3. 7. 2025

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

Ne/podceňování zastupitelnosti bezpečnostních rolí dle zákona o kybernetické bezpečnosti

Řada společností, které již ví, že se zařadí mezi poskytovatele regulovaných služeb, v tuto chvíli bohužel netuší, že zákon o kybernetické bezpečnosti (dále jen „ZKB“), zavádí u poskytovatelů regulované služby vysoké pokuty za nezajištění zastupitelnosti kontaktních osob. V článku se tedy čtenář dozví, jaké údaje má poskytovatel regulované služby NÚKIBU hlásit, jaké jsou sankce za nesplnění zákonných povinností, kdo může vykonávat jednotlivé bezpečnostní role a zda lze bezpečnostní role zajistit za pomoci outsourcingu.

Hlášení kontaktních údajů a sankce za nesplnění povinností

V ust. § 11 odst. 1 ZKB je uvedeno, že poskytovatel regulované služby má povinnost hlásit NÚKIBU kontaktní údaje, kterými se rozumí identifikační údaje fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ve věcech upravených ZKB. Dle důvodové zprávy k ust. § 11 ZKB nemá docházet k situacím, kdy budou pověřené kontaktní osoby nedostupné a bez jakéhokoli zástupu. Nedostupnost kontaktních osob je dle ZKB navíc považována za nesplnění povinnosti nahlásit funkční a aktuální kontaktní údaje. Nenahlášení funkčních a aktuálních údajů je dle ust. § 59 odst. 4 písm. c) ZKB přestupkem, za který NÚKIB může uložit poskytovateli regulované služby ve vyšším režimu pokutu až do výše 100.000.000 Kč. Poskytovatelům regulované služby v nižším režimu může NÚKIB dle ust. § 59 odst. 4 písm. d) ZKB za nenahlášení údajů uložit pokutu až do výše 50.000.000 Kč.

NÚKIB chce pod pohrůžkou vysoké pokuty zajistit efektivní komunikaci i v případě, kdy bude hlavní kontaktní osoba například dlouhodobě nepřítomná, nebo zrovna nebude dostupná. Dostatečnou zastupitelnost, tedy odpovídající počet kontaktních osob, nelze dle ZKB exaktně určit, bude se odvíjet zejména od velikosti a kapacit regulované osoby, případně počtu regulovaných služeb. NÚKIB prozatím doporučuje u menších organizací uvést minimálně dvě nebo tři kontaktní osoby, aby byla zajištěna jejich dostatečná zastupitelnost. U větších organizacích důvodová zpráva ZKB mlčí, domnívám se tedy, že větší společnosti by logicky měly uvést alespoň 4 kontaktní osoby. [1]

Požadavky kladené na bezpečnostní role u poskytovatelů regulované služby ve vyšším režimu povinností

V ust. § 5 odst. 7 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností je dále stanoveno, že statutár zajistí zastupitelnost bezpečnostních rolí uvedených v odstavci 6 písmene a) a b) předmětné vyhlášky (tzn. statutár vždy musí zajistit zastupitelnost manažera a architekta kybernetické bezpečnosti).

Požadavky kladené na manažera a architekta kybernetické bezpečnosti, stejně jako jiné bezpečnostní role (auditora kybernetické bezpečnosti a garanta aktiva) jsou dále uvedeny v ust. § 6 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Ve stejném

ustanovení je uvedeno, že: *„povinná osoba při určování osob zastávajících bezpečnostní role přihlédne k doporučením uvedeným v příloze č. 5 k této vyhlášce“*.[2]

Zmíněna příloha č. 5 poměrně detailně upravuje požadavky na jednotlivé bezpečnostní role, které by měly být ze strany poskytovatele regulované služby v režimu vyšších povinností dodržovány. Poskytovatel regulované služby by měl dbát doporučení NÚKIBU a splnit u každé z bezpečnostních rolí stanovené požadavky. Předmětná příloha podmiňuje obsazení rolí požadavky na:

1. klíčové činnosti, kdy u každé z rolí je definováno, co by daná osoba měla mít v rámci společnosti na starost;

2. znalosti, které zahrnují např. znalost řízení rizik, znalost kontextu povinné osoby, určitých norem a relevantních právních předpisů, hardwarových komponentů, operačních systémů apod.;

3. zkušenosti, mezi které se např. řadí řízení a interpretování výsledků řízení rizik, bezpečný vývoj softwaru, navrhování a implementace bezpečnostních opatření;

4. vzdělání a praxi, která u auditora, architekta a manažera kybernetické bezpečnosti odpovídá alespoň 3 rokům praxe v oblasti kybernetické bezpečnosti, nebo absolvování studia na vysoké škole a alespoň 1 roku praxe v oblasti auditu informační nebo kybernetické bezpečnosti;

5. relevantní certifikaci, kdy každá z bezpečnostních rolí musí obdržet určitý certifikát, např. Certified Ethical Hacker (CEH), CompTIA Security +, Certified Information Security Manager (CISM), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA), Lead Auditor Information Security Management Systém (Lead Auditor ISMS), Auditor BI (akreditační schéma ČIA);

6. další podmínky jako je např. dostatečný rozpočet, neslučitelnost bezpečnostních rolí s jinými rolemi apod. [3]

U každé z bezpečnostních rolí je uvedeno, jaké náležitosti by měla splnit, a poskytovatel regulované služby by se jich měl v maximální možné míře držet. Kloním se k závěru, že NÚKIB by mohl tolerovat odchylku, co do vymezení klíčových činností a zkušeností, u požadovaného vzdělání a praxe je však mnohem menší prostor pro odchýlení se od požadovaných náležitostí. Uvedený požadavek je dle doporučení NÚKIBU totiž považován za nezbytné minimum pro splnění zákonných povinností.

Stejně tak je nutné upozornit na to, že:

1. role manažera kybernetické bezpečnosti není slučitelná s rolemi odpovědnými za provoz ICT a s dalšími provozními či řídicími rolemi;

2. role architekta kybernetické bezpečnosti není slučitelná s rolemi odpovědnými za provoz ICT;

3. role auditora není slučitelná s rolemi 1. výboru pro řízení kybernetické bezpečnosti, 2. manažera kybernetické bezpečnosti, 3. architekta kybernetické bezpečnosti, 4. garanta aktiva ani s rolemi odpovědnými za provoz ICT.[4]

Možnost outsourcingu bezpečnostních rolí

Vyhláška o kybernetické bezpečnosti dále nestanovuje konkrétní způsoby splnění povinností, ale pouze jejich rámec, společnosti tedy můžou využívat i outsourcing. NÚKIB na svých stránkách uvádí

pouze to, že nedoporučuje např. outsourcing bezpečnostní role manažera kybernetické bezpečnosti (z prováděcích vyhlášek k ZKB totiž vyplývá, že manažer má znát kontext regulované osoby). Oproti tomu u role auditora kybernetické bezpečnosti, která je neslučitelná s ostatními bezpečnostními rolemi, je dle NÚKIBU outsourcing zpravidla efektivním řešením.

Využitím outsourcingu se však poskytovatel regulované služby nijak nezbavuje odpovědnosti za řízení bezpečnosti a také se zvyšují nároky na správné řízení klíčových dodavatelů. Lze tedy shrnout, že vyhláška outsourcing bezpečnostních rolí nikde nezakazuje, pokud však poskytovatel regulované služby využívá outsourcing, musí dbát na to, že je stále plně zodpovědný za plnění povinností dle ZKB.[5]

Závěr a doporučení pro statutáry

Je patrné, že ZKB klade na poskytovatele regulované služby v režimu vyšších povinností celou řadu nových povinností a společnosti, které se zařadí do vyššího režimu povinností, musí do budoucna počítat s vynaložením dalších finančních prostředků na zajištění dostatku bezpečnostních rolí. U malých organizací by měly být uvedeny alespoň 3 kontaktní osoby, u větších organizací by bylo vhodné zajistit alespoň 4 kontaktní osoby.

Stejně tak by společnosti měly zajistit, aby se stávající zaměstnanci již teď dovzdělávali a získávali praxi v oblasti auditu informační nebo kybernetické bezpečnosti tak, aby do budoucna disponovali početnou základnou pracovníků, kteří by nad rámec svých stávajících povinností mohli zastávat bezpečnostní role. Společnosti, které se již teď začnou připravovat na příchod nového zákona, získají oproti ostatním společnostem konkurenční výhodu a mohou také ušetřit na nákladech za outsourcing.

Správné nastavení systému zastupitelnosti bezpečnostních rolí a plnění dalších povinností dle ZKB je s ohledem na složitost problematiky nicméně vždy vhodné konzultovat s odborníky na právo kybernetické bezpečnosti.

Mgr. Ondřej Rada,
advokátní koncipient

VKS LEGAL
ADVOKÁTNÍ KANCELÁŘ

VKS Legal advokátní kancelář, s. r. o.

dům u Nováků, Vodičkova 30
110 00 Praha 1 - Nové Město, 3. schodiště, 5. patro

tel.: +420 224 947 158
e-mail: office@akvks.cz

---

[1] Ust. § 11 a ust. § 59 a důvodová zpráva sněmovního tisku č. 759/0, vládní návrh zákona o kybernetické bezpečnosti

[2] Ust. § 5 a ust. § 6 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (sněmovní tisk č. 759/0)

[3] Příloha č. 5 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (sněmovní tisk č. 759/0)

[4] Tamtéž

[5] Informace volně dostupné >>> zde.

Další články:

- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory