****

V Praze dne 6. června 2025

Č. j. 3198/2025-NÚKIB-E/110

|  |  |
| --- | --- |
| **Název materiálu:** | **Návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností** |
| **Připomínkové místo:** | **Asociace malých a středních podniků a živnostníků ČR (AMSP ČR)** |
| **Telefon:** | **+420 737 518 056** |
| **e-mail:** | [amsp@amsp.cz](mailto:amsp@amsp.cz) , [pravni@amsp.cz](mailto:pravni@amsp.cz) |
| **Kontaktní osoba:** | Mgr. Andrea Buchtová |

**Připomínky k Vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností**

1. **Odstranění požadavků**

**Cíl:** Odstranit požadavky na vzdělání a praxi manažerů kybernetické bezpečnosti, totéž v případě auditorů a architektů KB, a to včetně přílohy č. 5.

**Odůvodnění:** Vzhledem k tomu, že počet regulovaných osob v režimu vyšších povinností bude oproti současnému stavu několikanásobně vyšší, vznikne akutní potřeba velkého množství manažerů kybernetické bezpečnosti. Tito odborníci budou potřební prakticky okamžitě, neboť budou muset nastavit pravidla kybernetické bezpečnosti u tisíců nově regulovaných subjektů.

Zatímco NÚKIB odhaduje počet dotčených subjektů na přibližně 1 500, domníváme se, že tento počet bude výrazně vyšší. Do režimu vyšších povinností mohou totiž nově spadat také holdingy menších a středních podniků, které naplní kritéria obratu a počtu zaměstnanců souhrnně. Takové údaje přitom nelze z veřejných zdrojů spolehlivě ověřit a lze předpokládat, že takových subjektů budou ve výsledku stovky.

Regulace v režimu vyšších povinností se tak může vztahovat i na řadu malých a středních podniků, které jsou součástí širší podnikové struktury.

Rozumíme požadavku úřadu, aby subjekty v režimu vyšších povinností měly ve svých řadách zkušené odborníky. Nicméně v rozsahu, v jakém je nový zákon vyžaduje, tito specialisté reálně na trhu práce neexistují. Čím více formálních požadavků bude na tyto role kladeno přímo ve vyhlášce, tím větší riziko vzniká, že především střední podniky, velké podniky, pro něž je regulovaná služba jen okrajovou činností, nebo holdingy složené z menších firem nebudou schopny tyto odborníky vůbec zajistit.

Je zřejmé, že motivací většiny subjektů bude obsazení těchto pozic kvalifikovanými lidmi – ať už interně, nebo formou outsourcingu od specializovaných firem s doložitelnou praxí. Riziko však spočívá v tom, že v okamžiku účinnosti zákona vznikne extrémní tlak na trh práce, kdy budou všechny regulované subjekty najednou poptávat stejný typ kvalifikace. Tato situace je vysoce pravděpodobná, a přesto nebyla v rámci RIA adekvátně zohledněna, ačkoliv na to opakovaně upozorňovala řada připomínkových míst.

Za této situace považujeme za naprosto nezbytné **zmírnit formální požadavky na tyto role ve vyhlášce**, aby vůbec bylo možné požadavky zákona naplnit v praxi.

1. **Protiopatření podle § 20 zákona**

**Cíl:** Protiopatření podle § 20 odst. 1 a) a c) zákona

**Odůvodnění:** Z povahy samotného nástroje „Varování“ a také na základě jeho názvu je zřejmé, že nemá sloužit jako povinný vstup do hodnocení rizik. Důvodová zpráva k zákonu jasně uvádí, že Varování není transpozičním nástrojem podle směrnice NIS2 – tuto funkci plní pouze Výstraha a Reaktivní protiopatření.

Zavedení povinnosti pro všechny subjekty v režimu vyšších povinností, aby Varování zohledňovaly ve svém hodnocení rizik, tak představuje gold plating – tj. nadbytečné rozšíření povinností nad rámec požadavků evropské legislativy. Tato povinnost by proto měla být z návrhu zcela vypuštěna.

Je nutné zdůraznit, že úřad již podle návrhu zákona získává nové a významné pravomoci nad rámec směrnice NIS2 v rámci Mechanismu prověřování bezpečnosti dodavatelského řetězce. V jeho rámci může být Varování využito jako jedno z opatření obecné povahy, určené poskytovatelům strategicky významných služeb. Tento mechanismus považujeme za dostatečný a proporcionální k dosažení cíle, aniž by bylo nutné plošně zatěžovat všechny regulované subjekty další povinností.

1. **Změna doby uchovávání**

**Cíl:** Změna na následující znění – uchovává záznamy těchto událostí alespoň po dobu 6 měsíců.

**Odůvodnění:** Návrh stanoví nepřiměřeně dlouhou dobu pro uchovávání údajů. Odůvodnění uvedené v důvodové zprávě není nijak podloženo konkrétními daty, analýzami ani odkazy na relevantní zdroje, a tudíž není možné jeho závěry nezávisle ověřit.

Úřad sice v důvodové zprávě uvádí, že „účelem tohoto ustanovení není povinnost uchovávat všechny logy ze všech technických aktiv po dobu 18 měsíců“, a dále tvrdí, že by mělo dojít k individuálnímu posouzení, jaké záznamy budou podle § 23 a po jakou dobu uchovávány. Zároveň však deklaruje, že 18 měsíců je výchozí hodnota, od které se lze odchýlit pouze na základě „řádného odůvodnění“ opřeného o výstupy systému řízení bezpečnosti informací a o bezpečnostní potřeby dané organizace.

Takto formulované ustanovení bude mít v praxi efektivně stejný dopad, jako by šlo o plošně závaznou minimální dobu pro uchovávání veškerých logů. Žádná organizace totiž nebude chtít riskovat, že její vlastní posouzení bude při případné kontrole ze strany úřadu shledáno nedostatečným, a že jí v důsledku hrozí sankce. To povede k preventivnímu uchovávání veškerých záznamů po dobu minimálně 18 měsíců – bez ohledu na jejich význam či potřebu – což je ekonomicky i provozně neúnosné, zejména pro malé a střední podniky.

Z těchto důvodů navrhujeme buď zkrácení této doby, nebo formulaci právního předpisu takovým způsobem, který neukládá faktickou povinnost, ale skutečně umožňuje individuální a přiměřené vyhodnocení podle typu záznamů, míry rizik a charakteru organizace.