23. 7. 2024

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

Stav regulace kybernetické bezpečnosti v České republice ve světle probíhající transpozice NIS 2: Úvod

Směrnice NIS2[1] je přelomovým evropským právním předpisem v oblasti kybernetické bezpečnosti, který má významný dopad na postupy a povinnosti evropských společností v oblasti kybernetické bezpečnosti. Dalším důležitým evropským právním předpisem v oblasti kybernetické bezpečnosti je nařízení o digitální provozní odolnosti (Digital Operational Resilience Act, DORA), které zavádí harmonizovaný rámec pro dohled a dozor nad řízením rizik v oblasti informačních a komunikačních technologií ze strany finančních institucí a poskytovatelů služeb IKT z řad třetích stran. Podrobnější informace o rozsahu a důsledcích nařízení DORA uvedeme v samostatném přehledu.

Česká republika je průkopníkem v oblasti regulace kybernetické bezpečnosti s vlastním specializovaným zákonem, nicméně pro sladění s požadavky NIS2 se národní zákonodárci rozhodli přijmout zcela nový **zákon o kybernetické bezpečnosti** (dále jen "**Zákon**"), který se v současné době nachází v legislativním procesu a měl by vstoupit v platnost ve druhé polovině letošního roku[2].

Tento článek slouží jako úvod pro nadcházející sérii článků týkajících se regulace kybernetické bezpečnosti, jejímž cílem bude v prvé řadě seznámit čtenáře se základními parametry chystaného Zákona, udržet jej v obraze během legislativního procesu a – jakmile budou známy jeho přesné parametry, blíže představit konkrétní povinnosti.

Jaké hlavní změny Zákon zavádí?

Rozšířená oblast působnosti

Oproti současnému právnímu rámci Zákon významně rozšíří okruh regulovaných subjektů v oblasti kybernetické bezpečnosti, která bude nově dopadat na nová odvětví a zároveň rozšíří ta již pod regulaci spadající. V důsledku toho se odhaduje, že počet regulovaných subjektů (v návrhu Zákona zatím označovaných jako poskytovatelé regulované služby) v České republice výrazně vzroste, a to ze současných přibližně 300 subjektů na odhadem až 12 000, především z řad velkých a středních podniků.

Poskytovatelé regulované služby budou muset tuto tzv. regulovanou službu sami identifikovat Úřadu, v opačném případě může Úřad rozhodnout z moci úřední. Poskytovatelé regulované služby budou podle své velikosti, počtu uživatelů či jiných kritérií, dále stanovených prováděcí vyhláškou, spadat do režimu **vyšších** nebo **nižších** povinností.

Mezi regulovaná odvětví patří (neúplný výčet):

- **energetika**; elektřina, ropa, zemní plyn, vodík.
- **doprava**; letecká, železniční, vodní, silniční;
- **bankovnictví**;

- **infrastruktura finančního trhu;**
- **zdravotnictví**;
- **digitální infrastruktura**;
- **vesmír**
- **Výroba, produkce a distribuce chemických látek;**
- **Výroba, zpracování a distribuce potravin;**
- **Výroba**; zdravotnických prostředků, počítačů, elektronických a optických přístrojů a zařízení, motorových vozidel aj.;
- **digitální poskytovatelé;**
- **výzkum**.

Základní povinnosti

Návrh Zákona navazuje na stávající pravidla a NIS2 a ukládá poskytovatelům regulovaných služeb soubor základních povinností, kolem nichž jsou strukturována zvláštní pravidla, a to:

1. hlášení (kontaktních) údajů;
2. zavádění a provádění bezpečnostních opatření;
3. hlášení kybernetických bezpečnostních incidentů;
4. provádění protiopatření; a
5. stanovení rozsahu řízení kybernetické bezpečnosti.

Návrh Zákona, respektive jeho prováděcích vyhlášek rovněž počítá se zvýšením odpovědnosti a zavádění nových povinností pro osoby ve vrcholném vedení společností, školení zaměstnanců či zavedení bezpečnostních rolí jako manažer či architekt kybernetické bezpečnosti, což s sebou přinese nároky na nábor nových pracovních sil. V neposlední řadě zákon zavede nové požadavky na bezpečnost v dodavatelském řetězci za účelem prověřování rizik spojených s dodavateli poskytovatelů strategicky významných služeb.

Jak je již u transpozic zásadních směrnic EU obvyklé, návrh Zákona rovněž počítá se zavedením nových a vyšších forem sankcí, včetně pokut počítaných podle celosvětového obratu podniku. Vzhledem k vysoké celoevropské prioritě kybernetické bezpečnosti se navíc očekává, že Úřad, sám usilující o značné dozorové pravomoci, bude na plnění povinností Zákona důsledně dohlížet, včetně provádění šetření na místě, tzv. dawn raidů.

Co by nyní měla každá společnost udělat?

Očekává se, že konkrétní povinnosti podle Zákona začnou na společnosti dopadat v průběhu roku 2025, nicméně je na místě, aby každá (česká) společnost důsledně sledovala vývoj právní regulace. Již nyní, ještě před vstupem Zákona v platnost, lze provést předběžné posouzení, zda a do jaké míry se nová pravidla příslušné společnosti dotknou.

Vzhledem k tomu, že Zákon zavede pro mnoho společností nové povinnosti, a dosažení souladu s ním si vyžádá značný čas a zdroje, doporučujeme též včas vyčlenit dostatečné zdroje a zajistit poradenskou podporu – jak technického, tak právního charakteru.

Sebastian Špeta

Martin Svoboda

schönherr
ADVOKÁTNÍ KANCELÁŘ

Schönherr Rechtsanwälte GmbH, organizační složka
Jindřišská 937/16
110 00 Praha 1

Tel.: +420 225 996 500
Fax: +420 225 996 555
e-mail: se.speta@schoenherr.eu
e-mail: ma.svoboda@schoenherr.eu

---

[1] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii.

[2] Ke dni publikace tohoto článku byl návrh zákona připravený Národním úřadem pro kybernetickou a informační bezpečnost (dále jen "Úřad") schválen Vládou k předložení do Poslanecké sněmovny Parlamentu České republiky.

Další články:

- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků
- Evropská unie mění pravidla plateb: více odpovědnosti, intenzivnější zpracování dat, více kontrol
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Novinky z české a evropské regulace finančních institucí za měsíc květen 2026
- Sport versus EU – aktuální sportovní kauzy rozhodované Soudním dvorem EU
- Postavení finančního arbitra v kontextu nařízení Brusel I bis - Funkční pojetí „soudu“, osvědčení podle čl. 53 a možnost výkonu nálezu v jiných členských státech EU
- ESG Simple jako praktická opora pro ESG reporting malých a středních podniků
- Novinky z české a evropské regulace finančních institucí za měsíc duben 2026
- Dvě kiwi denně: EU schválila první zdravotní tvrzení pro čerstvé ovoce
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor