5. 6. 2025

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

Nový zákon o kybernetické bezpečnosti: co se mění a jak se připravit?

Evropská směrnice NIS 2 přináší zásadní změny v oblasti kybernetické bezpečnosti a její transpozicí se mění i český právní rámec. Nový návrh zákona o kybernetické bezpečnosti zavádí dvoustupňovou regulaci poskytovatelů služeb, rozšiřuje okruh povinných osob a nově umožňuje státu hodnotit rizika v dodavatelském řetězci. Článek shrnuje, koho se nová pravidla týkají, jaké povinnosti firmám vzniknou a jaké dopady může mít nová úprava na jejich vnitřní fungování.

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, známá jako NIS 2, představuje reakci Evropské Unie na rostoucí kybernetická rizika a roztříštěnost národních pravidel v oblasti ochrany sítí a informačních systémů, resp. kybernetické bezpečnosti jako celku. Jejím cílem je posílit odolnost evropské digitální infrastruktury, zavést přísnější a jednotnější bezpečnostní standardy napříč členskými státy a rozšířit rozsah regulace na další odvětví a organizace, které jsou klíčové pro fungování společnosti a ekonomiky. Česká republika na tuto směrnici reaguje návrhem zcela nového zákona o kybernetické bezpečnosti, který nahradí dosavadní zákon č. 181/2014 Sb. a přinese širší okruh povinných subjektů, zavedení dvou režimů povinností podle velikosti a významu organizace, nové povinnosti v oblasti bezpečnosti dodavatelského řetězce a zpřísněné požadavky na řízení rizik a hlášení incidentů. Nová pravidla se tak budou vztahovat i na organizace, které dosud regulovány nebyly, a ty budou muset zavést odpovídající bezpečnostní opatření a zajistit soulad se zákonnými požadavky.

Na koho se nová pravidla budou vztahovat?

Návrh zákona o kybernetické bezpečnosti stanoví, že se nová pravidla vztahují na poskytovatele regulovaných služeb. Těmi jsou organizace, které současně splňují tři podmínky: působí v regulovaném odvětví (například v energetice, zdravotnictví, dopravě nebo v oblasti digitálních služeb), poskytují konkrétní regulovanou službu uvedenou ve vyhlášce o regulovaných službách a zároveň splňují tzv. podmínky významnosti, a to zejména s ohledem na svou velikost a případná další kritéria uvedená v této vyhlášce. Posouzení toho, zda jsou tyto podmínky naplněny, budou muset organizace provádět zpravidla samostatně, nicméně novela taktéž umožňuje, aby v případě pochybností rozhodl o zařazení konkrétního subjektu do regulace Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) ve správním řízení. Pokud budou splněny podmínky pro zařazení mezi regulované subjekty, bude poskytovatel zařazen buď do režimu vyšších, nebo nižších povinností podle svého ekonomického, společenského nebo bezpečnostního významu pro Českou republiku.

Jaké povinnosti novela kybernetického zákona přináší?

Regulovaným subjektům vzniká podle návrhu zákona soubor základních povinností, které jsou společné bez ohledu na to, zda spadají do režimu vyšších nebo nižších povinností. Patří mezi ně zejména ohlášení poskytované regulované služby, oznámení kontaktních údajů odpovědných osob, stanovení rozsahu řízení kybernetické bezpečnosti, zavedení přiměřených bezpečnostních opatření a hlášení kybernetických incidentů prostřednictvím portálu NÚKIB. V případě vydání reaktivních

opatření ze strany úřadu musí regulovaná organizace zajistit jejich včasné provedení. Pro zahájení hlášení incidentů a plnění povinností v oblasti bezpečnostních opatření platí přechodná lhůta v délce jednoho roku od doručení rozhodnutí o registraci regulované služby.

Nad rámec těchto základních povinností stanoví návrh zákona dva režimy regulace, a to režim vyšších povinností a režim nižších povinností. Rozsah a konkrétní podoba dalších povinností se mezi těmito režimy liší. Základním rozlišovacím kritériem, podle kterého je subjekt zařazen do jednoho z režimů, je zejména jeho velikost, přičemž platí, že pokud alespoň u jedné poskytované služby spadá do vyššího režimu, vztahuje se tento vyšší režim i na všechny ostatní regulované služby, které poskytuje. V režimu vyšších povinností se uplatňuje podrobnější katalog bezpečnostních opatření, incidenty se hlásí přímo NÚKIB a možné sankce zahrnují i opatření typu pozastavení certifikace nebo dočasného zákazu výkonu funkce člena statutárního orgánu. Subjekty v režimu nižších povinností mají mírnější rozsah požadavků a incidenty hlásí Národnímu CERT.

Kontrola dodavatelů a nové sankce: co novela umožňuje státu?

Vedle základních povinností přináší návrh zákona o kybernetické bezpečnosti také nová pravidla v oblasti bezpečnosti dodavatelského řetězce a posiluje pravomoci státu v oblasti dozoru a sankcí. Dodavatelský řetězec v oblasti kybernetické bezpečnosti zahrnuje zejména poskytovatele softwaru, hardwaru, cloudových služeb nebo jiných technologií, které regulovaná organizace používá pro provoz svých systémů. Poskytovatelé strategicky významných služeb budou nyní povinni aktivně posuzovat rizika u svých klíčových dodavatelů, vést o těchto dodavatelích evidenci a zajistit, že i jejich subdodavatelský řetězec splňuje požadavky zákona. Novinkou je i možnost státu (konkrétně NÚKIB nebo vlády) rozhodnout o omezení nebo zákazu používání konkrétní technologie, či dodavatele, pokud by jejich využití mohlo představovat závažné bezpečnostní riziko. Tyto zásahy se tak mohou dotknout i dříve běžných obchodních rozhodnutí soukromých firem. Zákon rovněž rozšiřuje systém dozoru, přičemž NÚKIB bude oprávněn provádět kontroly, ukládat nápravná opatření a v krajním případě i donucující opatření. Výše pokut se bude odvíjet od závažnosti porušení a režimu, do kterého regulovaný subjekt spadá. Ve vyšším režimu mohou sankce dosáhnout až 250 milionů Kč nebo 2 % z celosvětového ročního obratu, přičemž tímto obratem se rozumí součet tržeb všech propojených společností v rámci jednoho podniku. Sankce hrozí například za nezavedení bezpečnostních opatření, nehlášení incidentů nebo nesplnění rozhodnutí NÚKIB. Ani firmy v nižším režimu však nejsou mimo kontrolní rámec. I jim může být uložena pokuta až 175 milionů Kč nebo 1,4 % z celosvětového obratu, a to například za nesplnění základních oznamovacích povinností nebo neposkytnutí součinnosti při zvládání incidentů.

Jak správně zahájit přípravu na novou regulaci?

Po účinnosti zákona je na každé organizaci, aby samostatně posoudila, zda na ni dopadá nová právní úprava v oblasti kybernetické bezpečnosti. Pokud organizace zjistí, že splňuje podmínky regulovaného subjektu, měla by bez zbytečného odkladu podniknout první kroky k nastavení vnitřního systému řízení kybernetické bezpečnosti. Klíčové je v první fázi ohlásit regulovanou službu prostřednictvím Portálu NÚKIB, nahlásit kontaktní údaje odpovědných osob a stanovit rozsah řízení kybernetické bezpečnosti, tedy vymezit, jakých částí infrastruktury a činností se regulace týká. Pokud organizace tento rozsah nestanoví, má se za to, že se zákon vztahuje na celou její strukturu. Následně je třeba zahájit implementaci bezpečnostních opatření dle vyhlášky příslušné pro režim, do něhož je organizace zařazena, provést školení zaměstnanců, přizpůsobit interní dokumentaci a nastavit vnitřní systém oznamování a evidence incidentů. Ačkoliv samotná povinnost hlášení incidentů a implementace bezpečnostních opatření nabývá účinnosti až po uplynutí přechodné lhůty jednoho roku od doručení rozhodnutí o registraci regulované služby, je na místě s jejich přípravou začít co nejdříve. Vzhledem k rozsahu a komplexnosti nové právní úpravy je proto včasné zahájení přípravy na plnění zákonných povinností nezbytné pro všechny regulované subjekty bez ohledu na

zařazení do konkrétního režimu.

Compliance v kybernetické bezpečnosti jako konkurenční výhoda?

Zavedením nové právní úpravy kybernetické bezpečnosti se řízení kybernetických rizik stává zákonnou povinností pro širší okruh subjektů a zároveň i klíčovým prvkem důvěryhodnosti každé organizace, která spadá do rozsahu regulace. Regulované subjekty budou muset prokázat schopnost řídit kybernetická rizika, včas reagovat na incidenty a systematicky chránit svou digitální infrastrukturu. V praxi tak může správně nastavený systém kybernetické bezpečnosti fungovat jako konkurenční výhoda, a to jednak v očích zákazníků a obchodních partnerů, ale také i při účasti ve veřejných zakázkách, či při navazování nové obchodní spolupráce.

Závěrem lze říci, že novela zákona o kybernetické bezpečnosti nepřináší pouze nové povinnosti, ale představuje také jednu ze zásadních změn v řízení organizace. Veřejné i soukromé organizace spadající do rozsahu regulace tak budou muset kybernetickou bezpečnost začlenit do svých procesů s maximální vážností a odpovědností.

Mgr. Daniel Půlpán,
právník

JELÍNEK & PARTNEŘI
ADVOKÁTNÍ KANCELÁŘ

Advokátní kancelář JELÍNEK & Partneři s.r.o.

Pardubice - Dražkovice 181
533 33 Pardubice - Dražkovice

Truhlářská 1108/3
110 00 Praha 1

Tel.: +420 466 310 691
e-mail: advokati@advokatijelinek.cz

Další články:

- Nová „tlačítková" povinnost pro e-shopy
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Darování pro případ smrti nemovité věci zapsané v katastru nemovitostí a určení výše odměny soudního komisaře
- Flotilová novela: Kdo a kdy musí nově získat licenci k distribuci pojištění?

- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Právní due diligence nemovitostí: na co se v praxi skutečně zaměřit
- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie
- 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 právnické osobě
- Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu