veřejnou zakázku vypovědět bez zbytečného odkladu poté, co zjistí, že v jejím plnění nelze pokračovat, aniž by bylo porušeno OOP
- Sledování procesu přijímání OOP, připomínkování návrhu OOP, tvorba žádostí o udělení výjimky

Děkuji za pozornost.

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.

vlachova@polac.cz

vlachova@akccs.cz