31. 3. 2020

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

Řízení dodavatelů při zajišťování kybernetické bezpečnosti

K povinnostem, které mají některé orgány a osoby podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „ZKB"; tyto orgány a osoby dále jen „povinné osoby"), patří také řízení dodavatelských vztahů. Ustanovení ZKB provádí vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „VKB"). Proces řízení dodavatelských vztahů můžeme z hlediska ZKB, resp. VKB rozdělit na etapy plánování, pořizování, realizace a ukončení vztahu.

Předpokladem řádného průběhu řízení dodavatelských vztahů je připravenost povinné osoby vyžadovaná uvedenými právními předpisy. Jde mj. o stanovení systému řízení bezpečnosti informací, provedení analýzy rizik, stanovení bezpečnostních opatření, zpracování bezpečnostních politik a bezpečnostní dokumentace apod.

V **etapě plánování** povinná osoba dle § 13 VKB v souvislosti s plánovanou akvizicí, vývojem a údržbou chráněného systému mj. řídí rizika a významné změny a stanoví bezpečnostní požadavky, které zahrne do projektu akvizice, vývoje a údržby. Povinná osoba má v této etapě rovněž zajistit bezpečnost vývojového a testovacího prostředí.

Projekt akvizice, vývoje a údržby bude podkladem pro zpracování zadávací dokumentace pro výběr dodavatele zamýšleného plnění, který proběhne v **etapě pořizování**. V případě veřejných zadavatelů je nezbytné zadávací dokumentaci zpracovat dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**")[1]. VKB rozlišuje dvě úrovně dodavatelů – „běžné" a významné ve smyslu § 2 písm. n) VKB. Významným dodavatelem je vždy provozovatel chráněného systému a dále každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti chráněného systému. Podle § 8 VKB musí povinná osoba řídit rizika spojená s dodavateli. Podle názoru autora jde zejména o rizika ve vztahu k hrozbám spojeným se způsobilostí dodavatele poskytovat zamýšlené plnění, se slabým postavením zadavatele ve smluvním vztahu, s nedostatkem prostředků alokovaných pro provádění vztahu na obou smluvních stranách apod.

Podstatnou činností zadavatele bude zpracování smlouvy, na základě které bude dodavatel zamýšlené plnění poskytovat. U běžných dodavatelů je třeba v návrhu smlouvy zohlednit stanovená bezpečnostní opatření, výsledky analýzy rizik dle § 8 odst. 1 VKB, potřebu součinnosti pro provádění auditu kybernetické bezpečnosti, potřebu řízení bezpečnosti lidských zdrojů apod. U významných dodavatelů je v návrhu smlouvy nezbytné zohlednit rovněž relevantní oblasti uvedené v příloze č. 7 VKB, jakož i potřebu součinnosti takového dodavatele dle § 8 odst. 2 VKB.

Pro povinné osoby, které jsou orgány veřejné moci, obsahuje ZKB speciální úpravu vztahující se na dodavatele poskytující služby cloud computingu. Do smlouvy je v takovém případě vedle výše uvedeného nezbytné zahrnout náležitosti dle § 4 odst. 5 ZKB[2].

V **realizační etapě** je dle § 8 odst. 2 VKB zadavatel povinen u plnění poskytovaných významnými dodavateli pravidelně hodnotit rizika a kontrolovat provádění bezpečnostních opatření. Přestože je to výslovně upraveno jen pro významné dodavatele, je vhodné zvážit přiměřené provádění těchto

činností i u plnění poskytovaných běžnými dodavateli. Řízení rizik je dynamická, průběžná činnost, což vyplývá jednak z obecných pravidel upravených § 3 VKB, ale i ze samotného smyslu a účelu ZKB, kterým je zajištění bezpečnosti informací v chráněných systémech existujících v kybernetickém prostoru, což je vysoce komplexní a neustále se měnící prostředí. Přirozeným důsledkem je pak potřeba pravidelného přezkoumávání bezpečnostních opatření. To se zpravidla neobejde bez součinnosti dodavatele, se kterou je proto nezbytné počítat při formulování smlouvy.

Podle § 12 VKB musí povinná osoba při **ukončení vztahu** zajistit odebrání nebo změnu přístupových oprávnění osob na straně dodavatele. Pokud se ukončuje smluvní vztah s administrátorem nebo osobou zastávající bezpečnostní roli, je povinná osoba dle § 9 VKB povinna zajistit předání odpovědností. ZKB upravuje v § 6a povinnost provozovatele některých chráněných systémů předat správci data, provozní a další informace, pokud o to správce požádá nebo pokud provozovatel přestane systém provozovat. Jiné povinnosti vztažené k ukončení vztahu s dodavatelem ZKB a VKB výslovně neupravují. Případné negativní dopady vyplývající z nedostatečně smluvně zajištěného ukončení vztahu s dodavatelem, zvláště jde-li o ukončení z hlediska dodavatele nedobrovolné, by se však měly projevit při hodnocení dodavatelských rizik v předchozích etapách procesu řízení dodavatelských vztahů. Důsledkem bude nezbytnost mít pro bezproblémové ukončení vztahu s dodavatelem sjednán tzv. exit plán (případně jeho zpracování a pravidelnou aktualizaci) a povinnost dodavatele podle tohoto plánu postupovat. Nutnost exit plánu je výslovně upravena v § 4 odst. 5 písm. d) ZKB pro smlouvy orgánů veřejné moci s dodavateli poskytujícími služby cloud computingu.

Lze shrnout, že řízení dodavatelských vztahů podle právní úpravy kybernetické bezpečnosti je komplexní proces vyžadující na straně zadavatele dostatečnou připravenost. Oba právní předpisy kladou nároky na obsah smluvního vztahu, přičemž rozsah jejich dopadů do návrhu smlouvy závisí na povaze zamýšleného plnění. Některé náležitosti smluvních vztahů uvádí ZKB, resp. VKB výslovně, jiné vyplývají z jejich ustanovení nepřímo. Systém řízení bezpečnosti informací musí být schopen reagovat na vývoj bezpečnostních hrozeb a je tedy z povahy věci dynamickým fenoménem. Z toho vyplývá, že úprava součinnosti dodavatele sjednaná ve smlouvě musí být dostatečně široká a flexibilní, aby umožňovala průběžné reagování na vývoj systému řízení bezpečnosti informací zadavatele.

Mgr. Ing. Robert Kotzian, Ph.D.
Právník a bývalý programátor-analytik

E-mail: robert@kotzian.cz

---

[1] KOTZIAN, R. *Veřejné zakázky a kybernetická bezpečnost.* 28. 1. 2020, epravo.cz. K dispozici >>> zde.

[2] V některých případech se smluvní náležitosti požadované § 4 odst. 5 ZKB dublují s požadavky vyplývajícími z VKB.

Další články:

- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- TOP 5 judikátů z korporátního práva za rok 2025
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- SCHEJBAL& PARTNERS stáli u získání jedné z prvních licencí dle MiCA v ČR
- Proč dnes více než polovina M&A transakcí ve střední Evropě nekončí podpisem
- Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi
- Návrh nového zákona o digitální ekonomice
- Byznys a paragrafy, díl 30.: Jednání za s.r.o. – zápis jednatelského oprávnění do obchodního rejstříku
- Prověřování zahraničních investic a kybernetická regulace: řízená služba jako nová transakční proměnná
- Předběžné opatření a další instituty k ochraně věřitelů při přeměnách