Bird & Bird

Jak NIS 2 mění kyberbezpečnost v telekomunikacích v České republice

Ján Kuklinca

červenec 2025

Česká republika konečně do vnitrostátního práva implementovala požadavky směrnice NIS2 pro oblast kybernetické bezpečnosti, a to prostřednictvím nového zákona o kybernetické bezpečnosti (dále jen „**zákon**“). Níže shrnujeme jeho klíčové požadavky zejména pro sektor telekomunikací.

Co nový zákon znamená pro poskytovatele telekomunikačních služeb a další společnosti?

Nad rámec dobře známých dopadů NIS2 – tj. širší rozsah regulace a přísnější sankce –přináší zákon i několik dalších novinek.

Mnohé z nich byly zavedeny zcela cíleně, neboť právě Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), čerpajíc ze svých zkušeností z aplikace současného zákona, byl tím orgánem, který implementaci jménem vlády ČR připravoval.

Mezi klíčové aspekty patří detailnější pravidla pro vymezení rozsahu ISMS (systému řízení bezpečnosti informací), široké vymezení povinnosti hlásit incidenty, podrobný katalog bezpečnostních opatření a nová pravomoc omezit nebo dokonce zakázat nezabezpečené produkty či dodavatele v dodavatelském řetězci. Navzdory všemu však zákon o kybernetické bezpečnosti není dokonalý – institut „hlavní provozovny“ pro poskytovatele digitálních infrastrukturních služeb mohl být vyřešen lépe.

Vymezení rozsahu ISMS

Zákon zohledňuje, že jedna společnost může provozovat různé činnosti, a ty ne vždy musí být vzájemně provázané.

Pokud jsou různá podnikání na sobě zcela nezávislé v tom smyslu, že nesdílejí žádná primární ani podpůrná aktiva, může zcela oddělená neregulovaná služba zůstat mimo vydefinovaný rozsah ISMS. Společnost však má povinnost zdokumentovat to, proč se daná aktiva netýkají regulovaných služeb.

Dále je třeba zmínit, že pokud se určitý regulovaný subjekt stane podle NIS2 subjektem ve vyšším režimu povinností ve vztahu k jedné regulované službě, musí požadavky ve vyšším režimu uplatňovat na všechny své regulované služby – tj. i na ty, které by jinak spadaly jen do nižšího režimu.

Široké vymezení povinnosti hlásit incidenty

Na rozdíl od směrnice NIS2, která ukládá povinnost hlásit **významné incidenty**, budou muset společnosti spadající do vyššího režimu povinností v České republice hlásit **všechny** incidenty kybernetického původu, pokud ve vztahu k nim nelze vyloučit úmyslné jednání (ať už vnitřní, či vnější). Jen pro subjekty v nižším režimu povinností platí, že nahlašují pouze významné incidenty.

Dobrou zprávou pro poskytovatele služeb elektronických komunikací je, že už nebudou muset hlásit kybernetické incidenty podle zákona o elektronických komunikacích. Podle tohoto předpisu se povinnost hlásit incidenty omezí výhradně na nekybernetické incidenty.

Podrobná bezpečnostní opatření

Co se týče bezpečnostních opatření, zákon ukládá subjektům ve vyšším režimu přijmout **celkovou bezpečnostní politiku** a průběžně udržovat rámec řízení a správy rizik (tzv. risk management). Ten zahrnuje pro různá rizika dokumentovaný plán řízení rizika (tzv. risk treatment plan). Pro subjekty ve vyšším režimu existuje 25 potenciálních oblastí bezpečnostních opatření, z nichž mnohá obsahují velice podrobná dílčí pravidla (například určování minimální délky hesla pro různé kategorie uživatelů).

Subjekty ve vyšším režimu musí také jmenovat několik **kyberbezpečnostních rolí** – zejména manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a nezávislého auditora kybernetické bezpečnosti.

Bezpečnost dodavatelského řetězce

V zájmu posílení odolnosti dodavatelského řetězce získá Česká republika také **pravomoc omezit nebezpečné produkty či dodavatele**. Tato možnost jde nad rámec samotné směrnice NIS2. Česká vláda tak může pro subjekty strategického významu pomocí vyhlášky omezit konkrétní dodavatele či používání konkrétních produktů. Tento aspekt se týká zejména provozovatelů telekomunikačních sítí, které to může omezit v možnosti využívat zařízení od dodavatelů představujících geopolitické riziko vůči České republice.

Problematická „Hlavní provozovna“

Jeden z problematických bodů zákona je nedostatečné zohlednění mechanizmu **hlavní provozovny** (“main establishment”) a s tím spojené výhradní jurisdikce (tzv. one-stop-shop) pro poskytovatele digitálních infrastrukturních služeb. Ačkoli zákon o kybernetické bezpečnosti odkazuje i na prováděcí nařízení Evropské komise týkající se těchto poskytovatelů, u některých aspektů, které s konceptem souvisí, je překvapivě vágní. Hrozí, že poskytovatelé digitálních infrastrukturních služeb (např. cloudoví poskytovatelé či poskytovatelé řízených služeb – managed services) by podle některých výkladů mohli podléhat nejen jurisdikci země, v níž mají svou „hlavní provozovnu“ kybernetické bezpečnosti, ale současně i jurisdikci České republiky.

Jaké budou další kroky a jak se zákon projeví v praxi?

Zákon o kybernetické bezpečnosti nyní čeká na oficiální zveřejnění ve Sbírce zákonů a následné nabytí účinnosti k 1. listopadu 2025.

V mezidobí lze očekávat, že NÚKIB oficiálně vydá již z veliké části připravené prováděcí vyhlášky, které blíže upravují povinnosti vyplývající ze zákona (např. **kompletní seznam regulovaných služeb** nebo již zmíněný **podrobný katalog bezpečnostních opatření**).

Společnosti budou mít od data nabytí účinnosti zákona **60 dní** na **sebe-vyhodnocení toho, které regulované služby se jich týkají a na zaslání registračního formuláře** k NÚKIBu. Po potvrzení registrace ze strany NÚKIBu začne běžet **roční přechodné období**, během něhož budou muset dotčené subjekty zavést bezpečnostní opatření a připravit se na případné hlášení incidentů v souladu s novou právní úpravou.

twobirds.com

Abu Dhabí • Amsterdam • Bratislava • Brusel • Budapešť • Casablanca • Dubaj • Dublin • Düsseldorf • Frankfurt • Haag • Hamburk • Helsinky • Hongkong • Kodaň • Londýn • Lyon • Madrid • Milán • Mnichov • Peking • Paříž • Praha • Rijád • Řím • San Francisco • Šanghaj • Singapur • Stockholm • Sydney • Šen-čen • Tokio • Varšava