Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Brno 16. února 2026

Č. j. 7508/2026-NÚKIB-E/210

NUKIX005QX22

Věc: Poskytnutí informací podle § 14 odst. 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Vážený pane [redacted]

Národní úřad pro kybernetickou a informační bezpečnost (dále jen jako „**Úřad**“ nebo „**NÚKIB**“) obdržel dne 3. února 2026 Vaši žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. V žádosti požadujete poskytnutí „*všech stanovisek NÚKIB (a jiných souvisejících dokumentů) k analýzám rizik, které povinný subjekt vypracoval v souvislosti s níže uvedenými řízeními u Úřadu pro ochranu hospodářské soutěže:*

ÚOHS-S0207/2021/VZ

ÚOHS-S0358/2019/VZ

ÚOHS-S0262/2019/VZ

ÚOHS-S0196/2022/VZ

ÚOHS-S0628/2023/VZ“.

Tímto Vám sděluji, že požadované dokumenty jsou přílohou této odpovědi. NÚKIB nebyl Úřadem pro ochranu hospodářské soutěže požádán o stanovisko ve věci vedené pod sp. zn. ÚOHS-S0207/2021/VZ.

S pozdravem

Elektronický podpis: 16.2.2026
Certifikát autora podpisu:
Jméno: Mgr. Vít Hrazdíra
Vydal: I.CA EU Qualified CA2/RSA 06/2022
Platnost do: 19.11.2026 19:15 +01:00

Mgr. Vít Hrazdíra
vedoucí oddělení právního
Národní úřad pro kybernetickou
a informační bezpečnost

Přílohy:
Příloha 1 - Sdělení k postupu společnosti Metropolnet, a. s.

Příloha 2 - Sdělení k analýze rizik Ministerstva životního prostředí

Příloha 3 - Sdělení k postupu Ministerstva životního prostředí

Příloha 4 - Sdělení k analýze rizik Oblastní nemocnice Příbram

Příloha 5 - Sdělení k analýze rizik Klatovská nemocnice a spol

Obdrží:

Vypraveno dne:
viz časový údaj na obálce datové zprávy

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č. j.: 3128/2019-NÚKIB-E/350 Brno, 25. 11. 2019

Sdělení k postupu společnosti Metropolnet, a. s.

Vaše č. j.: ÚOHS-S0358/2019/VZ-28460/2019/512/KMo

Vážená paní vedoucí,

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“) obdržel žádost Úřadu pro ochranu hospodářské soutěže (dále jen „**ÚOHS**“) ze dne 17. října 2019 o vyjádření k analýze rizik vypracované společností Metropolnet, a. s. (dále jen „**zadavatel**“), pro účely zadání veřejné zakázky „Obnova páteřní a přístupové infrastruktury“ (ev. č. Z2019-025302). Spolu s žádostí byly NÚKIB doručeny i následující dokumenty zadavatele (sdružené do jednoho souborného dokumentu):

- Studie stavu sítě Metropolnet a.s., návrh modernizace, monitoringu a správy sítě (PROJEKT 10): Specifikace Modelu M.T.B.M. v rámci podání na ÚHOS ze dne 1. 10. 2019,
- Analýza kyberbezpečnosti a bezpečnosti IS v rámci přípravy na certifikaci ISO 27000 ze dne 13. 3. 2017,
- Dílčí riziková analýza zaměřená na diskové pole a na aktivní síťové prvky v core vrstvě ze dne 28. 3. 2019, a
- Dílčí aktualizace Projekt 10: Riziková analýza a další konsekvence kyberbezpečnosti ke dni 30. 6. 2019.

Oproti deklaraci obsažené v obsahu obdrženého souborného dokumentu nebyla součástí Vašeho podání přílohová tabulka obsahující kompletní analýzu rizik zaměřenou na disková pole a na aktivní síťové prvky v core vrstvě. Tento dokument si tedy NÚKIB od zadavatele vyžádal (jde o dokument „Dílčí hodnocení rizik ZoKB_pro diskové pole a síťové prvky“). Spolu s tímto dokumentem NÚKIB od zadavatele obdržel též dokumenty „Hodnocení rizk ZoKB_pro VIS final“, „Hodnocení rizk ISO27000 final“ a „Metropolnet - komentář tabulky rizik shrnutí_v5 - prijate rev“; tyto dokumenty obsahují obecné hodnocení rizik pro vybrané systémy spravované zadavatelem bez přímé návaznosti na vydání varování NÚKIB ze dne 17. 12. 2018 a posloužily jako podpůrné materiály pro vypracování tohoto stanoviska.

Předně je třeba uvést, že NÚKIB v současné době neeviduje společnost Metropolnet, a. s. jako povinnou osobu podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „**ZKB**“). NÚKIB do dnešního dne nevydal žádné rozhodnutí nebo opatření obecné povahy, kterým by zadavatele určil povinnou osobou podle § 3 ZKB, a žádné řízení o určení v současné době nevede. Stejně tak zadavatel do dnešního dne neinformoval NÚKIB o tom, že by byl některou z povinných osob, u kterých dochází k tzv. samourčení (tzn. povinnou osobou se subjekt stává ze zákona naplněním definičních znaků a je

automaticky povinen nahlásit NÚKIB své kontaktní údaje). NÚKIB nadto ani nedisponuje informacemi, na základě kterých by získal důvodné podezření, že zadavatel je povinnou osobou podle § 3 ZKB a v rozporu se zákonem své kontaktní údaje nenahlásil.

V zadávací dokumentaci k veřejné zakázce „Obnova páteřní a přístupové infrastruktury“ (dostupné z profilu zadavatele) je na str. 4 uvedeno, že zadavatel v rámci svých činností technicky zajišťuje chod sítě a provoz informačních systémů Statutárního města Ústí nad Labem, vč. Magistrátu Statutárního města Ústí nad Labem, úřadů městských částí a dalších organizací zřizovaných MMÚL. Ani Statutární město Ústí nad Labem není povinnou osobou podle § 3 ZKB (ani na základě rozhodnutí NÚKIB, ani na základě samourčení) a zejm. s ohledem na počet obyvatel Statutárního města Ústí nad Labem a skutečnost, že obce nemohou být správci významných informačních systémů ve smyslu § 2 písm. d) a § 3 písm. e) ZKB, nelze předpokládat, že by se Statutární město Ústí nad Labem mělo v dohledné době povinnou osobou stát. Zadavatel tedy v současné době není ani provozovatelem informačního nebo komunikačního systému povinné osoby ve smyslu § 2 písm. g) ZKB [ani významným dodavatelem ve smyslu § 2 písm. n) vyhlášky č. 82/2018 Sb., bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), dále jen „**VKB**“].

Lze pak uzavřít, že pokud není zadavatel povinnou osobou podle ZKB, nelze u něj dovodit ani povinnost postupovat podle pravidel obsažených v ZKB. Uvedené však neznamená, že by zadavatel nemohl aplikovat ustanovení ZKB a VKB ve svých strukturách dobrovolně, např. z důvodu, že to po něm požadují jeho smluvní partneři nebo jeho zřizovatel, nebo z důvodu, že zadavatel usiluje o získání certifikace ISO 27000 (celá koncepce VKB je založena právě na normě ISO 27001). Zadavatel nadto na str. 4 dokumentu „Dílčí riziková analýza zaměřená na diskové pole a aktivní síťové prvky v core vrstvě“ uvádí, že „*[s]polečnost Metropolnet zajišťuje přístup přes síť MVČR ke kritické infrastruktuře státu z pohledu zákona o kybernetické bezpečnosti (KIVS = komunikační infrastruktura veřejné správy, CMS = centrální místo služeb). Tudíž je nutné, aby požadavky kladené na Kritickou infrastrukturu MV splňovala i firma Metropolnet, tj. prakticky naplňovala požadavky Kybernetického zákona*.“ Zadavatel zde tedy dovozuje svou povinnost zajišťovat bezpečnost informací podle ZKB ze skutečnosti, že přistupuje do systémů, které musejí požadavky ZKB splňovat. Taková povinnost zadavateli sice neplyne ze zákona (ZKB, resp. VKB pouze stanoví povinným osobám povinnost řídit své dodavatele), nicméně uvedený požadavek může být obsažen v podmínkách provozování citovaných systémů Ministerstva vnitra, resp. může být předmětem dalších smluvních ujednání mezi zadavatelem a Ministerstvem vnitra (jejich obsah však NÚKIB není znám).

K zohlednění varování NÚKIB ze dne 17. 12. 2018 zadavatelem pak lze uvést, že varování ve smyslu § 12 ZKB je aktem s obecnou platností, kterým NÚKIB informuje širokou veřejnost o existenci hrozby v oblasti kybernetické bezpečnosti. Varování samo o sobě neukládá žádné povinnosti, stejně jako není určeno pouze omezenému okruhu adresátů. Speciální ustanovení ZKB a VKB stanoví, které orgány a osoby (povinné osoby) mají zákonnou povinnost zohlednit varování v procesu řízení rizik. Lze však předpokládat (a NÚKIB to považuje z hlediska zajištění vysoké úrovně kybernetické bezpečnosti v České

republice za vysoce žádoucí), že i orgány a osoby, které nespadají do působnosti ZKB, budou s informací obsaženou ve varování v rámci řízení bezpečnosti svých informačních systémů dále pracovat a budou ji zohledňovat v procesu řízení rizik. Jak VKB, tak norma ISO 27001 totiž požadují, aby povinné osoby, resp. subjekty aplikující normu, při řízení rizik zohledňovaly jim známé relevantní hrozby. Je přitom lhostejné, zda se o nich subjekt dozvěděl z varování NÚKIB či z jiného veřejného či vlastního zdroje.

Co se týče samotného posouzení souladnosti postupu zadavatele při tvorbě analýzy rizik s ustanoveními ZKB a VKB, předně je třeba upozornit, že ačkoli výslovně žádáte o posouzení postupu zadavatele při tvorbě analýzy rizik, obsah analýzy rizik a způsob jejího provedení je třeba posuzovat i v kontextu předcházejících a navazujících kroků zadavatele tvořících v souhrnu proces řízení rizik. Proces řízení rizik sestává z hodnocení rizik (jehož součástí je identifikace, analýza a vyhodnocení rizik), výběru a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik [srov. § 2 písm. i) VKB]. Výběr konkrétního bezpečnostního opatření, jehož implementace sníží hodnotu rizika na akceptovatelnou úroveň, pak musí být založen nikoli pouze na samotné analýze rizik (jejímž výsledkem je striktně vzato pouze stanovení hodnoty rizika), nýbrž i na navazujícím vyhodnocení rizik (tedy určení, zda je riziko akceptovatelné či nikoli) a zvážení v úvahu přicházejících bezpečnostních opatření. Postup povinné osoby by přitom měl korespondovat s již nastavenými pravidly pro řízení rizik. Pro posouzení správnosti postupu povinné osoby při tvorbě analýzy rizik je krom jiného nezbytné i posouzení toho, zda celý proces hodnocení rizik, do něhož tvorba analýzy rizik spadá a od jehož zbylých součástí je funkčně neoddělitelná, byl proveden v souladu s metodikou k tomu vyhotovenou [srov. § 5 odst. 1 písm. a) VKB].

Po prostudování poskytnutých dokumentů NÚKIB konstatuje, že hodnocení rizik zadavatelem, jak bylo v předložených dokumentech prezentováno, ve vztahu ke konkrétní veřejné zakázce neodpovídá požadavkům obsaženým v ZKB a VKB. NÚKIB zejm. shledává jako nedostatečnou identifikaci primárních a podpůrných aktiv a vazeb mezi nimi, výběr konkrétních podpůrných aktiv, na základě jejichž hodnocení došlo k zákazu použití prostředků dotčených obchodních společností v zadávacím řízení, dále lze identifikovat určitou zmatečnost a nejednotnost v popisu stupnic pro hodnocení jednotlivých proměnných vzorce pro výpočet hodnoty rizika a v popisu samotného vzorce a v neposlední řadě též nesprávné zohlednění varování NÚKIB ze dne 17. 12. 2018 při stanovení hodnot jednotlivých proměnných vzorce pro výpočet rizika (zejm. došlo nejen k úpravě hodnoty hrozby, ale na některých místech též k úpravě hodnoty zranitelnosti). Předložené materiály pak prezentují postupy pro hodnocení rizik jak podle pravidel normy ISO 27001, tak podle pravidel obsažených v ZKB a VKB. Není zřejmé, zda a z jakého důvodu zadavatel provádí či hodlá provádět dvojí hodnocení rizik. Žádné z těchto hodnocení však samo o sobě ani v souhrnu nevyhovuje kompletním požadavkům ZKB a VKB.

Postup zadavatele při hodnocení rizik a při navazujícím výběru bezpečnostního opatření je tedy z pohledu NÚKIB nedostatečně zdokumentován a je obecně (pro nezainteresovanou osobu) neopakovatelný a zmatečný. Stejně tak je zmatečný i samotný způsob zapracování varování NÚKIB ze dne 17. 12. 2018 do procesu hodnocení rizik. Z výše uvedených důvodu pak postup zadavatele nelze označit za souladný se ZKB a VKB.

Co se týče hodnocení souladnosti postupu zadavatele s pravidly obsaženými v normě ISO 27001, to

obecně není v kompetenci NÚKIB. Ačkoli VKB z uvedené normy v podstatné části vychází (a NÚKIB tedy v mnoha případech při hodnocení zákonnosti postupu povinných osob s obsahem norem řady ISO 27000 pracuje), stále existují určité odlišnosti (např. ve způsobu výběru primárních aktiv nebo v rozsahu volnosti, kterou subjekty v určitých otázkách disponují). NÚKIB je pak pověřen dozorováním dodržování ZKB a VKB, nikoli norem řady ISO 27000, a jeho kontrolní postupy jsou tomu přizpůsobeny.

NÚKIB nevylučuje, že pokud by zadavatel provedl hodnocení rizik řádně podle všech pravidel obsažených ve VKB a vyvaroval se výše uvedeným pochybením, výsledek hodnocení rizik by byl shodný a rozporované bezpečnostní opatření by bylo pro snížení identifikovaných rizik možné i nadále považovat za jediné akceptovatelné (zadavatel sice nesprávně zohlednil varování NÚKIB ze dne 17. 12. 2018 při stanovení hodnot jednotlivých proměnných vzorce pro výpočet rizika, současně však výslovně zmínil, avšak dále nehodnotil rizika, která by mohla být z pohledu NÚKIB relevantní a u nichž by hodnota rizika pravděpodobně také překročila hranici pro akceptaci rizika). Stejně tak nelze vyloučit, že zadavatelův postup ve výsledku vyhovuje požadavkům normy ISO 27001. Za současného stavu a na základě předložených dokumentů je však třeba uzavřít, že výběr bezpečnostního opatření se nezakládá na hodnocení rizik provedeném zcela v souladu s požadavky ZKB a VKB.

V případě potřeby je NÚKIB připraven poskytnout Vašemu úřadu ke způsobu hodnocení postupu zadavatele podrobnější informace.

S pozdravem

Národní úřad
pro kybernetickou
a informační bezpečnost

Digitálně podepsal
Adam Kučínský
Datum: 2019.11.25
15:33:31 +01'00'

Adam Kučínský
ředitel odboru regulace

datovou schránkou
Úřad pro ochranu hospodářské soutěže
třída Kpt. Jaroše 7, 604 55 Brno

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č. j.: 2198/2019-NÚKIB-E/350 Brno, 06.09.2019

Sdělení k analýze rizik Ministerstva životního prostředí

Vaše č. j.: ÚOHS-S0262/2019/VZ-21968/2019/523/JMa

Vážený pane vedoucí,

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“) obdržel žádost Úřadu pro ochranu hospodářské soutěže (dále jen „**ÚOHS**“) ze dne 12. 8. 2019 o vyjádření k analýze rizik vypracované Ministerstvem životního prostředí (dále jen „**zadavatel**“) pro účely zadání veřejné zakázky „Pořízení serverů pro resort MŽP v roce 2019“ (ev. č. Z2019-008830). Spolu s žádostí byly NÚKIB doručeny i následující součásti bezpečnostní dokumentace a bezpečnostní politiky zadavatele:

- Analýza rizik – servery, verze 2 platná ke dni 15. 1. 2019 (dále jen „**analýza rizik**“),
- Pokyn Manažera kybernetické bezpečnosti ze dne 2. 5. 2019 (dále jen „**pokyn MKB**“) a jeho přílohy 1 až 3.

Ačkoli výslovně žádáte o posouzení zákonnosti postupu zadavatele při tvorbě analýzy rizik, považuji za vhodné upozornit, že obsah analýzy rizik a způsob jejího provedení je třeba posuzovat i v kontextu předcházejících a navazujících kroků zadavatele tvořících v souhrnu proces řízení rizik. Proces řízení rizik sestává z hodnocení rizik (jehož součástí je identifikace, analýza a vyhodnocení rizik), výběru a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik [srov. § 2 písm. i) vyhlášky č. 82/2018 Sb., bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), dále jen „**VKB**“]. Výběr konkrétního bezpečnostního opatření, jehož implementace sníží hodnotu rizika na akceptovatelnou úroveň (v tomto případě dodání druhého kusu poptávaného zařízení od výrobce odlišného od výrobce výslovně citovaného ve varování NÚKIB ze dne 17. 12. 2018), pak musí být založen nikoli pouze na samotné analýze rizik (jejímž výsledkem je striktně vzato pouze stanovení hodnoty rizika), nýbrž i na navazujícím vyhodnocení rizik (tedy určení, zda je riziko akceptovatelné či nikoli) a zvážení v úvahu přicházejících bezpečnostních opatření. Postup povinné osoby by přitom měl korespondovat s již nastavenými pravidly pro řízení rizik.

Pro posouzení správnosti postupu povinné osoby při tvorbě analýzy rizik je krom jiného nezbytné i posouzení toho, zda celý proces hodnocení rizik, do něhož tvorba analýzy rizik spadá a od jehož zbylých součástí je funkčně neoddělitelná, byl proveden v souladu s metodikou k tomu vyhotovenou [srov. § 5 odst. 1 písm. a) VKB]. Dokument Analýza rizik – servery byl podle informací obsažených na kartě „Verze“ vyhotoven dne 10. 12. 2019 (zde jde pravděpodobně o překlep) a aktualizován dne 15. 1. 2019. Pokyn MKB, který jste NÚKIB spolu s žádostí poskytl, je datován ke dni 2. 5. 2019, tento konkrétní dokument

tedy nemohl být použit pro hodnocení rizik realizované v lednu 2019. NÚKIB se obrátil na zadavatele s žádostí o vysvětlení rozporu v datech vyhotovení jednotlivých dokumentů, resp. o zaslání znění metodiky pro hodnocení rizik, podle které postupoval při tvorbě hodnocené analýzy rizik. Odpovědí zadavatele ze dne 27. 8. 2019, č. j. MZP/2019/210/312, bylo NÚKIB sděleno, že pokyn MKB datovaný ke dni 2. 5. 2019, který byl poskytnut ÚOHS, existoval v obsahově stejné podobě již před datem 2. 5. 2019, a to pod názvem „Pokyn Manažera kybernetické bezpečnosti pro řízení aktiv a řízení rizik v oblasti kybernetické bezpečnosti na Ministerstvu životního prostředí_verze 1“. Rozpor v datech vyhotovení je dle vyjádření zadavatele způsoben tím, že v případě obou dokumentů (Analýza rizik – servery; Pokyn manažera kybernetické bezpečnosti) byly ÚOHS poskytnuty nejaktuálnější verze dokumentů. Spolu s vyjádřením byl NÚKIB zaslán i Pokyn Manažera kybernetické bezpečnosti pro řízení aktiv a řízení rizik v oblasti kybernetické bezpečnosti na Ministerstvu životního prostředí datovaný ke dni 7. 1. 2019. Po porovnání obou dokumentů NÚKIB konstatuje, že dokumenty jsou obsahově shodné, liší se pouze po formální stránce.

Po prostudování všech poskytnutých dokumentů NÚKIB shledal, že pro řádné zhodnocení postupu zadavatele při hodnocení rizik není třeba vyžadovat od něj další informace. Předložená dokumentace je srozumitelná a návodná a je z ní zřejmé, jakým způsobem zadavatel při hodnocení rizik a tvorbě posuzované analýzy rizik postupoval. Dílčí nedostatky, která NÚKIB identifikoval, nemohou mít vliv na výsledky procesu hodnocení rizik. Na základě informací obsažených v dokumentech, které byly NÚKIB Vaším úřadem poskytnuty, pak NÚKIB uzavírá, že **předložená analýza rizik splňuje požadavky ZKB a VKB a je provedena v souladu s obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti**. Podrobnosti uvádím níže.

Předložená analýza rizik je podle svého obsahu reakcí na varování NÚKIB ze dne 17. 12. 2018 (dále jen „**varování**“), kterým NÚKIB označuje použití technických a programových prostředků vybraných obchodních společností (dále jen „**dotčené společnosti**“) za hrozbu v oblasti kybernetické bezpečnosti. Předmětem analýzy rizik jsou pouze aktiva, která mají vazbu na plnění poptávané v rámci přezkoumávané veřejné zakázky. Současně však dokument obsahuje i plán zvládání rizik a prohlášení o aplikovatelnosti, z čehož lze dovodit, že jde o analýzu rizik sloužící pro standardní hodnocení rizik ve smyslu § 5 VKB [aktualizovanou v souladu s § 5 odst. 1 písm. h) bod 3 VKB], byť zaměřenou na konkrétní technické aktivum – servery, a jemu přidružená primární a podpůrná aktiva. S ohledem na úzce vymezený předmět veřejné zakázky a skutečnost, že jde o standardní, generické plnění, které je již ve strukturách zadavatele používáno a se kterým má zadavatel zkušenosti (zejm. v tom smyslu, že je schopen identifikovat relevantní zranitelnosti jednotlivých aktiv a hrozby, které na aktiva mohou působit), lze tuto analýzu rizik využít i pro účely tzv. předsmluvního hodnocení rizik ve smyslu § 8 odst. 2 písm. a) VKB.

NÚKIB se při hodnocení zákonnosti předložené analýzy rizik (resp. celého procesu hodnocení rizik, jehož byla analýza rizik součástí) zaměřil primárně na to, zda zadavatel postupoval v souladu s metodikou k tomu stanovenou (zde pokynem MKB), zda jsou metodika i praktický postup zadavatele při hodnocení rizik srozumitelné a přezkoumatelné, zda pravidla obsažená v metodice korespondují s pravidly

obsaženými v ZKB a VKB a se standardy v oblasti kybernetické bezpečnosti a zda zadavatel tam, kde mu metodika i právní předpisy umožňují jednat dle svého vlastního uvážení (zejm. při přiřazování hodnot aktivům, hrozbám a zranitelnostem), nejednal neodůvodněně excesivně. Dále pak NÚKIB hodnotil rozsah aktiv, u nichž byla hodnocena rizika, jejich souvislost s předmětem veřejné zakázky a způsob zapracování informace obsažené ve varování do procesu hodnocení rizik. Dílčí nepřesnosti a nedostatky, které NÚKIB identifikoval, spočívaly zejména v absenci podrobnějšího hodnocení důsledků závislostí mezi jednotlivými aktivy, nepřesném rozdělení jednotlivých úrovní škály pro hodnocení rizik a nezohlednění zavedených bezpečnostních opatření při stanovení hodnoty rizika spojeného s použitím prostředků dotčených společností. Uvedené nedostatky však samostatně ani v souhrnu nemohly mít vliv na výsledek hodnocení rizik, neboť výsledná hodnota rizika by stále dosahovala neakceptovatelné úrovně.

Na základě předložených informací tedy lze shrnout, že zadavatelem provedené hodnocení rizik odpovídá požadavkům, které na něj klade ZKB a VKB, a jeví se jako souladné s postupy, které jsou definovány v pokynu MKB. Některá rizika spojená s použitím prostředků dotčených společností, která zadavatel hodnotil jako neakceptovatelná, pak zadavatel v souladu s pokynem MKB neakceptuje, v důsledku čehož do zadávací dokumentace zanesl požadavek na zdvojení dodaných výrobků, čímž má být dosaženo stavu vysoké dostupnosti řešení. Postup pro zvládání zbylých rizik, která byla v analýze rizik identifikována jako neakceptovatelná, není z předložené dokumentace zřejmý, je však otázkou, nakolik je tato skutečnost relevantní pro posouzení zákonnosti postupu zadavatele ve Vámi přezkoumávaném zadávacím řízení.

V případě potřeby je NÚKIB připraven poskytnout Vašemu úřadu ke způsobu hodnocení postupu zadavatele podrobnější informace.

S pozdravem

Národní úřad
pro kybernetickou
a informační bezpečnost

Digitálně podepsal
Adam Kučínský
Datum: 2019.09.06
17:34:44 +02'00'

Adam Kučínský
ředitel odboru regulace

datovou schránkou
Úřad pro ochranu hospodářské soutěže
třída Kpt. Jaroše 7, 604 55 Brno

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č. j.: 2841/2019-NÚKIB-E/350 Brno, 23. 10. 2019

Sdělení k postupu Ministerstva životního prostředí

Vaše č. j.: ÚOHS-S0262/2019/VZ-27156/2019/523/JMa

Vážený pane vedoucí,

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“) obdržel žádost Úřadu pro ochranu hospodářské soutěže (dále jen „**ÚOHS**“) ze dne 4. 10. 2019 o stanovisko k postupu Ministerstva životního prostředí (dále jen „**zadavatel**“) při výběru opatření ke zvládání rizik navazujícího na výsledky procesu hodnocení rizik, k jehož zákonnosti se NÚKIB vyjádřil ve svém předchozím přípisu. Konkrétně požadujete vyjádření, zda dle názoru NÚKIB zadavatel v souladu s příslušnými právními předpisy a obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti mohl zvolit i jiné technické opatření, než opatření spočívající v dodání druhého kusu poptávaného zařízení od výrobce odlišného od výrobce výslovně citovaného ve varování NÚKIB ze dne 17. 12. 2018 (dále jen „**varování**“), kterým by zamezil riziku nedostupnosti služby, a zda bylo předmětné opatření zvoleno v souladu s obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti.

Úvodem, pro pochopení celého kontextu volby a implementace bezpečnostních opatření pro snížení kybernetických bezpečnostních rizik povinnými osobami podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „**ZKB**“), považuji za nezbytné uvést následující. Orgány a osoby uvedené v § 3 písm. c) až f) ZKB jsou podle § 4 odst. 2 ZKB povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému a vést o nich bezpečnostní dokumentaci. Bezpečnostním opatřením se podle § 4 odst. 1 ZKB rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru. ZKB v § 5 stanoví výčet jednotlivých organizačních a technických bezpečnostních opatření, jejichž přijímání je ze zákona vyžadováno, obsah a rozsah jednotlivých bezpečnostních opatření stanoví prováděcí právní předpis, kterým je vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti, dále jen „**VKB**“). Jedním z bezpečnostních opatření je řízení rizik, kterým se rozumí činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik [srov. § 2 písm. i) VKB]. V rámci řízení rizik povinná osoba mj. zpracuje a zavede plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání

rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob realizace bezpečnostních opatření. Hodnocení rizik souvisejících s plněním předmětu výběrového řízení (na něž pak navazují další fáze procesu řízení rizik) se provádí též ve vztahu k významným dodavatelům v rámci výběrového řízení a před uzavřením smlouvy; takové hodnocení rizik se provede přiměřeně podle přílohy č. 2 k VKB.

ZKB ani VKB nestanoví podrobnější informace ke způsobu výběru opatření ke zvládání rizik, platí tedy (a tyto postupy vycházejí z technických norem regulujících systém řízení bezpečnosti informací, zejm. ČSN ISO/IEC 27001 a ČSN ISO/IEC 27005; na normách ISO/IEC řady 27000 je ostatně založena celá VKB), že konkrétní opatření ke zvládání rizik volí povinná osoba na základě svých specifických potřeb, především při zohlednění struktury informačního nebo komunikačního systému, jehož rizika mají být mitigována, pravidel obsažených v bezpečnostních politikách a bezpečnostní dokumentaci a dalších postupů a požadavků, kterými je povinná osoba v rámci své činnosti vázána. Nezbytnou součástí zvažování přiměřenosti bezpečnostního opatření [o které hovoří § 3 písm. c) VKB] je též posouzení hospodárnost zvoleného postupu, zejm. tedy zda náklady spojené se zavedením bezpečnostního opatření nejsou neúměrné nákladům spojeným s realizací rizika.[1] Volba konkrétního opatření ke snížení identifikovaného rizika je výlučně v odpovědnosti povinné osoby.

Výčet opatření ke zvládání rizik přitom není konečný – konkrétní podoba opatření se odvíjí především od charakteru rizika, na které má reagovat, atributu bezpečnosti, na který má reagovat (důvěrnost, dostupnost, integrita), úrovně zabezpečení, které má být jeho implementací dosaženo, architektury systému, do kterého má být implementováno, lokace, ve které má být implementováno, důležitosti aktiva, jehož rizika mají být regulována, finančních možností povinné osoby atd. Konkrétní opatření, které je pro mitigaci určitého rizika zavedeno v jedné organizaci, nemusí být vhodné pro jinak strukturovanou organizaci. Jedno technické opatření může ve vztahu k různým systémům regulovat riziko různým způsobem a v různé kvalitě. Některá technická opatření mohou být s ohledem na jejich provedení unikátní a v jiných organizacích nereplikovatelná, některá inovativní technická opatření nemusí být povinným osobám z jejich činnosti vůbec známa. Ze všech těchto a dalších důvodů je výběr konkrétních opatření ke zvládání rizik ponechán povinným osobám, neboť nikdo nezná regulované systémy a kontext jejich fungování lépe než právě povinné osoby.

Úlohou NÚKIB v této věci je pak především kontrola toho, zda bezpečnostní opatření, která má povinná osoba povinnost zavést a provést, jsou zaváděna a prováděna v rozsahu nezbytném pro zajištění kybernetické bezpečnosti konkrétního systému a zda povinné osoby zohledňují požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich systém (situaci lze například připodobnit tomu, že ÚOHS obecně nehodnotí vhodnost řešení poptávaných ve veřejných zakázkách z hlediska potřeb zadavatelů, ale pouze to, zda zadavatelé při formulaci svých požadavků nevybočují z mantinelů pro zadávání veřejných zakázek). Ve vztahu k přijatým opatřením pro zvládání rizik tedy NÚKIB hodnotí, zda skutečně vedou k požadovanému cíli (snížení rizika na akceptovatelnou úroveň) a zda nejsou

[1] K tomu srov. např. metodický materiál NÚKIB dostupný zde: https://www.govcert.cz/download/kii-vis/obecne/Neprimerene-naklady_v2.1.pdf.

nepřiměřená, nikoli zda povinná osoba zvážila všechna možná řešení (to lze učinit jen vůči opatřením, která jsou uvedena v rámci VKB, ale ne vůči všem možným řešením) a zvolila nejoptimálnější z nich. „Zvážení v úvahu přicházejících bezpečnostních opatření“ zmíněné v předchozím vyjádření NÚKIB má sloužit povinným osobám k tomu, aby z v úvahu přicházejících řešení vybraly to nejoptimálnější z hlediska svých potřeb.

Ze zkušeností NÚKIB lze konstatovat, že pro zajištění dostupnosti služby povinné osoby v praxi obvykle zvažují následující postupy:

a) nasazení technického opatření eliminujícího zranitelnost(i) aktiva nebo hrozby spojené s používáním aktiva,

b) implementaci nového řešení za současného zachování provozu (byť nouzového) starého řešení,

c) redundanci, tedy zdvojení používaných zařízení,

d) eliminaci rizikové technologie (obvykle v případech, kdy zranitelnost aktiva nemůže být eliminována jiným způsobem nebo kdy hrozbu spojenou s použitím aktiva nelze eliminovat jiným způsobem).

Varování označuje za hrozbu v oblasti kybernetické bezpečnosti použití technických a programových prostředků určitých obchodních společností (dále jen „**dotčené společnosti**“), a to bez další specifikace. Míří tedy na všechny technické a programové prostředky, které dotčené společnosti nabízejí na trhu. Stejně tak varování nijak nehodnotí zranitelnosti jednotlivých zařízení vyráběných dotčenými společnostmi. Důvody pro vydání varování (uvedené v odůvodnění varování) nejsou vázány na konkrétní zranitelnosti, kterými mohou jednotlivá zařízení disponovat. Lze předpokládat, že hrozba, kterou prostředky dotčených společností představují, může být realizována jednak prostřednictvím „standardních“ zranitelností (které jsou s prostředky určitého typu obvykle spojeny), jednak prostřednictvím zranitelností, které mohou být pro prostředky dotčených společností specifické.

Z výše uvedeného důvodu je z pohledu NÚKIB nevhodné, aby povinné osoby samy, bez informací, které má NÚKIB k dispozici a které jsou vedeny v utajovaném režimu a veřejnosti nepřístupné, dovozovaly (*de facto* spíše tipovaly), které zranitelnosti jsou s prostředky dotčených společností spojeny a reagovaly na ně specifickými technickými opatřeními [tedy aby v tomto případě postupovaly podle výše uvedeného písm. a)].

Obecně lze konstatovat, že každé zařízení má nějaké zranitelnosti a stejně tak každé zařízení je vystaveno nějakým hrozbám. Každá zranitelnost či hrozba je v principu eliminovatelná, jde však o to, zda si je povinná osoba její existence vědoma a zda je v jejích možnostech a schopnostech eliminaci provést. Tím, že varování neobsahuje podrobnější informace o zranitelnostech nebo hrozbách spojených s prostředky dotčených společností a je koncipováno takto obecně, *de facto* NÚKIB sděluje, že jakákoli hrozba přímo související s prostředky dotčených společností je pravděpodobná až víceméně jistá a může být zneužita jakoukoli příhodnou zranitelností zařízení, která nemusí být ani v současné době známa. Pokud povinná osoba nezná specifika zranitelností a hrozeb spojených s uvedenými zařízeními, těžko na ně může nějak specificky reagovat.

Variantu uvedenou pod písm. b), tedy zachování nahrazovaného řešení v provozu (byť v nouzovém režimu a jen pro případ výpadku nové technologie), je možné uvažovat pouze ve specifických případech (kdy je takové nastavení architektury systému vůbec možné) a NÚKIB ji považuje za krajně problematickou a dlouhodobě neudržitelnou. Zejm. je třeba si uvědomit, že na starou technologii nejsou mnohdy vydávány aktualizace, úroveň zabezpečení dramaticky klesá, takové řešení nadto nemusí být ani zahrnuto do maintenance procesů povinné osoby. Vzhledem k nevyhnutelné rostoucí poruchovosti a morálnímu zastarávání technologií lze toto řešení označit spíše za provizorní.

Redundance [písm. c)] je standardní a v praxi zcela běžné řešení pro zajištění vysoké úrovně dostupnosti služby (nehledě na zajištění důvěrnosti nebo integrity). Nadto jde o bezpečnostní opatření podle § 27 písm. d) VKB, jehož zavedení jsou povinné osoby ze zákona povinny zvažovat. Nasazením redundantního zařízení do struktury systému povinná osoba zajistí, že v případě výpadku primárního zařízení budou např. veškeré relevantní procesy přesměrovány na redundantní, funkční zařízení. Výpadek primárního zařízení tak neovlivní fungování služby samotné, resp. v případě ztráty dat na primárním zařízení budou data zachována na záložním zařízení.

Varianta d) pak vede ke kompletnímu zajištění bezpečnosti informačních a komunikačních systémů (tj. jejich dostupnosti, důvěrnosti i integrity). Jak již bylo uvedeno výše, povinné osoby nemají kompletní informace o všech hrozbách a zranitelnostech spojených s použitím prostředků dotčených společností. Zavedením „mírnějšího“ bezpečnostního opatření tedy nemusí reagovat (vědomě či nevědomě) na celé spektrum problémů, tedy na všechna nebezpečí, která jsou s použitím uvedených prostředků spojena. Pokud však cílem přijetí bezpečnostního opatření není současné zajištění dostupnosti, důvěrnosti a integrity, ale pouze některé z těchto složek (např. dostupnosti), může být varianta úplného zákazu použití prostředků dotčených společností ve strukturách povinné osoby naopak z hlediska ZKB a VKB nepřiměřená.

Ve vztahu k situaci zadavatele lze na základě výše uvedeného uzavřít, že jím zvolené opatření představuje zákonem předpokládané a standardně užívané opatření pro zajištění dostupnosti služby. Pro redundantní zařízení jsou pak stanoveny speciální požadavky (na výrobce zařízení), které jsou založeny na obsahu varování a výsledcích provedené analýzy rizik a které mají zajistit dostupnost služby v případě, že dojde k výpadku zařízení, jehož výrobcem je dotčená společnost. Takto nastavený požadavek se z dostupných informací a s ohledem na skutkové okolnosti posuzovaného případu jeví jako smysluplný a neexcesivní. Z vyjádření zadavatele ze dne 18. 7. 2019 citovaného v obou přípisech zaslaných NÚKIB Vaším úřadem v této věci pak vyplývá, že zvolené bezpečnostní opatření snižuje hodnotu identifikovaného rizika na akceptovatelnou úroveň. Na základě zkušeností NÚKIB pak lze dovodit, že není příliš pravděpodobné, že by existovalo i jiné technické řešení, kterým by zadavatel byl schopen srovnatelným způsobem zajistit vysokou dostupnost služby a snížit tím hodnotu identifikovaného rizika na akceptovatelnou úroveň (mimo úplný zákaz použití prostředků dotčených společností).

S pozdravem

Národní úřad
pro kybernetickou
a informační bezpečnost

Digitálně podepsal
Adam Kučínský
Datum: 2019.10.23
11:47:45 +02'00'

Adam Kučínský
ředitel odboru regulace

datovou schránkou

Úřad pro ochranu hospodářské soutěže
třída Kpt. Jaroše 7, 604 55 Brno

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Adam Kučínský
ředitel odboru regulace

Brno 7. července 2022

Č. j.: 8297/2022-NÚKIB-E/350

Sdělení k analýze rizik Oblastní nemocnice Příbram

Vaše č. j.: ÚOHS-17847/2022/535

Vážená paní vedoucí,

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“) obdržel žádost Úřadu pro ochranu hospodářské soutěže (dále též „**ÚOHS**“) ze dne 26. května 2022 o vyjádření k analýze rizik vypracované Oblastní nemocnicí Příbram (dále jen „**zadavatel**“) pro účely zadání veřejné zakázky „Datové uložiště“ (ev. č. Z2022-009336). Spolu s žádostí byl NÚKIB doručen i následující dokument zadavatele:

- Analýza a hodnocení rizik spojených s přípravou realizace veřejné zakázky „Datová uložiště“ ze dne 7. února 2022, včetně dvou příloh (dále jen „doručený dokument“).

Předně je třeba uvést, že NÚKIB v současné době neeviduje zadavatele jako povinnou osobu podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „**ZKB**“). Přestože zadavatel o sobě ve Vámi doručeném dokumentu uvedl, že je provozovatelem a poskytovatelem základní služby a správcem informačního systému základní služby dle § 3 písm. f), tak NÚKIB do dnešního dne nevydal žádné rozhodnutí nebo opatření obecné povahy, kterým by zadavatele určil povinnou osobou podle § 3 ZKB, a žádné řízení o určení v současné době nevede. Stejně tak do dnešního dne nedošlo ani k tzv. samourčení (tzn. povinnou osobou se subjekt stává ze zákona naplněním definičních znaků a je automaticky povinen nahlásit NÚKIB své kontaktní údaje). Tudíž NÚKIB nemá informace o tom, že by zadavatel byl povinnou osobou podle § 3 písm. f) ZKB.

Lze pak uzavřít, že pokud není zadavatel povinnou osobou podle ZKB, nelze u něj dovodit ani povinnost postupovat podle pravidel obsažených v ZKB. Uvedené však neznamená, že by zadavatel nemohl aplikovat ustanovení ZKB a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „**VKB**“) ve svých strukturách dobrovolně, např. z důvodu, že to po něm požadují jeho smluvní partneři nebo jeho zřizovatel, nebo z důvodu, že zadavatel usiluje o získání certifikace ISO 27000 (celá koncepce VKB je založena právě na normě ISO 27001).

K zohlednění varování NÚKIB ze dne 17. prosince 2018 zadavatelem pak lze uvést, že varování ve smyslu § 12 ZKB je aktem s obecnou platností, kterým NÚKIB informuje širokou veřejnost o existenci hrozby v

oblasti kybernetické bezpečnosti. Varování samo o sobě neukládá žádné povinnosti, stejně jako není určeno pouze omezenému okruhu adresátů. Speciální ustanovení ZKB a VKB stanoví, které orgány a osoby (povinné osoby) mají zákonnou povinnost zohlednit varování v procesu řízení rizik. Lze však předpokládat (a NÚKIB to považuje z hlediska zajištění vysoké úrovně kybernetické bezpečnosti v České republice za vysoce žádoucí), že i orgány a osoby, které nespadají do působnosti ZKB, budou s informací obsaženou ve varování v rámci řízení bezpečnosti svých informačních systémů dále pracovat a budou ji zohledňovat v procesu řízení rizik. Jak VKB, tak norma ISO 27001 totiž požadují, aby povinné osoby, resp. subjekty aplikující normu, při řízení rizik zohledňovaly jim známé relevantní hrozby. Je přitom lhostejné, zda se o nich subjekt dozvěděl z varování NÚKIB či z jiného veřejného či vlastního zdroje.

Co se týče zodpovězení Vašich otázek:

- je dle Vašeho odborného názoru předmětná analýza rizik provedená zadavatelem z formálního a obsahového hlediska v souladu s dotčenými právními předpisy (zejména ZKB a VKB) a obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti (tj. lege artis), a pokud ano,
- mohl dle Vašeho odborného názoru zadavatel v souladu s dotčenými právními předpisy (zejména ZKB a VKB) a obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti (tj. lege artis) zvolit v šetřeném případě i jiné technické opatření než sporné opatření, resp. bylo předmětné bezpečnostní opatření v podobě sporného opatření zvoleno v souladu s obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti (tj. lege artis)?

Postup zadavatele při tvorbě analýzy rizik, obsah analýzy rizik a způsob jejího provedení je třeba posuzovat i v kontextu předcházejících a navazujících kroků zadavatele tvořících v souhrnu proces řízení rizik. Proces řízení rizik sestává z hodnocení rizik (jehož součástí je identifikace, analýza a vyhodnocení rizik), výběru a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik [srov. § 2 písm. i) VKB]. Výběr konkrétního bezpečnostního opatření, jehož implementace sníží hodnotu rizika na akceptovatelnou úroveň, pak musí být založen nikoli pouze na samotné analýze rizik (jejímž výsledkem je striktně vzato pouze stanovení hodnoty rizika), nýbrž i na navazujícím vyhodnocení rizik (tedy určení, zda je riziko akceptovatelné či nikoli) a zvážení v úvahu přicházejících bezpečnostních opatření. Postup povinné osoby by přitom měl korespondovat s již nastavenými pravidly pro řízení rizik. **Pro posouzení správnosti postupu povinné osoby při tvorbě analýzy rizik je krom jiného nezbytné i posouzení toho, zda celý proces hodnocení rizik, do něhož tvorba analýzy rizik spadá a od jehož zbylých součástí je funkčně neoddělitelná, byl proveden v souladu s metodikou k tomu vyhotovenou** [srov. § 5 odst. 1 písm. a) VKB].

V doručeném dokumentu, který od Vás NÚKIB obdržel, však není uvedena kompletní analýza rizik, tak jak ji VKB chápe, ale spíše toliko konstatování jejího závěru. NÚKIB proto žádostí ze dne 13. června 2022 požádal přímo zadavatele o zaslání kompletní analýzy rizik, pokud tedy takovou analýzou rizik disponuje a zároveň jej vyzval k vysvětlení toho, proč sám sebe označuje za poskytovatele základní služby, když jím nebyl určen. Dne 17. června 2022 obdržel NÚKIB odpověď. Zadavatel ve svém vyjádření mj. uvedl,

že vedení nemocnice: *„přijalo rozhodnutí na plnou implementaci kybernetických a informačních bezpečnostních opatření ve shodě s VKB, a to i na dobrovolné bázi, s cílem, aby se neopakovala situace jako v Nemocnici Benešov, Fakultní nemocnici Brno, a nejnověji Ředitelství silnic a dálnic.“* Dále pak zadavatel uvedl, že vedení nemocnice *„si uvědomuje, že k aktuálnímu datu nemá provedenou Analýzu rizik ve shodě s metodikou NÚKIB, nicméně jako úvodní krok byla provedena GAP (rozdílová) analýza (podle metodiky NÚKIB), kterou je možno na vyžádání Vám poskytnout.“* Žádostí ze dne 20. června 2022 si NÚKIB uvedenou GAP analýzu od zadavatele vyžádal, avšak do dnešního dne žádnou odpověď neobdržel, přičemž stanovená lhůta k provedení úkonu již marně uplynula.

Na základě uvedeného je tudíž zřejmé, že zadavatel není povinnou osobou podle ZKB a zároveň si je vědom toho, že jím zpracovaná analýza rizik není ve shodě s metodikou NÚKIB.

Postup zadavatele při hodnocení rizik a při navazujícím výběru bezpečnostního opatření je tedy z pohledu NÚKIB nedostatečně zdokumentován a je obecně neopakovatelný a zmatečný. Stejně tak je zmatečný i samotný způsob zapracování varování NÚKIB ze dne 17. prosince 2018 do procesu hodnocení rizik. Z výše uvedených důvodu pak postup zadavatele nelze označit za souladný se ZKB a VKB.

NÚKIB nevylučuje, že pokud by zadavatel provedl hodnocení rizik řádně podle všech pravidel obsažených ve VKB a vyvaroval se výše uvedeným pochybením, výsledek hodnocení rizik by byl shodný a rozporované bezpečnostní opatření by bylo pro snížení identifikovaných rizik možné i nadále považovat za jediné akceptovatelné. Za současného stavu a na základě předložených dokumentů je však třeba uzavřít, že **výběr bezpečnostního opatření se nezakládá na hodnocení rizik provedeném zcela v souladu s požadavky ZKB a VKB.**

S pozdravem

Digitálně podepsal:
Martin Švéda
Národní úřad pro kybernetickou a informační bezpečnost
Dne: 07.07.2022 15:57

NÚKIB

v z. Martin Švéda
vedoucí Oddělení regulace soukromého sektoru

datovou schránkou
Mgr. Aneta Jonášová
vedoucí Oddělení veřejných zakázek 5
Úřad pro ochranu hospodářské soutěže
třída Kpt. Jaroše 7, 604 55 Brno

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

NUKIX003EZLB

Adam Kučínský
Ředitel odboru regulace

Praha 09. 01. 2024

Č. j.: 277/2024-NÚKIB-E/350

Sdělení k analýze rizik Klatovská nemocnice a spol

Vaše č. j.: ÚOHS-43612/2023/524

Vážená paní vedoucí,

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“) obdržel žádost č. j. ÚOHS-43612/2023/524 Úřadu pro ochranu hospodářské soutěže (dále též „**ÚOHS**“) ze dne 3. 11. 2023 o vyjádření k analýze rizik vypracované Klatovskou nemocnicí, a.s., IČO 26360527, se sídlem Plzeňská 929, 339 01 Klatovy (dále jen „**zadavatel**“) pro účely zadání veřejné zakázky „Modernizace ICT pro zvýšení kybernetické bezpečnosti“ (ev. č. Z2023-030576). Na základě doplnění č. j. ÚOHS-46882/2023/524 ze dne 23. 11. 2023 byly NÚKIB doručeny i následující dokumenty zadavatele, které nebyly v původní žádosti kvůli administrativnímu pochybení přiloženy:

- „Analýza rizik zakázky Modernizace ICT pro zvýšení kybernetické bezpečnosti“ zpracovaná zadavatelem 27. 10. 2023 (ve formátu .pdf),
- „Evidence aktiv a analýza rizik se zaměřením na varování NUKIB ze dne 17. 12. 2018“ zpracovaná zadavatelem 23. 6. 2023 (ve formátu .xlsx).

Nakonec obdržel NÚKIB doplnění č. j. ÚOHS-49066/2023/524 ze dne 7. 12. 2023. V něm ÚOHS informuje, že se v předmětné veřejné zakázce jedná o společné zadávání více zadavatelů, a nikoliv pouze o Klatovskou nemocnici, jak z důvodu administrativního pochybení uvedl v původní žádosti. Jako zadavatele tak označuje následující subjekty:

- Klatovská nemocnice, a.s., IČO 26360527, se sídlem Plzeňská 929, 339 01 Klatovy,
- Rokycanská nemocnice, a.s., IČO 26360900, se sídlem Voldušská 750, 337 01 Rokycany,
- Stodská nemocnice, a.s., IČO 26361086, se sídlem Hradecká 600, 333 40 Stod,
- Domažlická nemocnice, a.s., IČO 26361078, se sídlem Kozinova 292, 344 01 Domažlice,
- Nemocnice následné péče Svatá Anna, s.r.o., IČO 26360896, se sídlem Kyjovská 607, 348 15 Planá,
- Nemocnice následné péče LDN Horažďovice, s.r.o., IČO 26360870, se sídlem Blatenská 314, 341 01 Horažďovice.

Předně je třeba uvést, že NÚKIB v současné době neeviduje žádný ze subjektů jako povinnou osobu podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „**ZKB**“). NÚKIB do dnešního dne nevydal žádné rozhodnutí nebo opatření obecné povahy, kterým by zadavatele určil povinnou osobou podle § 3 ZKB, a žádné řízení o určení v současné době nevede. Stejně tak do dnešního dne nedošlo ani k tzv. samourčení (tzn. povinnou osobou se subjekt stává ze zákona naplněním definičních znaků a je automaticky povinen nahlásit NÚKIB své kontaktní údaje). Tudíž NÚKIB nemá informace o tom, že by zadavatel byl povinnou osobou podle § 3 písm. f) ZKB.

Lze pak uzavřít, že pokud není zadavatel povinnou osobou podle ZKB, nelze u něj dovodit ani povinnost postupovat podle pravidel obsažených v ZKB. Uvedené však neznamená, že by zadavatel nemohl aplikovat ustanovení ZKB a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „**VKB**“) ve svých strukturách dobrovolně, např. z důvodu, že to po něm požadují jeho smluvní partneři nebo jeho zřizovatel, nebo z důvodu, že zadavatel usiluje o získání certifikace ISO 27000 (celá koncepce VKB je založena právě na normě ISO 27001).

K zohlednění varování NÚKIB ze dne 17. prosince 2018 zadavatelem pak lze uvést, že varování ve smyslu § 12 ZKB je aktem s obecnou platností, kterým NÚKIB informuje širokou veřejnost o existenci hrozby v oblasti kybernetické bezpečnosti. Varování samo o sobě neukládá žádné povinnosti, stejně jako není určeno pouze omezenému okruhu adresátů. Speciální ustanovení ZKB a VKB stanoví, které orgány a osoby (povinné osoby) mají zákonnou povinnost zohlednit varování v procesu řízení rizik. Lze však předpokládat (a NÚKIB to považuje z hlediska zajištění vysoké úrovně kybernetické bezpečnosti v České republice za vysoce žádoucí), že i orgány a osoby, které nespadají do působnosti ZKB, budou s informací obsaženou ve varování v rámci řízení bezpečnosti svých informačních systémů dále pracovat a budou ji zohledňovat v procesu řízení rizik. Jak VKB, tak norma ISO 27001 totiž požadují, aby povinné osoby, resp. subjekty aplikující normu, při řízení rizik zohledňovaly jim známé relevantní hrozby. Je přitom lhostejné, zda se o nich subjekt dozvěděl z varování NÚKIB či z jiného veřejného či vlastního zdroje.

Zároveň lze také poukázat na novou právní úpravu kybernetické bezpečnosti v České republice. V současné chvíli probíhá legislativní proces návrhu nového zákona o kybernetické bezpečnosti. Ten transponuje směrnici Evropského parlamentu a Rady 2022/255 ze dne 14. 12. 2022, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (dále jen „**NIS2**“). Právě s přicházející regulací dochází ke značnému rozšíření povinných subjektů. V oblasti zdravotnictví pak bude regulovanou službou mj. „poskytování zdravotní péče“. Zadavatel společně s ostatními výše uvedenými subjekty tedy s největší pravděpodobností naplní kritéria pro učení regulované služby. Transpoziční lhůta dle směrnice NIS2 požaduje účinnost nového zákona k 18. říjnu 2024. Poté budou mít subjekty lhůtu jimi poskytované regulované služby identifikovat, provést jejich registraci a zápis do evidence a následně musí začít plnit povinnosti plynoucí za ZKB, včetně toho, že do jednoho roku musí zavádět bezpečnostní opatření.

Na základě uvedeného lze tedy konstatovat, že je zcela na místě, aby takové subjekty postupovaly

již nyní v souladu s budoucí právní úpravou, jestliže se chtějí vyvarovat následnému nesouladu při zavádění bezpečnostních opatření a plnit povinnosti plynoucí ze ZKB. Jak známo, zadávací řízení na veřejnou zakázku dokáže být zdlouhavým procesem. Zároveň situace, kdy zadavatel vysoutěží něco, co se pro něho stává téměř ihned obsoletním, jde zcela zjevně proti základním principům zadávacího řízení a veřejných zakázek jako takových (zásada hospodárnosti, efektivnosti a účelnosti).

Co se týče zodpovězení Vašich otázek:

- je dle Vašeho odborného názoru předmětná analýza rizik provedená zadavatelem z formálního a obsahového hlediska v souladu s dotčenými právními předpisy (zejména ZKB a VKB) a obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti (tj. lege artis), a pokud ano,
- mohl dle Vašeho odborného názoru zadavatel v souladu s dotčenými právními předpisy (zejména ZKB a VKB) a obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti (tj. lege artis) zvolit v šetřeném případě i jiné technické opatření než sporné opatření, resp. bylo předmětné bezpečnostní opatření v podobě sporného opatření zvoleno v souladu s obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti (tj. lege artis)?

Postup zadavatele při tvorbě analýzy rizik, obsah analýzy rizik a způsob jejího provedení je třeba posuzovat i v kontextu předcházejících a navazujících kroků zadavatele tvořících v souhrnu proces řízení rizik. Proces řízení rizik sestává z hodnocení rizik (jehož součástí je identifikace, analýza a vyhodnocení rizik), výběru a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik [srov. § 2 písm. i) VKB]. Výběr konkrétního bezpečnostního opatření, jehož implementace sníží hodnotu rizika na akceptovatelnou úroveň, pak musí být založen nikoli pouze na samotné analýze rizik (jejímž výsledkem je striktně vzato pouze stanovení hodnoty rizika), nýbrž i na navazujícím vyhodnocení rizik (tedy určení, zda je riziko akceptovatelné či nikoli) a zvážení v úvahu přicházejících bezpečnostních opatření. Postup povinné osoby by přitom měl korespondovat s již nastavenými pravidly pro řízení rizik. **Pro posouzení správnosti postupu povinné osoby při tvorbě analýzy rizik je krom jiného nezbytné i posouzení toho, zda celý proces hodnocení rizik, do něhož tvorba analýzy rizik spadá a od jehož zbylých součástí je funkčně neoddělitelná, byl proveden v souladu s metodikou k tomu vyhotovenou** [srov. § 5 odst. 1 písm. a) VKB].

Po prostudování všech poskytnutých dokumentů NÚKIB shledal, že pro řádné zhodnocení postupu zadavatele při hodnocení rizik potřebuje od zadavatele některé věci vysvětlit. Dne 20. 12. 2023 se proto uskutečnilo jednání s panem Tomášem Šenkem, který je manažerem kybernetické bezpečnosti zadavatele a je rovněž autorem obou doručených dokumentů. Na tomto jednání se podařilo všechny nesrovnalosti vyjasnit a věc uzavřít s tím, že se jednalo o zjevnou chybu v psaní a počtech.

V doručených dokumentech jsme objevili drobné nesrovnalosti. V jednom dokumentu byla například stanovena hranice akceptovatelnosti na hodnotu 31 a ve druhém případě na 32.

Vyhodnocení varianty v .pdf a .xlsx se úplně neshodovalo. Došlo ke špatnému výpočtu rizika pro variantu II. a III. Správně měl být použitý vzorec jako ve variantě I., tedy aktivum x hrozba x zranitelnost. Místo toho byl použit vzorec aktivum x hrozba x hrozba. Na druhou stranu je třeba upozornit, že tato chyba neměla vliv na výsledek procesu hodnocení rizik. Došlo pouze k tomu, že namísto kritického (červená) bylo riziko vyhodnoceno jako vysoké (oranžová). V obou případech se však jedná o neakceptovatelná rizika.

Předložená dokumentace je jinak srozumitelná, návodná a je z ní zřejmé, jakým způsobem zadavatel při hodnocení rizik a tvorbě posuzované analýzy rizik postupoval. Dílčí nedostatky, která NÚKIB identifikoval, nemohou mít vliv na výsledky procesu hodnocení rizik. Na základě informací obsažených v dokumentech, které byly NÚKIB Vaším úřadem poskytnuty, pak NÚKIB uzavírá, že **předložená analýza rizik splňuje požadavky ZKB a VKB a je provedena v souladu s obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti**.

Ke druhá otázce lze uvést, že na základě vysvětlení a doložené analýzy rizik je evidentní, že varianta s použitím technických nebo programových prostředků společnosti Huawei Technologies Co., Ltd., Šen-Čen, Čínská lidová republika, a společnosti ZTE Corporation, Šen-Čen, Čínská lidová republika, přináší pro zadavatele rizika, která není schopen snížit, případně by taková bezpečnostní opatření na snížení těchto rizik přinesla nepřiměřeně vysoké finanční náklady. **Předmětné bezpečnostní opatření v podobě stanovené zadávací podmínky se proto jeví jako souladné s obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti**.

Postup zadavatele při hodnocení rizik a při navazujícím výběru bezpečnostního opatření je tedy z pohledu NÚKIB dostatečně zdokumentován a varování NÚKIB ze dne 17. prosince 2018 je správně zapracováno do procesu hodnocení rizik. **Z výše uvedených důvodu pak lze postup zadavatele označit za souladný se ZKB a VKB.**

S pozdravem

Elektronický podpis: 11.1.2024
Certifikát autora podpisu:
Jméno: Adam Kučínský
Vydal: I.CA EU Qualified CA2/RSA 06/2022
Platnost do: 22.5.2024 15:36 +02:00

datovou schránkou
Mgr. Zuzana Kutálková
vedoucí Oddělení veřejných zakázek 4
Úřad pro ochranu hospodářské soutěže
třída Kpt. Jaroše 7, 604 55 Brno