Stát vstupuje do závěrečné fáze přípravy návrhu zákona o snižování rizik spojených s dodavateli informačních a komunikačních technologií

24.11.2022 - | Národní úřad pro kybernetickou a informační bezpečnost

Připravit návrh zákona, zavádějící mechanismus prověřování dodavatelů, uložila Bezpečnostní rada státu NÚKIB v červnu 2022, s termínem předložení návrhu vládě v květnu 2023.

„Jsem rád, že se nám i přes složitost této problematiky daří plnit harmonogram přípravy návrhu zákona a že se již nyní blížíme okamžiku, kdy budeme moci s partnery ze státní správy, soukromého a akademického sektoru konzultovat konkrétní znění této mimořádně významné legislativy,“ říká k postupu ředitel NÚKIB Lukáš Kintr a dále dodává: *„Věřím, že pokud budou všechny strany zapojené do přípravy aktivní a konstruktivní, může mít Česká republika do dvou let komplexní systém pro omezení závislosti státu na nedůvěryhodných zahraničních dodavatelích. V oblasti informačních technologií tak do budoucna doufejme předejdeme situaci, jakou nyní pozorujeme například v souvislosti s dodávkami ropy a zemního plynu z Ruské federace.“*

Mechanismus prověřování dodavatelů, jak je hlavní produkt návrhu zákona zkráceně nazýván, by měl státu umožnit odhalit nedůvěryhodné dodavatele technologických prvků nejvýznamnější, tzv. strategické infrastruktury České republiky, vyhodnotit riziko spojené s těmito dodavateli a v případě vysokého rizika omezit využití takových dodavatelů v dané infrastruktuře.

Jak již označení „nejvýznamnější“ napovídá, připravovaný zákon by se neměl vztahovat na všechny systémy a služby regulované zákonem o kybernetické bezpečnosti, ale pouze na jejich podmnožinu s největším dopadem na stát a společnost. Ze současného členění povinných osob zákona o kybernetické bezpečnosti by měl nový zákon dopadnout na kritickou informační infrastrukturu a část informačních systémů základních služeb.

Do budoucna se nicméně kategorizace regulovaných osob v oblasti kybernetické bezpečnosti změní v důsledku aktualizace směrnice EU o kybernetické bezpečnosti, tzv. NIS2. Jelikož však provedení NIS2 do vnitrostátního práva připravuje NÚKIB jako gestor pro oblast kybernetické bezpečnosti, jsou obě legislativní změny chystány společně a v synergii. Výsledné návrhy by tedy měly plně odpovídat jak českým, tak celounijním potřebám a požadavkům. NIS2 tak ve vztahu k mechanismu prověřování dodavatelů změní pouze pojmy, nijak ale nezmění rozsah subjektů, kterých se mechanismus dotkne.

Prověřování by měl podle návrhu mechanismu provádět NÚKIB ve spolupráci s ministerstvy, zpravodajskými službami a dalšími organizačními složkami státu, majícími relevantní informace pro posouzení důvěryhodnosti dodavatele. Základem mechanismu však budou elementární informace o dodavatelích, poskytnuté jednotlivými správci regulované infrastruktury. Tyto informace stát spojí s vlastními informacemi a informacemi získanými od zahraničních partnerů a vyhodnotí na jejich základě naplnění či nenaplnění konkrétních kritérií pro prověření dodavatele. Daná kritéria budou zkoumat

otázky existence a závažnosti hrozeb plynoucích z dodavatelských řetězců pro národní bezpečnost

nebo veřejný pořádek prostřednictvím možnosti cizího státu převzít dodavatele, využít jej ke státní špionáži, narušit dostupnost cizí kritické infrastruktury a jiných rizik.

Samotné prověřováni bude stát moci provádět jak se zaměřením na dodavatele, kteří již svá plnění do strategické infrastruktury dodávají, tak na jejich poddodavatele a na potenciální dodavatele. Pokud bude identifikováno riziko spojené s dodavatelem, bude stát moci využití takového dodavatele v regulované infrastruktuře omezit obdobou současného varování dle zákona o kybernetické bezpečnosti či přímo zakázat formou opatření obecné povahy, směřujícího na množinu strategické infrastruktury. Na prověření dodavatele nebude existovat nárok a není ani ambicí státu prověřit všechny dodavatele, ale pouze ty, u kterých bude možná hrozba nějak indikována, například na základě aktuální bezpečnostní situace.

Cílem mechanismu je prověřovat zejména budoucí dodavatele. S omezením by tedy měly být všechny strany seznámeny nejlépe ještě před výběrem konkrétního dodavatele a uzavřením smlouvy. Může se ale stát, že bude některý dodavatel vyhodnocen jako nedůvěryhodný až po uzavření smlouvy. V takovém případě bude správci infrastruktury dána přiměřená lhůta pro to nahradit plnění od nedůvěryhodného dodavatele jiným, tak aby omezení zasáhlo do jeho podnikání či jiných činností co nejméně. Celý proces bude tedy maximálním způsobem chránit práva správce infrastruktury i samotného dodavatele a bude co možná nejvíce transparentní, včetně možnosti dotčených orgánů a osob vyjádřit se k rozsahu zamýšleného zákazu využití dodavatele.

Dne 7. prosince 2022 plánuje NÚKIB uspořádat seminář k připravovanému návrhu zákona (více viz pozvánka), kde účastníkům umožní diskutovat o prověřování dodavatelů v širších souvislostech. Tato akce volně navazuje na předchozí diskuse o této problematice, které se odehrály v červenci a v listopadu 2022 na půdě Poslanecké sněmovny Parlamentu České republiky a v září 2022 na konferenci CyberCon Brno či panelu v CEVRO Institutu v Praze. Možnost seznámit se s návrhem zákona a vyjádřit se k němu budou mít v následujících týdnech organizační složky státu zapojené do přípravy, v prvním čtvrtletí příštího roku pak bude možnost vyjádření se otevřena široké odborné veřejnosti.

Informace o dalším postupu, včetně možnosti vyjádření se k návrhu, budou uvedeny na webových stránkách NÚKIB.

https://www.nukib.cz/cs/infoservis/aktuality/1911-stat-vstupuje-do-zaverecne-faze-pripravy-navrhu-zakona-o-snizovani-rizik-spojenych-s-dodavateli-informacnich-a-komunikacnich-technologii