Becker
Becker & Poliakoff
advokátní kancelář

Kybernetická bezpečnost

Od 1. listopadu 2025 vstoupil v účinnost nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti („NZKB“). Jde o největší změnu v regulaci kybernetické bezpečnosti za poslední dekádu a její dopady budou cítit napříč celým českým hospodářstvím. Zákon implementuje evropskou směrnici NIS2 a zároveň ruší dosavadní právní rámec, který fungoval od roku 2014. Tím končí tedy i systém, kdy Národní úřad pro kybernetickou a informační bezpečnost („NÚKIB“) sám určoval okruh regulovaných subjektů. Nově je odpovědnost za určení povinností přenesena přímo na jednotlivé organizace, každá firma, úřad či instituce musí sama posoudit, zda spadá do regulace.

Do konce roku 2025 (tedy do 60 dnů od účinnosti zákona) musí každá organizace povinně provést tzv. sebeidentifikaci, zaregistrovat své regulované služby v portálu NÚKIB a přezkoumat své stávající procesy. Následně má 12 měsíců na plnou implementaci bezpečnostních opatření, revizi interních směrnic, plánů reakce na incidenty a úpravu smluv s dodavateli. Celý proces je časově i finančně náročný proto doporučujeme nečekat a začít ihned.

Regulované služby: základ sebeidentifikace

Současně s NZKB vstoupila v účinnost řada vyhlášek NÚKIB, které podrobně upravují povinnosti jednotlivých organizací. Vyhláška NÚKIB č. 408/2025 Sb., o regulovaných službách, obsahuje detailní seznam služeb, které podléhají zákonu, a stanovuje kritéria, podle nichž se poskytovatel musí sám identifikovat. Regulace zasahuje celkem osmnáct sektorů, od energetiky, dopravy a zdravotnictví až po digitální infrastrukturu, cloudové služby nebo finanční technologie. Vyhláška tak umožňuje organizacím určit, zda jsou poskytovateli regulované služby a zda spadají do režimu tzv. vyšších či nižších povinností.

Vyšší a nižší povinnosti: dvě úrovně bezpečnosti

Jakmile organizace zjistí, že je poskytovatelem regulované služby, musí splnit registrační povinnost vůči NÚKIB

a připravit se na implementaci bezpečnostních opatření. Jejich obsah není univerzální, liší se podle toho, zda je služba zařazena do režimu tzv. vyšších nebo nižších povinností. Pro režim vyšších povinností platí vyhláška NÚKIB č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, která ukládá rozsáhlé technické, organizační i procesní požadavky. Mezi ně patří např. formalizované řízení rizik, podrobná bezpečnostní dokumentace, kontinuální monitorování, pokročilé šifrovací standardy, pravidelné penetrační testování nebo řízení privilegovaných přístupů. Tento režim dopadá zejména na poskytovatele služeb, jejichž narušení by mohlo mít závažný dopad na fungování společnosti nebo státu.

Pro méně kritické služby je určen režim nižších povinností, upravený vyhláškou NÚKIB č. 410/2025 Sb, o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. Ta stanovuje především minimální požadavky na bezpečnostní politiku, základní systém řízení rizik, pravidelná školení, řízení přístupů, zálohování nebo postup obnovy po incidentu. I když jde o mírnější režim, jeho požadavky představují oproti stávající praxi významné posílení bezpečnostních standardů ve firmách, ale zároveň i vyšší administrativní, personální a finanční zátěž.

Přísnější pravidla hlášení incidentů a sankce za nedodržení

NZKB rovněž zavádí přísnější pravidla pro hlášení incidentů. Významné bezpečnostní incidenty bude nutné oznámit do 24 hodin, všechny ostatní do 72 hodin. Vyhlášky 409/2025 a 410/2025 Sb. zároveň určují, jak se významnost incidentu posuzuje a jak má být hlášení strukturováno. Odpovědnost za splnění povinností nese nejen samotný poskytovatel regulované služby, ale i jeho statutární orgány. Těm hrozí osobní sankce až do výše deseti milionů korun. Právnickým osobám pak může být uložena pokuta až 200 milionů korun nebo čtyři procenta celosvětového obratu, podle toho, která částka bude vyšší.

Kyberbezpečnost dodavatelů pod kontrolou

Velká pozornost se nově věnuje také bezpečnosti dodavatelského řetězce. Vyhláška č. 408/2025 Sb. ukládá poskytovatelům povinnost identifikovat významné dodavatele a posuzovat jejich bezpečnost. Vyhlášky č. 409/2025 a 410/2025 Sb. pak stanovují konkrétní požadavky na smlouvy, auditní práva či sdílení bezpečnostních informací. Firmy tak budou muset důkladně prověřit například poskytovatele cloudových služeb, dodavatele informačních technologií nebo externí správce bezpečnostních řešení.

Co to znamená v praxi?

Ještě v průběhu roku 2025 by měla každá organizace provést tzv. sebeidentifikaci podle vyhlášky č. 408/2025 Sb., přezkoumat své procesy a porovnat je s požadavky příslušné vyhlášky o bezpečnostních opatřeních, ať už v režimu vyšších nebo nižších povinností. Následovat by měla revize interních směrnic, aktualizace plánů reakce na incidenty, úprava smluv s dodavateli a včasná registrace poskytované regulované služby v systému NÚKIB. Implementace všech povinností může zabrat měsíce, a proto je vhodné začít co nejdříve.

Naše advokátní kancelář se problematice kybernetické bezpečnosti, implementaci NIS2 i samotného NZKB věnuje. Pomáháme klientům s kompletním procesem – od prvotní sebeidentifikace přes přípravu registrace v IS NÚKIB až po tvorbu bezpečnostních politik, smluvních dokumentů a zastupování při kontrolách. NZKB není jen další administrativní povinností, ale příležitostí výrazně zvýšit bezpečnost a odolnost vaší organizace. Pokud si chcete být jistí, že budete připraveni včas a správně, rádi vám pomůžeme.