5. 8. 2025

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

Směrnice NIS2 a zákon o kybernetické bezpečnosti: tak už jdeme do finále?

Evropská směrnice NIS2 a nový zákon o kybernetické bezpečnosti přinášejí pro obchodní společnosti zásadní změny v oblasti povinností v oblasti kybernetické bezpečnosti. Nová legislativa významně rozšiřuje okruh subjektů, na něž se povinnosti vztahují, zavádí detailnější požadavky na organizační a technická opatření a stanovuje přísnější sankce za jejich nedodržení. Protože legislativní proces aktuálně pokročil a došlo ke schválení zákona Sněmovnou a zákon zamířil ke schválení do Senátu, cílem tohoto článku je poskytnout přehled o aktuální situaci schvalovacího procesu a hlavních změn, které z nové právní úpravy vyplývají, a upozornit na kroky, které by měly podniky přijmout pro zajištění souladu s novými pravidly, protože se mohou obchodních společností týkat již od podzimu roku 2025.

Úvodem ke kybernetické bezpečnosti

Evropská unie musela vzhledem k rostoucímu počtu kybernetických hrozeb, jejich rostoucí složitosti a nebezpečnosti i přeshraniční charakter reagovat vydáním přísnější a aktuálnější právní regulace. Původní směrnice NIS1 již nepostačovala k zajištění dostatečné úrovně kybernetické bezpečnosti napříč členskými státy. Jak uvádí samotná směrnice (EU) 2022/2555, „nerovnoměrné provádění směrnice (EU) 2016/1148 vedlo k roztříštěnosti v přístupu k řízení kybernetických rizik a hlášení incidentů“[1].

Směrnice NIS2 přinesla sjednocení pravidel a výrazně zpřísňuje požadavky na řadu odvětví, včetně energetiky, dopravy, zdravotnictví, digitální infrastruktury, ale nově i na mnohé obchodní společnosti.

Nová pravidla a koho se vlastně týkají?

Zásadní změnou je rozšíření okruhu subjektů, na které se regulace vztahuje. Zatímco původní úprava dopadala převážně na tzv. poskytovatele základních služeb, nově se povinnosti vztahují na tzv. povinné osoby rozdělené do dvou kategorií:

- Základní povinné osoby – typicky větší podniky ze sektorů uvedených v příloze č. 1 zákona, např. energetika, doprava, bankovnictví, zdravotnictví, vodárenství apod.
- **Významné povinné osoby** – podniky z přílohy č. 2 zákona (např. pojišťovnictví, odpadové hospodářství, výzkum, výroba a distribuce chemikálií, potravinářství aj.), pokud splní určité velikostní kritérium (více než 50 zaměstnanců nebo obrat nad 10 milionů EUR).

Dle důvodové zprávy k zákonu o kybernetické bezpečnosti se předpokládá, že povinnosti dopadnou až na 6 000 subjektů v ČR[2] a tak se na ně podrobněji zaměříme níže:

Nový zákon klade důraz na proaktivní přístup ke kybernetické bezpečnosti.

Mezi klíčové povinnosti patří:

Zavedení bezpečnostních opatření – podniky musí implementovat technická a organizační opatření odpovídající míře rizika, mj. v oblasti řízení rizik, ochrany sítí a systémů, prevence incidentů, řízení přístupových práv, školení zaměstnanců apod.[3]

Hlášení incidentů – povinné osoby musí incidenty s významným dopadem hlásit NÚKIB bez zbytečného odkladu, nejpozději do 24 hodin od zjištění incidentu[4].

Vedení dokumentace – zákon požaduje vedení dokumentace o přijatých opatřeních, o provedených auditech a školeních.

Role vrcholového vedení – odpovědnost za kybernetickou bezpečnost nese statutární orgán společnosti a to bez ohledu na způsob, jakým deleguje tuto oblast v rámci struktury společnosti. Jeho povinností je zajistit dostatečné zdroje a dohled nad plněním požadavků.

ENISA doporučuje, aby zejména malé a střední podniky zahájily přípravu včas, a to prostřednictvím interního auditu a sestavení bezpečnostní strategie[5].

Jaké hrozí sankce a kdo má na starosti dohled?

Zákon posiluje pravomoci dozorového orgánu, kterým je Národní úřad pro kybernetickou bezpečnost – NÚKIB. V případě porušení povinností hrozí podnikům následující sankce:

- pokuta až do výše 10 milionů EUR nebo 2 % celkového ročního celosvětového obratu,
- v případě zvlášť závažného porušení až 250 milionů Kč dle § 52 zákona o kybernetické bezpečnosti[6].

Povinné osoby mají rovněž povinnost umožnit výkon kontroly, poskytovat součinnost a uchovávat dokumentaci po stanovenou dobu.

Doporučení pro praxi

Obchodním společnostem, na které se nová úprava vztahuje, doporučujeme, pokud tak již neučinily, zrealizovat následující kroky vedoucí ke splnění jejich povinností dle nového zákona:

- Zmapovat si, zda spadají do působnosti zákona, a to dle oboru činnosti a velikosti podniku.
- Provést audit stávajících procesů a systémů, identifikovat slabá místa.
- Vypracovat interní politiku kybernetické bezpečnosti a začlenit ji do řízení rizik.
- Zajistit si včas školení zaměstnanců a zavést postupy pro reakci na incidenty.
- Zajistit dostatečnou dokumentaci o provedených opatřeních.

Závěrem a k legislativnímu procesu

Nová úprava v oblasti kybernetické bezpečnosti přináší obchodním společnostem nejen nové povinnosti, ale i příležitost ke zvýšení své odolnosti vůči rostoucím kybernetickým hrozbám. Klíčovým předpokladem úspěchu je včasná příprava a zapojení vedení podniku do procesu zabezpečení informačních systémů.

Aktuálně je dobrou zprávou, že byl návrh zákona o kybernetické bezpečnosti schválen Poslaneckou sněmovnou 25. dubna 2025 a že Senát má na jeho projednání lhůtu do 12. června 2025. Od 16. května se rozběhl i navrhovací proces týkající se prováděcích vyhlášek. Je tedy v případě jistého optimistického úhlu pohledu možná předpokládat, že zákon nabude účinnosti možná již v říjnu roku 2025 a na tuto skutečnost se začít aktivně připravovat.

Mgr. Kristína Udržalová,
právnička

PADĚRA & PARTNEŘI s.r.o. advokátní kancelář

Svaté Anežky České 32
530 02 Pardubice

Tel.: + 420 773 240 555
E-mail: info@akprp.cz

Použité zdroje:

1. Směrnice (EU) 2022/2555 Evropského parlamentu a Rady ze dne 14. prosince 2022 o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v Unii (směrnice NIS2)

2 .Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti (sněmovní tisk č. 617/0, 2024)

3. ENISA: „Security Measures under the NIS2 Directive“, únor 2023

4. Zákon o kybernetické bezpečnosti, § 27 a násl. (verze po transpozici směrnice NIS2)

5. ENISA: „Cybersecurity Training Guide for SMEs“, 2023

6. Zákon o kybernetické bezpečnosti, § 52 odst. 1

7. NÚKIB: „NIS2 a co znamená pro české podniky“, dostupné >>> zde.

8. Sobek, T.: „Kybernetická bezpečnost v podnikové praxi“, DSM – Data Security Management, 1/2024

Další články:

- Pluralita vedoucích odštěpného závodu
- „Těžko na cvičišti, lehko na bojišti“, aneb proč je kvalitní prodejní dokumentace klíčová (nejen) v automotive segmentu

- Územní plán jako klíčový faktor při oceňování pozemků
- Výpis z německého živnostenského rejstříku – kdy ho můžete potřebovat a kde a jak jej získat
- Aktuality ze světa nekalé soutěže
- Podíly pro zaměstnance v obchodních společnostech
- Evidence skutečných majitelů se uzavírá veřejnosti
- Transfer Pricing: Na co si dát pozor s blížícím se koncem roku
- Byznys a paragrafy, díl 24.: Digitalizace korporátního práva: EU cílí na snížení administrativy při přeshraničním podnikání
- Oceňování ochranných známek
- Zákon o prověřování zahraničních investic v kontextu nových návrhů Evropské komise