

27. 12. 2024

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

Co nového přináší návrh zákona o kybernetické bezpečnosti nejen v oblasti sankcí za jeho porušení?

Návrh zákona o kybernetické bezpečnosti (sněmovní tisk č. 759) je transpozicí evropské bezpečnostní směrnice NIS 2. Kromě implementace evropské úpravy do českého právního řádu je jeho hlavním účelem nastavení alespoň základní úrovně kybernetického zabezpečení v organizacích, které poskytují své služby ve významných odvětvích pro fungování státu, jakými jsou např. energetika, výkon státní správy, potravinářský průmysl nebo zdravotnictví.

Dle požadavků uvedených ve směrnici měl zákon nabýt účinnosti ke dni 18. října 2024, nicméně je stále v legislativním procesu (aktuálně, tedy v prosinci 2024, je před 2. čtením, po projednávání ve výborech Poslanecké sněmovny) a jeho účinnost se tak odhaduje na polovinu roku 2025. Na koho se má tento zákon vztahovat a co nového přinese nejen v oblasti kyberbezpečnosti? To se dozvíte na několika následujících řádcích.

Koho se tato právní úprava bude týkat?

Nový zákon bude dopadat na ty poskytovatele regulovaných služeb, kteří jsou buď středním nebo velkým podnikem^[1] nebo kteří jsou významní pro zabezpečení důležitých společenských nebo ekonomických činností či pro bezpečnost v České republice. Co se vymezení regulovaných služeb týče, návrh zákona přímo uvádí jejich seznam. Jedná se o služby, které jsou nějakým způsobem významné pro zabezpečení důležitých společenských či ekonomických činností nebo bezpečnost státu. Typickými příklady regulovaných odvětví jsou tedy například energetika, doprava, vybrané digitální služby, zdravotnictví nebo vesmírný průmysl.

Regulované služby jsou dále rozděleny do dvou kategorií dle stanovené míry povinností, a to na služby spadající pod režim vyšších povinností a na služby v režimu povinností nižších. Podle toho, do které kategorie daná služba spadá, se liší míra a intenzita povinností, které budou jejímu poskytovateli zákonem ukládány. Podrobnosti k tomuto rozdělení stejně jako výčet odvětví, která pod regulaci spadají, uvádí nejen návrh samotného zákona, ale i návrh prováděcí vyhlášky o regulovaných službách, která je jeho přílohou.

Jaké budou povinnosti dotčených subjektů?

Návrh zákona zavádí pro poskytovatele regulovaných služeb mnohé povinnosti související se zajištěním vyšší úrovně kybernetické ochrany, minimalizací rizik spojených s kybernetickými hrozbami a primárně posílením odolnosti strategicky významných odvětví proti těmto hrozbám. Nižší uvádíme přehled klíčových povinností, které se poskytovatelů po nabytí účinnosti tohoto zákona budou týkat. Zde je však třeba podotknout, že návrh zákona je stále v legislativním procesu a je tedy možné, že finální verze zákona se od té aktuální ještě odchýlí.

V první řadě mají poskytovatelé regulovaných služeb povinnost do 60 dnů od naplnění podmínek pro registraci regulované služby, tuto skutečnost ohlásit Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“ nebo „Úřad“), jakožto ústřednímu správnímu úřadu pro oblast kybernetické bezpečnosti. S tím je spojená také povinnost na základě následujícího rozhodnutí Úřadu o registraci nahlásit a aktualizovat kontaktní údaje. Následně mají poskytovatelé jeden rok na to, aby implementovali veškeré povinnosti a bezpečnostní opatření, která po nich zákon vyžaduje podle režimu, do kterého služba spadá. Mezi ty patří například vymezení pracovních rolí, které se budou věnovat primárně kyberbezpečnosti nebo zajištění stanovené míry zabezpečení pro jejich interní komunikační síť.

Poté, co jsou ve společnosti zavedené veškeré požadované změny, nejpozději tedy do jednoho roku od registrace, vzniká poskytovatelům povinnost hlásit (v míře dle režimu, do kterého služba spadá) kybernetické bezpečnostní incidenty Úřadu a v případě nutnosti a možného ohrožení dodávek služby o nich také informovat své zákazníky.

NÚKIB má zároveň dle návrhu zákona informační povinnost vůči Evropské komisi v oblasti počtu registrovaných poskytovatelů regulovaných služeb, analýz kybernetických hrozeb a incidentů a dalších informací potřebných pro evropskou spolupráci v daném odvětví.

Jaké sankce budou hrozit za porušení těchto povinností?

Návrh zákona veškeré pravomoci v oblasti dohledu nad dodržováním povinností a jejich případné vymáhání svěřuje NÚKIB. Orgánem pro kontrolu jeho činnosti má být Poslanecká sněmovna.

Primárním způsobem nápravy mají být dle návrhu zákona tzv. nápravná opatření. Ty nastupují v případě, kdy Úřad poskytovatele upozorní na neplnění jemu uložených zákonných povinností a uloží mu způsob a lhůtu, do které má zjištěné nedostatky napravit. Nejedná se tedy primárně o sankci, ale spíše o postup, pomocí kterého může Úřad na společnosti působit. Naopak, nejčastěji užívanou sankcí za nesplnění povinností, které návrh zákona předpokládá, budou pokuty. Ty návrh zákona umožňuje až do výše 250 000 000 Kč nebo 2 % celosvětového ročního obrátu dané společnosti. Netýkají se však pouze společností, které služby poskytují, ale také jakékoliv fyzické osoby, která by například vystupovala ve funkci jednatele.

V krajních případech poté návrh zákona počítá s tzv. jinými správními tresty, které nejsou postaveny na finančních ztrátách. Jednou z nich je například pozastavení platnosti certifikace o kybernetické bezpečnosti, kterou poskytovatel potřebuje k poskytování služeb. Zcela nejzajímavější sankcí však bude možnost dočasného zákazu výkonu funkce člena statutárního orgánu. Uložení tohoto správního trestu však bude možné pouze u služeb v režimu vyšších povinností a za splnění určitých podmínek. Mezi ně patří zejména situace, kdy člen statutárního orgánu významně a/nebo opakovaně porušuje při výkonu své funkce povinnosti, což vede k nesplnění nápravného opatření, které Úřad společnosti uložil. Jako sankci tedy Úřad může výkon jeho funkce zakázat až do doby, kdy dojde k nápravě

nedostatků, zároveň však minimálně na šest měsíců. O uložení této sankce Úřad rozhoduje z úřední povinnosti, nelze o ni tedy požádat.

Shrnutí

Návrh zákona o kybernetické bezpečnosti představuje důležitý krok v posílení ochrany strategických služeb v České republice. K dosažení tohoto cíle zavádí rozsáhlý systém povinností pro poskytovatele služeb v klíčových odvětvích a zároveň umožňuje NÚKIB tyto povinnosti prostřednictvím komplexních sankčních mechanismů vymáhat. Přestože se návrh zákona nachází stále v legislativním procesu, je třeba, aby se jím dotčené subjekty začaly na změny v něm obsažené připravovat, neboť budou mít výrazný vliv na jejich dosavadní fungování.

Veronika Havlová

Weinhold Legal

Weinhold Legal, s.r.o. advokátní kancelář

Florentinum
Na Florenci 15
110 00 Praha 1

Tel.: +420 225 385 333
Fax: +420 225 385 444
e-mail: wl@weinholdlegal.com

[1] Ve smyslu doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků

© EPRAVO.CZ - Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- [Byznys a paragrafy, díl 32.: Konkurenční doložka](#)
- [Skryté ujednání v realitní smlouvě - zbytečná hra na schovávanou](#)
- [Odpovědnost člena voleného orgánu dle § 159 OZ a vymezení škody způsobené právnícké](#)

osobě

- Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu
- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše