Zvýšení bezpečnosti dodavatelského řetězce pro strategickou infrastrukturu státu je v zájmu České republiky

23.9.2022 - | Národní úřad pro kybernetickou a informační bezpečnost

V reakci na zhoršující se bezpečnostní prostředí uložila BRS v červnu 2022 NÚKIB do konce května 2023 předložit vládě České republiky návrh zákona umožňující státu prověřování dodavatelů do své strategicky významné infrastruktury. Hlavním cílem tohoto prověřování je zvýšit odolnost a bezpečnost České republiky.

Současný vývoj ukazuje, že bezpečnost dodavatelského řetězce a spolehlivost dodavatelů v oblasti informačních a komunikačních technologií má zcela zásadní dopad na bezpečnost subjektů klíčových pro stát i společnost a tím také na národní bezpečnost jako takovou. Hrozby v oblasti kybernetické bezpečnosti plynoucí z dodavatelských řetězců technologií jsou již dlouhodobě známy, dosud však v našem právním řádu neexistuje komplexní právní řešení umožňující rizika plynoucí z těchto hrozeb pro strategickou infrastrukturu cíleně a účinně vyhodnocovat a snižovat. Připravovaný zákon si klade za cíl tento nevyhovující stav změnit.

Mechanismus prověřování dá státu možnost vyloučit z dodávek do strategicky významné infrastruktury vysoce rizikové dodavatele a významně tak omezí dopad negativních zahraničních vlivů na zajištění základních funkcí státu. Tím se sníží závislost nejvýznamnější infrastruktury na dodavatelích představujících strategickou hrozbu v oblasti kybernetické bezpečnosti, což přispěje k zajištění dlouhodobě udržitelné bezpečnosti a odolnosti. Tento mechanismus napomůže předcházet podobně nežádoucí závislosti a následným negativním dopadům, jako je tomu nyní například v případě zemního plynu.

Připravovaný návrh zákona zmocní relevantní orgány státu k vyhodnocení a případnému omezení rizikových dodavatelů. Vyhodnocována budou kritéria spojená s oblastmi, jako jsou vliv cizího státu na dodavatele či případy zneužití technologií k narušení strategické infrastruktury. Konkrétní podoba procesu prověřování je momentálně diskutována napříč relevantními orgány státní správy.

„Rozsah dopadu regulace zatím není přesně vymezen a intenzivně na něm pracujeme. Když mluvíme o strategické infrastruktuře, vycházíme z množiny systémů kritické informační infrastruktury a provozovatelů základních služeb dle současného znění zákona o kybernetické bezpečnosti. Samozřejmě nás v této oblasti čekají změny v souvislosti s implementací směrnice NIS2, díky které naroste počet povinných orgánů a osob až na několik tisíc subjektů. Připravovaný mechanismus ale bere tyto změny v potaz a na většinu těchto nových povinných osob nedopadne. Cílem je pokrýt množinu institucí, která poskytuje či zabezpečuje služby s nejvyšším dopadem na fungování státu a společnosti," sděluje k celé věci ředitel NÚKIB Lukáš Kintr.

Úřad pod jeho vedením při přípravě návrhu zákona předpokládá dodržení dosavadní osvědčené praxe. Tzn. Jakmile to bude aktuální, nad rámec běžného meziresortního připomínkového řízení bude odborné veřejnosti dána možnost poskytnout NÚKIB podněty k návrhu zákona. Vzhledem ke skutečnosti, že se jedná o komplexní a citlivou problematiku, NÚKIB vede a plánuje nadále vést širokou, odbornou a především konstruktivní debatu.

Samotný mechanismus staví na principech zákona o kybernetické bezpečnosti (ZKB). Připravovaná legislativa tak bude doplňovat současný přístup k zajišťování kybernetické bezpečnosti v České

republice, podle kterého se o komplexní zajištění bezpečnosti stará především správce systému či sítě. Mechanismus prověřování tak vnese do procesu nový vstup státu v podobě hodnocení strategické úrovně bezpečnosti dodavatelů. Jedná se o aspekty, které sami správci infrastruktury nejsou schopni provést a k jejichž posuzování a vyhodnocování je nejlépe vybaven právě stát se svým bezpečnostním a zpravodajským aparátem. Důležitou složkou mechanismu je nastavení procesu prověřování tak, aby pro splnění svého účelu co nejméně zatěžoval jak povinné subjekty, tak stát samotný. Prověřování se tedy bude týkat pouze dodávek do jasně, předem stanovených částí strategicky významné infrastruktury, která je kritická pro fungování České republiky. Dodávky, které nejsou relevantní pro bezpečnost této infrastruktury, prověřovány nebudou.

> Do doby, než bude nový zákon připraven a přijat, jsou nadále platné a účinné aktuální právní normy v oblasti kybernetické bezpečnosti. V kontextu omezení rizikových dodavatelů se pro povinné orgány a osoby dle ZKB jedná zejména o povinnost řídit rizika spojená s dodavateli dle ZKB a vyhlášky o kybernetické bezpečnosti. Správci a provozovatelé kritické informační infrastruktury a další povinné orgány a osoby dle ZKB jsou také nadále povinny zohledňovat dříve vydaná varování NÚKIB. Nezávaznou pomůckou, jak hodnotit rizikovost dodavatelů, může pro správce povinných subjektů být „Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice“ zpracované NÚKIB s dalšími partnery bezpečnostní komunity a využitelné i mimo sektor telekomunikací.

https://www.nukib.cz/cs/infoservis/aktuality/1876-zvyseni-bezpecnosti-dodavatelskeho-retezce-pro-strategickou-infrastrukturu-statu-je-v-zajmu-ceske-republiky