20. 4. 2023

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

Vybrané novinky v kybernetické bezpečnosti podle NIS2

Dne 14. prosince 2022 byla schválena směrnice Evropského parlamentu a Rady (EU) 2022/2555 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“)[1]. Směrnice NIS 2 má být jednotlivými členskými státy EU implementována nejpozději s účinností od 18. října 2024.

Na úrovni České republiky spadá Směrnice NIS 2 do gesce Národního úřadu pro kybernetickou bezpečnost („**NUKIB**“), který se na vydání Směrnice NIS 2 již předem připravoval. Již v lednu 2023 spustil NUKIB internetové stránky >>> zde, kde na jednom místě v ucelené podobě publikoval první návrh nového zákona o kybernetické bezpečnosti („**NZKB**“) a související prováděcí vyhlášky. Zhruba do poloviny března 2023 měla veřejnost možnost zasílat NUKIB jakékoli připomínky k NZKB. Ambicí NUKIB je, aby NZKB prošel legislativním procesem a nabyl platnosti již v polovině roku 2024.

NA KOHO NZKB DOPADNE?

První zásadní změnou je osobní působnost Směrnice NIS 2 a NZKB. Podle odhadů NUKIB a dalších odborníků Směrnice NIS 2 dopadne na 6.000 až 10.000 subjektů v České republice. V porovnání se stávajícím zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů („**SZKB**“) se jedná o zcela neporovnatelný rozsah. NZKB dopadne na poskytovatele regulovaných služeb („**povinné osoby**“) v celkem 18 odvětvích, přičemž povinné osoby se budou řadit do dvou kategorií.[2] První kategorie jsou povinné osoby v režimu vyšších povinností (tzv. *essentials*), které jsou považovány za kritické z pohledu státu na zajištění kybernetické bezpečnosti. Povinným osobám v režimu vyšších povinností budou stanoveny mj. rozšířené povinnosti a výlučně na ně budou dopadat některé specifické sankce (vizte dále). Druhou – bezesporu rozšířenější – kategorií budou povinné osoby v režimu nižších povinností (tzv. *important*), pro které platí o něco menší rozsah povinností a nižší sankce, a také se na ně neuplatní některé specifické sankční mechanismy.[3]

Povinné osoby podléhají registrační povinnosti u NUKIB. Všichni poskytovatelé regulované služby budou povinně hlásit své registrační a kontaktní údaje za účelem vedení jejich evidence a další údaje, které si NÚKIB důvodně vyžádá.

JAKÉ NOVÉ POVINNOSTI NZKB PŘINESE?

Celkový rozsah povinností se bude rozlišovat podle typu povinného subjektu. Subjekty v režimu vyšších povinností budou například povinny provádět pravidelné audity kybernetické bezpečnosti. Všechny povinné osoby budou muset dále zajišťovat pravidelná školení a osvětu osobám ve vrcholovém vedení za účelem prohlubování znalostí o kybernetické bezpečnosti.

Další podstatnou oblastí jsou mechanismy kontroly dodavatelského řetězce povinných osob. NZKB například výslovně dává povinným osobám spadajícím do působnosti zákona o zadávání veřejných zakázek možnost stanovit specifické požadavky na dodavatele, které nemohou být považovány za omezení hospodářské soutěže. Povinné osoby jsou povinny zajistit bezpečnost celého dodavatelského

řetězce. Povinné osoby dále musí pravidelně provádět hodnocení celkové kvality produktů a praktik v oblasti řízení dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje. NZKB dále nově zavádí kategorii tzv. významného dodavatele[4]. NUKIB v určitých případech uloží rozhodnutím povinnosti přímo významnému dodavateli, a to za účelem předložení data a informací v souvislosti s hrozícím nebo nastalým kybernetickým bezpečnostním incidentem. Tím se de jure rozšiřuje působnost NZKB nad rámec povinných osob i na osoby v dodavatelském řetězci povinné osoby.

Ve vztahu k bezpečnostně významným dodávkám dává NZKB možnost, aby NUKIB formou opatření obecné povahy a za účelem ochrany před ohrožením bezpečnosti ČR zakázal využití plnění konkrétního dodavatele. NZKB nestanoví časové omezení takového zákazu, ale pouze ukládá NUKIB jednou za tři roky přezkoumat, zda důvody pro vydání opatření obecné povahy nadále trvají.

NUKIB dále klade zesílený důraz na přijetí bezpečnostních opatření ze strany povinných osob.[5]

ZESÍLENÉ PRAVOMOCI NUKIB

NZKB významně rozšiřuje aktivní pravomoci samotného NUKIB bez vazby na další státní orgány.

Nejpatrnější je tento posun viditelný při stavu kybernetického nebezpečí. Stav kybernetického nebezpečí může ředitel NÚKIB nově samostatně vyhlásit až na 30 dní (podle SZKB jen na 7 dnů), přičemž tuto dobu lze se souhlasem vlády opakovaně prodloužit (podle SZKB byla maximální doba omezena na 30 dnů). NUKIB může (i) uložit povinnosti nejen povinným osobám, ale všem subjektům stojícím mimo rámec NZKB, (ii) nařídit práci v pohotovostním režimu, (iii) nařídit provedení skenu zranitelností nebo penetračního testu, nebo (iv) nařídit orgánům a osobám zpřístupnění neveřejných komunikačních sítí v jejich správě.

NUKIB může také formou vyhlášky stanovit osobám v režimu vyšších povinností nutnost zajistit, že určitá data a informace budou zpracovány jen výlučně na vymezeném území (například v ČR nebo EU).

VYBRANÉ SANKČNÍ MECHANISMY

V NZKB dochází k významnému nárustu maximální výše pokut za spáchané přestupky. Oproti SZKB kde byla maximální výše pokuty stanovena na 5.000.000 Kč, činí horní hranice pokuty za nejzávažnější přestupky povinných osob v režimu vyšších povinností až 250.000.000 Kč nebo 2 % ze světového obratu (co je vyšší). Pro povinné osoby v režimu nižších povinností pak činí horní hranice 175.000.000 Kč nebo 1,4 % ze světového obratu (co je vyšší).

Ve vztahu k povinným osobám v režimu vyšších povinností pak může příslušný soud na návrh NUKIB rozhodnout o pozastavení výkonu řídící funkce[6], a to na dobu nejméně 6 měsíců, pokud v důsledku provedené kontroly NUKIB zjistil závažné nebo opakované porušení povinností při výkonu řídící funkce spočívající v neodstranění nedostatků zjištěných při kontrole.

ZÁVĚR

Bez nadsázky lze říci, že NZKB přináší **revoluci** v oblasti kybernetické bezpečnosti. Nově dopadne na tisíce subjektů, kteří budou muset v horizontu necelých dvou let provést zásadní organizační a technické změny ve svých společnostech za účelem posílení své kybernetické bezpečnosti, aby plně dostály povinnostem podle NZKB. Ačkoli lze očekávat přiměřeně dlouhou legisvakanci, větší podniky a organizace by změny a připravenost na nové povinnosti měly zahájit již nyní. Personální, právní a finanční náklady na zajištění souladu s NZKB budou dosahovat milionů až stovek milionů korun u těch největších podniků.

Mgr. Tomáš Kessler,
advokát

GLATZOVA & Co.

GLATZOVA & Co., s.r.o.

Betlémský palác
Husova 5
110 00 Praha 1

Tel.: +420 224 401 440
Fax: +420 224 248 701
e-mail: office@glatzova.com

---

[1] Publikována v Úředním věstníku EU byla 27. prosince 2022.

[2] Kategorizace je uvedena v příloze I. a II. Směrnice NIS a v prováděcí vyhlášce NUKIB o regulovaných službách.

[3] Základním dělícím kritériem bude velikost podniku. Pro zjednodušení lze říci, že velké podniky v regulovaných oblastech budou spadat do režimu vyšších povinností a střední podniky do režimu nižších povinností.

[4] Pro účely NZKB se „významným dodavatelem“ rozumí každý, kdo s poskytovatelem regulované služby vstupuje do právního vztahu, který je významný z hlediska stanoveného rozsahu řízení kybernetické bezpečnosti.

[5] Bezpečnostní opatření se dělí na technická a organizační opatření a jejich podrobná specifikace bude uvedena v prováděcí vyhlášce o bezpečnostních opatřeních.

[6] Tj. člen statutárního orgánu, vedoucí odštěpného závodu, prokurista nebo podnikající fyzická

osoba.

Další články:

- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25
- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti
- Detekce podezřelého obchodu v kontextu hazardních her
- AI omnibus