Obce a kybernetická bezpečnost

právo s nadhledem

www.iora.cz

Směrnice NIS2

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

Směrnice NIS2 byla dne 27. prosince 2022 zveřejněna v Úředním věstníku Evropské unie. Publikovaná podoba směrnice NIS2 je oficiální a nebude se již dále měnit.

Směrnice není na území ČR přímo aplikovatelná, tj. není způsobilá přímo vytvářet práva a povinnosti pro fyzické či právnické osoby.

Transpozice do 17.10.2024

Nová legislativa ke kybernetické bezpečnosti

Stávající zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů – v naprosté většině případů nestanoví žádné povinnosti pro obce, povinnosti jsou vázány na tvz. kritickou infrastrukturu

Návrh nového zákona o kybernetické bezpečnosti v návaznosti na směrnici NIS2 již pracuje s konceptem tzv. poskytovatele regulované služby

Nový zákon dosud není schválen a tudíž nevyvolává žádné povinnosti. Očekává se schválení v první polovině 2024

Prováděcí právní předpisy – gestor NUKIB

Vazba na velikost povinného subjektu, obvykle pouze pokud je středním nebo velkým podnikem, tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK)

Poskytovatel regulované služby

Veřejná správa
poskytovatel regulované služby v režimu vyšších povinností:
krajem,
hlavním městem Praha, nebo
obcí s rozšířenou působností s nejméně 125 000 obyvateli
poskytovatel regulované služby v režimu nižších povinností
obcí s rozšířenou působností s počtem obyvatel do 125 000
Jiné oblasti s dopadem na obce
Výroba tepelné energie
Provoz soustavy zásobování tepelnou energií
Provozování vodovodu
Provozování kanalizace
Provoz zařízení určeného pro nakládání s odpady
Přeprava odpadu
Poskytování zdravotní péče

Pokud jeden subjekt poskytuje služby v obou režimech, uplatní se přísnější režim na veškerou činnost
Nutnost registrace

Povinnosti poskytovatele regulované služby

- Hlásit údaje – jak definuje Vyhláška o portálu NÚKIB
- Stanovit rozsah řízení kybernetické bezpečnosti – definuje scope bezpečnosti
- Zavádět bezpečnosti opatření – podle režimu v kterém je služba určena
- Hlásit kybernetické bezpečnostní incidenty
- Informovat zákazníky o incidentech a hrozbách
- Provádět protiopatření
- Plnit povinnosti z Mechanismu řízení bezpečnosti dodavatelského řetězce
- Podřídit se výkonu kontroly inspektorem

Bezpečnostní opatření se zavádí do jednoho roku od registrace regulované činnosti, jsou organizačního a technického charakteru.

Bezpečnostní opatření

•bezpečnostní opatření dělíme na organizační a technická

•**organizačními opatřeními poskytovatele regulované služby v režimu nižších povinností jsou:** zajišťování minimální úrovně kybernetické bezpečnosti, povinnosti vrcholového vedení, bezpečnostní role, řízení bezpečnostní politiky a dokumentace, řízení aktiv, řízení dodavatelů, bezpečnost lidských zdrojů, řízení změn, akvizice, vývoje a údržby, řízení přístupů, zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, řízení kontinuity činností

•**technickými opatřeními poskytovatele regulované služby v režimu nižších povinností jsou:** fyzická bezpečnost, bezpečnost komunikačních sítí, správa a ověřování identit, řízení přístupových oprávnění, detekce kybernetických bezpečnostních událostí, zaznamenávání bezpečnostních a relevantních provozních událostí, aplikační bezpečnost, kryptografické algoritmy, zajišťování dostupnosti regulované služby a zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Řízení dodavatelů a veřejné zakázky

Povinnost poskytovatelů regulované služby zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele a požadavky dát do smluv

Zohlednění bezpečnostních opatření není překážkou/omezením hospodářské soutěže podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek

Informace, které by mohly narušit kybernetickou bezpečnost organizace nejsou sdělovány dle zákona č. 106/1999 Sb., o svobodném přístupu informacím

Kontroly dodržování povinností

U poskytovatelů **regulovaných služeb v režimu vyšších povinností** bude kontroly i nadále provádět NÚKIB prostřednictvím svých zaměstnanců. Kontroly u poskytovatelů regulovaných služeb **v režimu nižších povinností budou prováděny tzv. inspektory**. Poskytovatel nižších regulovaných služeb má povinnost si kontrolu v pravidelném intervalu zajistit a také uhradit. „Osoba vykonávající funkci inspektora bude muset splňovat podmínky vymezené navrhovaným zákonem a navazující vyhláškou o inspektorech a obdržet od NÚKIB odpovídající autorizaci k výkonu kontrolní činnosti.”

Nespadáte do režimu regulovaných služeb?

Jako výchozí krok lze doporučit především zmapováním aktuálního stavu v obci (tzn. audit aktuálního stavu kybernetické bezpečnosti a potenciálních slabých míst) a vypracováním business impact analýzy (zejm. jaké by byly dopady narušení řádného fungování jednotlivých systémů na vaši obec; nejde přitom jen o nedostupnost používaných informačních systémů, ale i o narušení důvěrnosti nebo integrity shromažďovaných dat (možná vazba na jiné předpisy např. GDPR).

Je vhodné se rovněž zaměřit na školení relevantních osob v obci – základní školení pro všechny uživatele, odborné školení pro osoby, které v obci řeší/budou řešit kybernetickou bezpečnost, nezapomínat přitom i na vrcholný management (management si musí být vědom důležitosti řízení kybernetické bezpečnosti v obci).

NUKIB vydal metodické doporučení „Minimální bezpečnostní standard, podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti“, který je možné využít jako východisko pro další kroky.

Zdroje

https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=CS

https://osveta.nukib.cz/course/view.php?id=145

https://www.denmalychobci.cz/file/dmo/prezentace/57/henik_nukib.pdf

https://arion.cz/nis2-novy-zakon-o-kyberneticke-bezpecnosti/

https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/

Děkuji za pozornost

petr@iora.cz