Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIDĚLENO • BRNO • 3. ZÁŘÍ 2025

VERZE DOKUMENTU: 1.0

METODICKÝ MATERIÁL K VAROVÁNÍ ZE DNE 3. ZÁŘÍ 2025

Podpůrný materiál

Obsah

Úvod

Národní úřad pro kybernetickou a informační bezpečnost (dále také jen jako „Úřad“) vydal dne 3. září 2025 varování (č.j. 6159/2025-NÚKIB-E/350) před hrozbou v oblasti kybernetické bezpečnosti spočívající

- v předávání systémových a uživatelských dat do Čínské lidové republiky, na území zvláštních administrativních oblastí či subjektům usídleným na území Čínské lidové republiky nebo zvláštních administrativních oblastí, a
- ve vzdálené správě technických aktiv vykonávané z území Čínské lidové republiky, zvláštních administrativních oblastí či ze strany subjektů usídlených na území Čínské lidové republiky nebo zvláštních administrativních oblastí,

(dále jen „Varování“).

Varování je dostupné na úřední desce Úřadu (https://nukib.gov.cz/cs/uredni-deska/).

Čínská lidová republika a zvláštní administrativní oblasti, jimiž jsou pro účely Varování jmenovitě Hongkong a Macao, jsou v rámci tohoto metodického materiálu společně označovány dále jen jako „Území“.

Účelem tohoto metodického materiálu je poskytnout jeho adresátům praktické pokyny a informace související se zohledněním Varování.

Adresáty tohoto metodického materiálu jsou veškeré povinné subjekty podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB“).

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno – Žabovřesky

E-mail: regulace@nukib.gov.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

1 Manažerské shrnutí

Prostřednictvím varování Úřad upozorňuje na existenci hrozby v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat. Subjekty, které spadají do regulace ZKB, jsou povinny se touto hrozbou dále zabývat a zohlednit ji v analýze rizik, kterou v souladu s požadavky 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“), již pravidelně provádí. Varování tedy neznamená bezpodmínečný zákaz předávání systémových a uživatelských dat na Území nebo subjektům na Území usídleným ani zákaz výkonu vzdálené správy technických aktiv z Území nebo subjekty na Území usídlenými, ale nutnost zvážit případné bezpečnostní riziko z toho plynoucí.

Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně tak jako široké veřejnosti, nezakládá varování Úřadu žádnou povinnost, a to ani zprostředkovaně. Tyto subjekty tedy nejsou podle ZKB povinny varování Úřadu zohlednit, varování však mohou zohlednit dobrovolně.

Varování vydaná přede dnem účinnosti zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále také jen jako „nZKB“) se považují za varování vydaná podle ZKB. U subjektů regulovaných podle nZKB, které budou poskytovateli regulované služby v režimu vyšších povinností, bude varování vstupovat do hodnocení rizik, obdobně jako tomu je podle ZKB. Subjekty, které budou podle nZKB poskytovateli regulované služby v režimu nižších povinností, mohou varování ve většině případů zohlednit dobrovolně. V případě veřejných zakázek budou mít tito poskytovatelé možnost varování zohlednit skrze požadavky na své dodavatele, které budou podloženy dobrovolně zpracovanou analýzou rizik.

Pro usnadnění orientace v procesu zohlednění Varování slouží následující vizualizovaný kontrolní seznam, který ve zjednodušené podobě uvádí oblasti, kterým by povinná osoba měla věnovat pozornost. Kontrolní seznam mohou využít také osoby, pro které zohlednění varování není zákonnou povinností, avšak samy ho chtějí zohlednit. Jednotlivá témata jsou dále rozvedena v příslušných kapitolách tohoto metodického materiálu.

CO

- Co je institut varování.
- O čem je toto Varování.

PROČ

- Důvody vydání Varování.

KDO

- Koho se Varování týká.

JAK

- Jak určit aktiva relevantní pro Varování.
- Jak řídit rizika vyplývající z hrozby, na kterou Varování upozorňuje.
- Jak zavést bezpečnostní opatření pro ošetření rizik.

VEŘEJNÉ ZAKÁZKY

- Samostatná problematika souladu Varování se zákonem o zadávání veřejných zakázek.

2 Institut varování

2.1 Kdy Úřad vydá varování

Úřad je zřízen jako ústřední orgán státní správy pro oblast kybernetické bezpečnosti. Mezi jeho základní poslání patří v souladu s § 22 ZKB vydávat opatření, zajišťovat prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací a plnit další úkoly v oblasti kybernetické bezpečnosti stanovené ZKB. Jedním z těchto úkolů je v souladu s § 12 ZKB vydávání varování před hrozbou v oblasti kybernetické bezpečnosti. V souladu se ZKB tedy Úřad vydá varování, dozví-li se zejména z vlastní činnosti, z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti.

2.2 Co představuje institut varování

Podle § 12 ZKB Úřad prostřednictvím varování upozorňuje na existenci hrozby v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat. Subjekty povinné podle ZKB se na základě varování musí hrozbou dále zabývat a zohlednit ji v analýze rizik, kterou tyto subjekty v souladu s požadavky ZKB a VKB již pravidelně provádí.

3 Důvody vydání Varování

Na základě vlastních poznatků Úřadu, doplněných o informace získané od partnerů Úřadu, bylo konstatováno, že předávání systémových a uživatelských dat na Území nebo subjektům na Území usídleným, stejně jako umožnění výkonu vzdálené správy technických aktiv z Území nebo subjekty na Území usídlenými, představuje pro Českou republiku bezpečnostní hrozbu, na niž je nutné prostřednictvím daného Varování oficiálně a veřejně upozornit.

Výše popsané předávání dat, stejně jako umožnění výkonu vzdálené správy technických aktiv, představuje pro Českou republiku bezpečnostní hrozbu zejména z následujících důvodů:

- právní prostředí Čínské lidové republiky je z pohledu bezpečnosti České republiky nedůvěryhodné, neboť čínským vládním orgánům umožňuje provádět významné zásahy do fungování soukromých společností, v souvislosti s nimiž dává čínským vládním orgánům četné nástroje pro vynucení spolupráce těchto společností na špionážních aktivitách Čínské lidové republiky (toto právní prostředí je přitom zcela reálně aplikovatelné též na území zvláštních administrativních oblastí),
- vliv čínských státních nebo státem podporovaných společností v oblasti evropské kritické infrastruktury současně dlouhodobě roste,
- dlouhodobě se formuje také technologická závislost České republiky na Čínské lidové republice, před níž varuje i Bezpečnostní informační služba České republiky,
- Čínská lidová republika, resp. na ni navázaní aktéři, prokazatelně dlouhodobě vyvíjí škodlivé aktivity, které jsou v příkrém rozporu s bezpečnostními zájmy České republiky, stejně jako bezpečnostními zájmy některých dalších členských států Evropské unie, potažmo i států mimo Evropskou unii,
- ZKB regulované systémy představují páteř zajišťující poskytování velmi důležitých služeb, narušení jejichž dostupnosti, důvěrnosti či integrity by mělo dopad na značnou část osob nacházejících se na území České republiky, a tudíž je z pohledu bezpečnosti České republiky rizikové spoléhat se v této souvislosti na řešení, jejichž prostřednictvím dochází k přenosu dat na výrokem daného Varování specifikovaná Území, resp. subjektům na těchto Územích usídleným, popř. řešení, jejichž vzdálená správa je z výše uvedených Území, resp. ze strany subjektů na těchto Územích usídlených, vykonávána.

4 Co varování znamená pro jednotlivé subjekty

4.1 Povinné orgány nebo osoby podle § 3 písm. c) až f) ZKB

Správci nebo provozovatelé informačních a komunikačních systémů kritické informační infrastruktury, správci nebo provozovatelé významných informačních systémů a správci nebo provozovatelé informačních systémů základních služeb jsou povinni podle § 5 VKB pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém a informační systém základní služby identifikovat rizika, hodnotit rizika a identifikovaná rizika řídit.

Na základě řízení rizik potom výše uvedené subjekty zavádějí a provádějí bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti v souladu s § 4 odst. 2 ZKB. Bezpečnostní opatření jsou blíže specifikována ve VKB. V souvislosti s řízením rizik musejí podle § 5 odst. 1 písm. h) bodu 3 VKB tyto subjekty zohlednit mimo jiné i opatření podle § 11 ZKB, tedy i varování vydané podle § 12 ZKB.

Na základě vydaného varování tedy musejí výše zmíněné povinné subjekty v rámci zavedeného řízení rizik provést analýzu rizik, ve které zohlední hrozbu, a následně na riziko reagovat zavedením bezpečnostních opatření, která musí být v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotou daného rizika.

Výše zmíněné povinné subjekty jsou současně povinny podle § 8 VKB stanovit pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací (jehož nedílnou součástí je i vyhodnocení rizik), seznamovat s nimi tyto dodavatele a vyžadovat po dodavatelích plnění těchto pravidel.

Na informační nebo komunikační systémy orgánů nebo osob podle § 3 písm. c) až f) ZKB, které nejsou uvedeny v prvním odstavci této podkapitoly, se výše uvedené povinnosti nevztahují.

4.2 Povinné orgány nebo osoby podle § 3 písm. h) ZKB – poskytovatelé digitálních služeb

Poskytovatel digitální služby podle § 29 VKB zavádí bezpečnostní opatření podle prováděcího nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018. Toto nařízení poskytovateli digitální služby ukládá pro informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb v souvislosti se zajišťováním digitální služby podle ZKB, povinnost zavést a provádět vhodná a přiměřená bezpečnostní opatření k řízení bezpečnostních rizik. Mimo jiné poskytovateli digitálních služeb toto prováděcí nařízení Komise v čl. 2 ukládá, aby v rámci řízení bezpečnosti informací provedl analýzu rizik a řídil dodavatele.

Z praktického pohledu by tedy i poskytovatelé digitální služby měli vydané varování vzít v úvahu při provádění analýzy rizik i při řízení dodavatelů, a to na základě povinností, které jim stanovuje výše zmíněné prováděcí nařízení Komise.

Na informační systémy nebo sítě elektronických komunikací, které poskytovatel digitálních služeb nevyužívá v souvislosti se zajišťováním digitální služby podle ZKB, se výše uvedená povinnost nevztahuje.

4.3 Orgány nebo osoby, které nespadají pod ZKB

Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně tak jako široké veřejnosti, nezakládá varování žádnou povinnost, a to ani zprostředkovaně. Je tedy na jejich zvážení, jak budou s hrozbou, na kterou varování upozorňuje, dále pracovat.

4.4 Varování po účinnosti zákona č. 264/2025 Sb., o kybernetické bezpečnosti

Dne 4. srpna 2025 byl ve Sbírce zákonů vyhlášen zákon č. 264/2025 Sb., o kybernetické bezpečnosti. Tento zákon nahradí po své účinnosti od 1. listopadu 2025 současný ZKB jakožto hlavní předpis upravující kybernetickou bezpečnost v České republice. Prováděcí právní předpisy k tomuto zákonu v současné době procházejí legislativním procesem – níže je na tyto návrhy prováděcích právních předpisů a jejich ustanovení odkazováno tak, jaký je jejich obsah v okamžiku vydání tohoto metodického materiálu.

Podle § 71 odst. 3 nZKB platí, že se varování vydaná podle ZKB před dnem nabytí účinnosti nZKB považují za vydaná podle nZKB. Jinými slovy, varování vydaná podle § 12 ZKB mají být považována za varování vydaná podle § 22 nZKB.

Poskytovatelé regulované služby v režimu vyšších povinností podle nZKB budou povinni zohlednit varování v rámci bezpečnostních opatření (jako součást řízení rizik). Pokud je subjekt regulovanou osobou podle ZKB a bude poskytovatelem regulované služby v režimu vyšších povinností podle nZKB, nic se pro něj nemění, neboť po vydání varování je subjekt povinen zohlednit obsah varování v rámci řízení rizik podle § 5 odst. 1 písm. d) VKB, a tedy v době nabytí účinnosti nZKB již bude varování zohledněno. Jestliže se subjekt nově stane regulovaným poskytovatelem regulované služby v režimu vyšších povinností, a dosud nespadal do regulace ZKB, tak se pro zohlednění varování uplatní roční přechodné období dané nZKB, které je stanoveno pro zavedení bezpečnostních opatřeních.

Zohlednění varování pro poskytovatele regulované služby v režimu nižších povinností podle nZKB bude s výjimkou situace popsané v následujícím odstavci dobrovolné. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností nepracuje se stejným ustanovením, které by ukládalo tuto povinnost přímo, jako je tomu v případě vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. I když poskytovatelé regulované služby v režimu nižších povinností nemají zákonnou povinnost varování zohlednit, je potřeba přiměřené zohlednění obsahu varování doporučit – stejně jako v případě ostatních poskytovatelů regulované služby bude pro některé subjekty taková hrozba rizikem, pro jiné ne.

Zohlednění varování může být pro poskytovatele regulované služby přeneseně povinné v případě, kdy je možné jej zohlednit ve smlouvě s dodavateli. Přestože vyhláška

o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností nestanoví zohlednění obsahu varování v řízení rizik, stále obsahuje ustanovení o řízení dodavatelů a požadavcích na smlouvy s nimi. Jedná se o to, že jedním z bezpečnostních opatření pro poskytovatele regulované služby v režimu nižších povinností je zajištění relevantních požadavků ve smlouvách, které uzavírá se svými dodavateli podle § 4 odst. 5 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. Aby došlo k naplnění požadavku na správné řízení dodavatelů, je potřeba zavádět náležitě také relevantní požadavky na smlouvy. Obsah varování, stejně tak jako jiné veřejné informace, mohou mít vliv na obsah relevantních požadavků na smlouvy s dodavateli a v takovém případě je potřeba je pro správné řízení dodavatelů také zohlednit.

Dobrovolnost zohlednění varování pro poskytovatele v režimu nižších povinností však nevylučuje to, že tento poskytovatel může zpracovat analýzu rizik pro účely veřejné zakázky a tím definovat požadavky na své dodavatele. Bližší informace o zohlednění varování ve veřejných zakázkách jsou uvedeny níže.

5 Postup zohlednění Varování v procesu řízení aktiv a rizik

V jednotlivých kapitolách níže je uveden postup, jak s Varováním pracovat v rámci procesu řízení aktiv a rizik. S ohledem na to, že Úřad v minulosti vydal obsáhlý materiál Průvodce řízením aktiv a rizik[1], který je pravidelně podle potřeby aktualizován a věnuje se problematice řízení aktiv a rizik detailně, doporučujeme uvedený materiál využít v případě, kdy zpracovatel proces řízení aktiv a rizik teprve zavádí.

5.1 Identifikace relevantních aktiv s ohledem na Varování

Pro to, aby mohlo být Varování zohledněno, je nutné nejdříve určit relevantní primární aktiva, tedy informace a služby, které jsou v rozsahu systému řízení bezpečnosti informací, a u kterých dochází k předávání systémových a uživatelských dat nebo ke vzdálené správě technických aktiv.

Po identifikaci primárních aktiv, kterých se Varování týká, je dále nutné provést mapování vazeb a souvislostí s podpůrnými aktivy. Podpůrnými aktivy jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému. V tomto kroku je důležité neopomenout zohlednit také to, zda je podpůrné aktivum využíváno k předávání či ukládání dat v rámci dodavatelského řešení, jako jsou různé formy cloudových řešení a podobně.

K účelu evidence primárních i podpůrných aktiv slouží v prvé řadě zejména evidence aktiv zpracovaná v souladu s požadavky VKB, v určitých případech však bude potřeba dále provést detailní posouzení aktiv, protože v určitých případech nemusí být z pouhé evidence patrné, že by k předávání systémových a uživatelských dat nebo ke vzdálené správě technických aktiv relevantních pro Varování u aktiv mohlo docházet.

Po provedení těchto kroků dojde k situaci, kdy je zmapováno, jaká primární a podpůrná aktiva jsou z pohledu Varování relevantní, tedy:

- u kterých primárních aktiv může docházet nebo dochází k předávaní systémových a uživatelských dat nebo ke vzdálené správě technických aktiv,
- prostřednictvím jakých podpůrných aktiv může docházet nebo dochází k předávání systémových a uživatelských dat nebo ke vzdálené správě technických aktiv.

5.1.1 Detailní posouzení aktiv

Protože ne ve všech případech bude na první pohled zřejmé, zda dochází nebo může docházet k situaci popsané ve Varování z prosté evidence aktiv, je nutné u některých aktiv přistoupit k detailnímu posouzení.

[1] Verze dokumentu aktuální ke dni vydání tohoto metodického materiálu je dostupná na odkaze: https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf

Toto detailní posouzení zahrnuje například nutnost nahlédnutí do smluv s dodavateli, provedení informačního šetření z otevřených zdrojů, či například kontrolu síťové komunikace aktiva. Níže jsou proto uvedeny příklady oblastí, na které je nutné se při posuzování primárních, potažmo podpůrných aktiv, dále zaměřit, aby mohlo dojít k náležitému zohlednění Varování.

Výběr konkrétních oblastí bude záležet zejména na možnosti využití relevantních nástrojů pro danou analýzu a odborných znalostech osob pověřených touto analýzou. Níže uvedené oblasti zobrazují demonstrativní výčet, který má sloužit zejména jako inspirace pro osoby pověřené řešením této problematiky.

Interní evidence aktiv

Povinné osoby a orgány by měly nejen z důvodů regulatorních požadavků, ale i ve vlastním zájmu, mít přehled o tom, jakými aktivy disponují, potažmo jaká jsou aktiva v rozsahu systému řízení bezpečnosti informací.

Kromě evidence aktiv v souladu s požadavky VKB je vhodné provést šetření např. v rámci:

- Evidence smluv
- Evidence majetku, inventář majetku (např. v rámci ERP či ticketovacího systému)
- Dotazování osob odpovědných za správu majetku, jednotlivé informační systémy či technická aktiva
- Seznam technických aktiv (např. device management, mobile device management)
- Přezkum známých hostname a MAC adres technických aktiv (např. OUI výrobce)
- Konfigurace infrastruktury (např. v rámci nastavení virtualizované infrastruktury)
- Konfigurační databáze
- Topologie či schémata sítě

Na základě výstupů z těchto šetření lze vyhodnocovat indikátory aktivit relevantních pro toto Varování např.:

- Přezkum smluv a dohod s dodavateli
- Dodavatel aktiva z Území
- Zasílání dat na území

Řízení dodavatelů

U aktiv je vhodné provést na úrovni relevantních podpůrných aktiv analýzu dodavatelů, kteří se podílejí na předávání dat, nebo prostřednictvím kterých dochází ke vzdálené správě daných technických aktiv. V tomto případě je nutné neopomenout např. dodavatele cloudových řešení. U takových dodavatelů je pak nutné odpovědět si, případně hledat odpovědi na otázky:

- Co tito dodavatelé či jejich subdodavatelé v dodavatelském řetězci dodávají?
- Kdo vykonává servis technických aktiv či systémů ve stanoveném rozsahu?
- Kam jsou data v celém jejich životním cyklu odesílána a předávána, případně v jaké podobě?
- S jakými subdodavateli dodavatel spolupracuje v rámci daného aktiva či poskytování dodavatelské služby?

Na základě výše položených otázek je na místě podniknout určité kroky za účelem zjištění skutečného stavu v rámci dodavatelského řetězce, tedy zjištění, zdali nejen na úrovni přímého dodavatele ale i např. jeho subdodavatelů nedochází k činnostem relevantním pro toto Varování.

Přiměřenost zjišťování skutečného stavu v rámci dodavatelského řetězce se bude odvíjet od hodnoty aktiv relevantních pro toto Varování v rámci daného dodavatelského řetězce.

Mezi vhodné kroky v oblasti zjištění skutečného stavu v rámci řízení dodavatelů a subdodavatelů patří např. přezkum smluv a dohod s dodavateli (vč. technických specifikací v dodatcích, přílohách a další dokumentaci) nebo přímé dotazování v rámci daného dodavatelského řetězce.

Zohlednění vlastnických vztahů u dodavatelů a subdodavatelů

Rozkrývání vlastnické struktury a rizikových vazeb dodavatelů či subdodavatelů lze do značné míry provádět za pomoci informací z otevřených zdrojů. Tímto způsobem lze v některých případech odhalit relevantní vazby na rizikové prostředí, aniž by musely být vynaloženy vysoké finanční náklady.

Tento proces by měl zahrnovat identifikaci subjektu ve veřejných rejstřících nebo v nekomerčních agregátorech podnikových dat, včetně těch, které obsahující specificky informace o společnostech působících na Území (ovšem s tím, že přístup k některým těmto službám může být geograficky omezen). Identifikační a kontaktní údaje by se následně měly stát předmětem vyhledávání v internetových vyhledávačích, výsledky tohoto vyhledávání by následně měly být kriticky a opatrně vyhodnoceny s ohledem na věrohodnost zdrojů, ze kterých nalezené informace pocházejí. Zohledněn by přitom neměl být pouze aktuální stav, ale i okolnosti založení subjektu a jeho historický vývoj.

Příklady identifikačních a kontaktních údajů, které mohou být předmětem dalšího vyhledávání:

- Název, včetně originálního názvu v zemi původu
- Registrační číslo, např. IČO nebo obdobný identifikátor
- Sídlo
- Země (jurisdikce) registrace
- Webová doména
- Jména klíčových osob

- E-mailové adresy
- Telefonní čísla

Je vhodné zohlednit, že subjekty mohou být součástí komplexní korporátní struktury se složitým vlastnickým řetězcem. Relevantní může být přímý i nepřímý vlastnický vliv. Kromě veřejných rejstříků a evidencí mohou být nápomocny i původní dokumenty subjektu, například jím publikované výroční zprávy nebo informace obsažené na webu subjektu. Informace v těchto původních dokumentech by měly být porovnávány s dalšími dostupnými zdroji. Zvýšená pozornost by měla být věnována nejen společnostem sídlícím na Území, ale také společnostem se sídlem v jurisdikcích s nízkou mírou transparentnosti (např. tzv. daňové ráje), u kterých může být vazba na společnosti relevantní pro Varování či Území hůře zjistitelná a prokazatelná.

Pokud subjekt disponuje webovou doménou, je užitečné detailně se seznámit s jejím obsahem. Pro dohledání potenciálně relevantních změn obsahu webové prezentace v čase lze využívat služby nekomerčních internetových archivů. Lze také využívat nekomerční nástroje na analýzu domén pro identifikaci majitele domény, registrátora, lokality hostování, používaných IP adres a dalších informací dostupných o doméně subjektu.

Vysokou vypovídací hodnotu může mít i přítomnost subjektu na sociálních sítích, zejména pokud z ní vyplývá orientace na prostředí Území.

Dále, doporučujeme zvážit i ověření, zda subjekt nebo na něj navázané entity nejsou uváděny na sankčních seznamech (ať již tuzemských či zahraničních). K této činnosti lze využívat dostupné agregátory sankčních seznamů.

Povinné osoby a orgány mohou, s ohledem na hodnocení aktiv, zvážit využití i komerčních nástrojů či služeb, které jsou zaměřené na odhalování vazeb na prostředí Území.

Analýza komunikace

Na technické úrovni lze provést analýzu prostředí pomocí nástrojů umožňujících vyhodnocování na různých komunikačních vrstvách referenčního modelu ISO/OSI. Mezi tyto nástroje patří např.:

- Samotné aktivní síťové prvky
- Firewally
- Síťové sondy
- Pasivní či aktivní softwarové nástroje pro vyhodnocování komunikace
- Nástroje pro detekci či prevenci síťových anomálií a nežádoucí komunikace (IDS/IPS)
- Nástroje pro monitoring rozhraní, portů či fyzického připojení
- Logovací nástroje v rámci cloudových služeb
- Nástroje provádějící behaviorální analýzu nad technickými aktivy

- Nástroje pro sběr a vyhodnocování událostí (SIEM) nejen z výše uvedených nástrojů

Na základě výstupů z těchto nástrojů lze vyhodnocovat indikátory aktivit relevantních pro toto Varování, např.:

- IP adresy, ASN (řešeno např. v rámci nastavení geolokalizace/geofencingu)
- DNS dotazy, potažmo URL a doménová jména
- Nastavení SSL/TLS certifikátů (např. vydavatel)
- Korelace událostí při zohlednění možného času komunikace z Území

Možnosti zjištění skutečného stavu v této oblasti jsou limitovány nástroji a odbornými znalostmi. Také, z povahy fungování internetové komunikace, která s největší pravděpodobností nebude bez hlubší analýzy přímo vyhodnotitelná jako spojitelná s Územím (např. prokazatelná komunikace s IP adresami v ASN v rámci Území), tedy jako relevantní pro toto Varování, je nutné vynaložit přiměřenou míru úsilí s cílem zjištění celého možného komunikačního řetězce.

Technická analýza popsaná v této kapitole by měla probíhat průběžně v zájmu zjištění případných změn v oblasti technických aktiv, které by mohly být pro Varování relevantní (např. vznik nových komunikačních kanálů).

5.2 Zohlednění hodnoty aktiv

Po identifikaci všech relevantních primárních a podpůrných aktiv, prostřednictvím kterých dochází k předávání systémových a uživatelských dat nebo k přístupu k vzdálené správě technických aktiv, je vhodné přezkoumat hodnotu aktiv, tedy především u podpůrných aktiv zohlednit vazby na primární aktiva. Hodnota aktiva se nejčastěji určuje na základě jeho hodnocení z hlediska důvěrnosti, dostupnosti a integrity. Více informací případně naleznete v Průvodci řízením aktiv a rizik.

Výstupem této části je znalost hodnoty výše uvedených relevantních aktiv.

5.3 Zohlednění Varování v rámci procesu řízení rizik

Detailní návod pro proces řízení rizik je uveden v Průvodci řízením aktiv a rizik. Níže je uvedeno doplnění procesu řízení rizik o zohlednění tohoto Varování.

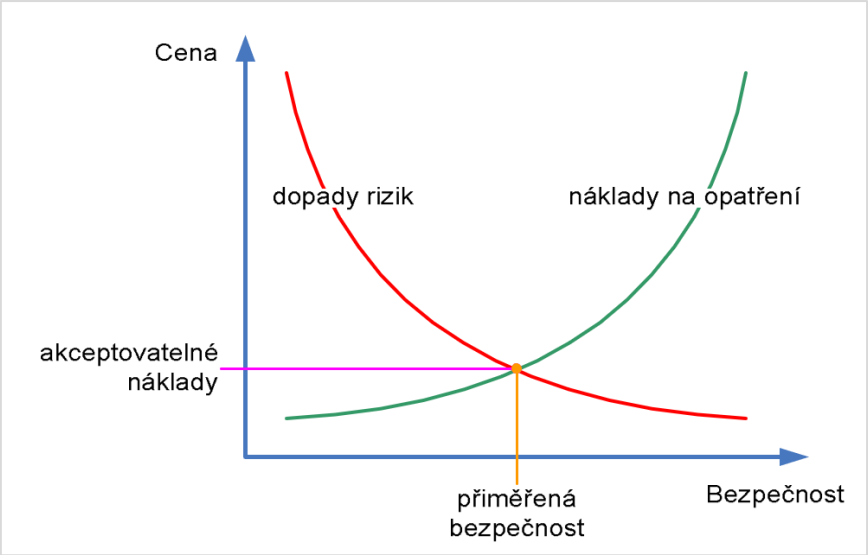
Základní princip řízení rizik zůstává při zohlednění Varování zachován, pouze dochází u vybraných aktiv k zohlednění nové hrozby a její hodnoty, což v některých případech povede k nalezení či určení nových relevantních zranitelností, a tedy i rizik vyplývajících z Varování, která bude potřeba ošetřit. Jedna z příkladových možností výpočtu hodnoty rizika je následující:

Riziko = hodnota aktiva (dopad) x hrozba x zranitelnost

Výsledná míra rizika následně definuje požadavky na ochranu, tedy na míru zavedení konkrétních bezpečnostní opatření, která je nutné zavést. To znamená, že bezpečnostní opatření snižují možnost naplnění nežádoucích jevů.

Akceptovatelné náklady na bezpečnost

Upozorňujeme, že náklady na bezpečnostní opatření by však měly být vždy přiměřené a neměly by převýšit náklady spojené s následky realizace rizika. To ilustruje následující schéma.



Obrázek 1 - Akceptovatelné náklady[2]

5.3.1 Zohlednění Varování v rámci analýzy rizik

Na základě provedeného detailního posouzení aktiv došlo k identifikaci aktiv, kterých se Varování týká a která mohou být ohrožena. U těchto aktiv bude nutné zohlednit hrozby, které Varování uvádí, a vytvořit relevantní kombinace hrozeb a zranitelností a následně podle stanoveného vzorce vyčíslit hodnotu rizika.

> Ze skutečností uvedených ve vydaném Varování vyplývá, že hrozbu, na kterou Varování upozorňuje, je v souladu s VKB potřeba hodnotit na úrovni **Vysoká, tedy jako pravděpodobnou až velmi pravděpodobnou**. V případě užití jiné stupnice hodnocení hrozby oproti uvedené ve VKB, je nutno tuto hrozbu ohodnotit způsobem odpovídajícím příslušné úrovni podle VKB.

Dalším krokem je identifikace relevantních zranitelností ve vztahu k danému aktivu a hrozbě z Varování. Příkladem takových zranitelností může být:

- Nedostatečné šifrování při přenosu dat
- Zastaralé nebo slabé šifrovací algoritmy
- Nedostatečné logování a provozní monitoring
- Zranitelnosti nástroje pro vzdálenou správu

[2] Viktor ONDRÁK, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

- Nedostatečně nastavený proces řízení dodavatelů jako neexistující pravidla pro dodavatele, či nedostatečně stanovené smluvní podmínky

Konkrétní hodnotu zranitelnosti doplní zpracovatel, zpravidla manažer kybernetické bezpečnosti, na základě rozhovoru s garantem aktiva, dostupných informací, případně odborných zkušeností.

Po vytvoření relevantních kombinací hrozeb, zranitelností a dotčených aktiv je možné zjistit výslednou hodnotu rizika, se kterou je nutné dále pracovat.

Účel analýzy rizik vzhledem k Varování

V případě, že analýza rizik bude dále sloužit jako podklad pro veřejné výběrové řízení, je vhodné, aby z hodnocení rizik, které slouží jako podklad pro výběr konkrétních bezpečnostních opatření, bylo zřejmé porovnání, jakým způsobem jsou hodnocena rizika související s předmětem Varování a jak jsou hodnocena rizika, která pod předmět Varování nespadají, tedy u nich není relevantní hrozba umožňující předávání systémových a uživatelských dat na Území anebo možnost výkonu vzdálené správy technických aktiv z Území.

Právě na tomto porovnání bude založen případný výstup dané analýzy rizik a závěr o tom, že použití daných podpůrných aktiv (např. technických aktiv, případně spolupráce s dodavatelem, který zajišťuje provoz, či správu dat a podobně) představuje v konkrétním případě neakceptovatelné riziko, které je potřeba dále ošetřit např. vyloučením konkrétní technologie z veřejné zakázky (více viz níže).

5.4 Zvládání rizik

Pokud vzniklé riziko spojené s předmětem Varování přesáhne akceptovatelnou úroveň, kterou má povinná osoba stanovenou (např. v souladu s požadavky VKB), je nutné přistoupit k zvládání (ošetření) daného rizika, které má za cíl řešit jeho případný negativní dopad.

Zvládání rizik může mít formu např.:

- Vyhnutí se riziku
    - Úplné odstranění rizika např. formou odstranění relevantního aktiva a jeho náhradou za jiné.
    - Tento způsob zvládání daného rizika je zpravidla nejúčinnější, a tedy i preferovanou, formou zvládání rizik.
- Snižování rizika (modifikace rizika, mitigace, redukce)
    - Přijetí bezpečnostních opatření v takové míře, že riziko klesne na akceptovatelnou úroveň (demonstrativní příklady pro toto Varování uvedeny níže).
- Akceptace rizika
    - Akceptované riziko je nutné evidovat a pravidelně jej kontrolovat, aby bylo povědomí o tom, zda nedošlo např. ke vzniku incidentu z něj vyplývajícího.

Současně by měly existovat strategie postupu pro případ řešení takového incidentu.

- Tento způsob zvládání rizika je ve většině případů vhodný jen krátkodobě, např. než jsou alokovány finanční prostředky na snížení rizika.

- Přenesení nebo sdílení rizika
  - Spočívá v zapojení, potažmo spoluúčasti, další strany, ať už interně či externě (např. sdílení následků dopadu daného rizika ve sdružení více společností či pokrytí následků v rámci pojištění).
  - Je vždy potřeba mít na paměti, že povinná osoba má vždy nepřenositelnou odpovědnost za to, že riziko bude nějakým způsobem řešeno.

Při zvládání rizik by mělo dojít k prioritizaci tak, aby nejdříve došlo k vyřešení nejvyšších rizik (s potenciálně nejvyšším dopadem), tedy ideálně i ke snížení všech rizik, která byla vyhodnocena jako neakceptovatelná.

5.4.1 Příklady zvládání rizik

Vzhledem k velké diverzitě informačních a komunikačních systémů, které spadají pod ZKB, nelze konkrétní příklady pro zvládání rizik, zejména bezpečnostní opatření pokrývající konkrétní rizika, paušálně specifikovat, jelikož je třeba zohledňovat příslušné prostředí a technologie organizace.

Vyloučení relevantního aktiva

Absolutním řešením z pohledu ošetření jakéhokoliv rizika je zbavit se příčiny vzniku daného rizika, tedy v tomto případě odstranění daného aktiva. Jestliže existuje možnost odstranění či vyloučení aktiva, které je spojeno s relevantní zranitelností a hrozbou vyplývající z tohoto Varování, a zároveň skrze např. použití alternativních nerizikových aktiv nebude ovlivněno fungování informačních systémů organizace či poskytování jejích služeb, mělo by toto řešení být preferovanou variantou.

Fyzické oddělení

Relevantní technická aktiva nejsou fyzicky propojena s ostatními technickými aktivy informačního systému (anglicky tzv. air gap), nejsou připojena ke komunikační síti pomocí drátového ani bezdrátového připojení.

Logické oddělení

Relevantní technická aktiva jsou fyzicky propojena s ostatními technickými aktivy informačního systému, avšak jsou oddělena na logické úrovni jako např. segmentace, segregace či mikrosegmentace komunikační sítě (využívající technologie firewallů, VLAN, ACL atd.) či oddělení na aplikační úrovni např. v rámci virtualizace, sandboxingu či oddělení domén.

Sledování komunikace a provozu

Komunikace relevantních technických aktiv je sledována, monitorována a vyhodnocována např. prostřednictvím síťových sond, IDS, IPS, EDR, NDR, XDR, nástrojů pro behaviorální analýzu, log agentů či jiných zdrojů logů, a/nebo SIEM.

Omezení komunikace na pouze nutnou

Komunikace relevantních technických aktiv je omezena pouze na nezbytně nutnou (tzv. komunikační whitelisting) nejčastěji pomocí aktivních síťových prvků (na úrovni IP adres, rozhraní, portů, protokolů, mikrosegmentace atd.) tak, aby bylo zabráněno realizaci nežádoucí komunikace, která není potřebná pro provoz daného aktiva, a mohla by naopak být zneužita k nežádoucím účelům.

Omezení vzdálené správy

Vzdálená správa relevantních technických aktiv je řízená. Není povolena bez časového omezení odkudkoliv, z jakéhokoliv zařízení, bez logování přístupů, bez jednoznačného ověření identity spravujícího. V této oblasti bude vhodnost bezpečnostních opatření záviset z velké míry na technických omezeních a možnostech konkrétního řešení dané vzdálené správy. Některá opatření v této oblasti lze realizovat i pomocí aktivních síťových prvků, firewallů či pokročilých nástrojů pro správu privilegovaných i vzdálených oprávnění (např. PIM/PAM).

Dokumentace

Zavedení relevantních bezpečnostních opatření by se mělo náležitě projevit i v relevantní provozní a bezpečnostní dokumentaci. Např. v případě zavedení organizačního bezpečnostního opatření, které omezuje vkládání citlivých informací do určitého informačního systému a jeho technických aktiv, je nutné náležitě aktualizovat dokumentaci k tomuto informačnímu systému za účelem vynutitelnosti požadavku a rozšíření povědomí o tom, že daná data nemají být do něj vkládána.

Řízení dodavatelů

Proces analýzy a řízení rizik uvedených výše je potřeba provést také v rámci výběru dodavatele a dané hodnocení (více k veřejným zakázkám viz kapitola níže), stejně jako výsledná opatření, je třeba promítnout do smluv s dodavateli. V souladu s § 4 odst. 4 ZKB jsou orgány a osoby uvedené v § 3 písm. c) až f) ZKB povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém, a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou.

V tomto případě může být vhodným bezpečnostním opatřením úprava pravidel pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací organizace, seznámení dodavatelů s těmito pravidly a vyžadování plnění těchto pravidel po dodavatelích. Bezpečnostní opatření definuje VKB, přičemž specifická úprava relevantních ustanovení do dodavatelských smluv je upravena v příloze VKB. Do těchto pravidel je na základě výsledků hodnocení rizik

vhodné uvést ustanovení, které bude upravovat možnost předávání systémových a uživatelských dat na Území či vzdálenou správu z Území.

Rozvoj bezpečnostního povědomí, vzdělávání a školení

Obdobně jako u jiných hrozeb a rizik v oblasti kybernetické bezpečnosti je žádoucí náležitě poučit všechny relevantní osoby (zejména např. vrcholné vedení, bezpečnostní role, administrátory, dodavatele, zaměstnance) o tom, jak je daná problematika ovlivňuje a jak předcházet z ní plynoucím rizikům. Toto poučení by mělo být realizováno systematicky v rámci doplnění plánu rozvoje bezpečnostního povědomí a rozšíření témat v rámci školení v oblasti kybernetické bezpečnosti.

Řízení výjimek z bezpečnostních opatření

V praxi se často stává, že některé věci nelze standardizovat a je potřeba vytvořit výjimky. V takovém případě je vhodné mít stanovený postup, za jakých podmínek lze výjimku udělit, a tyto výjimky také řídit. Řízením výjimek je v tomto případě myšleno evidovat udělené výjimky a aktivně usilovat o to, aby byly výjimky udělovány jen ve výjimečných případech a co nejdříve odstraňovány. Je nezbytné, aby výjimky byly vhodným způsobem řízeny, evidovány, podléhaly patřičnému schválení a pravidelnému přezkumu tak, aby nevznikaly či nepřetrvávaly výjimky nadbytečné. Toto bezpečnostní opatření bývá zpravidla spojeno i s dočasnou akceptací daného rizika.

Akceptace rizika

Akceptace může být pasivní (např. u malých a středních rizik, kde nebyla nalezena smysluplná opatření), což znamená, že nezavádíme žádné opatření kromě záznamu daného rizika, anebo také aktivní, což znamená, že vytvoříme v plánování lidských a finančních zdrojů určitou rezervu, která by měla případný výskyt rizika pokrýt, např. v plánu zvládání rizik.

Akceptovaná rizika nejsou dále řešena, nicméně je třeba je dále v průběhu realizace monitorovat a prověřovat, zdali se jejich parametry nemění.

6 Soulad se zákonem o zadávání veřejných zakázek

Úřad upozorňuje, že níže uvedené nastiňuje možnosti správců systémů při zajištění splnění povinností podle ZKB v souladu s předpisy regulujícími zadávání veřejných zakázek. Aplikaci níže nastíněných postupů je však třeba vždy zvažovat ve světle skutkových okolností konkrétního případu. K rozhodování o tom, zda je postup zadavatele souladný s pravidly obsaženými v zákoně č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), je pak příslušný Úřad pro ochranu hospodářské soutěže (dále jen „ÚOHS“), nikoli Národní úřad pro kybernetickou a informační bezpečnost.

ZZVZ i ZKB jsou zákonnými předpisy stejné právní síly, nenacházejí se v žádném stavu vzájemné nadřízenosti či podřízenosti, oba právní předpisy obecně nejsou v rozporu a orgány a osoby, které současně spadají do působnosti obou zákonů, jsou při své činnosti povinny postupovat tak, aby dostály oběma právním předpisům.

Proces analýzy a řízení rizik uvedený výše je nezbytné promítnout také do celého životního cyklu dodavatelských vztahů – od předběžného průzkumu trhu přes nastavení zadávacích podmínek až po kontrolu plnění a případné ukončení smlouvy.

Podrobná doporučení, včetně vzorových formulací do zadávacího řízení, obsahuje metodický materiál „Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost“ (dále jen „metodika k VZ a KB“)[3] – zejména:

- **kapitola 2** – Zohlednění požadavků vyplývajících z vyhlášky o kybernetické bezpečnosti při zadávání,
- **kapitola 3** – Omezení nákupu rizikových technologií,
- **kapitola 6** – Řízení poddodavatelů.

Obecně musí zadavatel při zadávání veřejných zakázek postupovat podle ZZVZ. Tento zákon v § 36 odst. 1 stanoví, že zadavatel nesmí vytvářet při stanovování zadávacích podmínek „*bezdůvodné překážky hospodářské soutěže*“. V případě, že oprávněná autorita (zde Úřad), která k tomuto kroku disponuje zákonným zmocněním (zde v § 22 písm. b) ZKB), vydává akt (zde Varování), který může v konkrétních případech vést k omezení hospodářské soutěže, nemůže být dodržení tohoto omezení při tvorbě zadávacích podmínek považováno za vytváření bezdůvodné překážky hospodářské soutěže. Tedy hospodářskou soutěž v tomto případě lze omezit již při stanovení zadávacích podmínek a nejedná se tím o porušení ZZVZ.

Je nutné si uvědomit, že každá zadávací podmínka omezuje hospodářskou soutěž. Zákaz omezit soutěž tedy neplatí absolutně, ale je vždy nutno zohlednit odůvodněné potřeby a požadavky zadavatele. Ten je oprávněn stanovit i takové zadávací podmínky, v jejichž důsledku bude určitá skupina dodavatelů z možnosti ucházet se o veřejnou zakázku vyloučena, musí však unést důkazní

[3] https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/metodiky-navody-doporuceni-a-standardy/

břemeno, že se nejedná o bezdůvodnou překážku hospodářské soutěže, tj. že příslušná zadávací podmínka má oporu v legitimních potřebách zadavatele (srov. rozsudek KS v Brně ze dne 30. září 2021 sp. zn. 29 Af 53/2019; dříve obdobně R 124/2018 z 19. října 2018 či R 216/2019 z 24. ledna 2020). Nadto ve vztahu k orgánům a osobám uvedeným v § 3 písm. c) až f) ZKB ustanovení § 4 odst. 4 ZKB stanoví, že jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém nebo informační systém základní služby a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle ZKB nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Zadavatelé by měli při tvorbě smluvních podmínek zejména:

1. **Explicitně převést relevantní bezpečnostní opatření (§ 4 odst. 4 ZKB, § 8 VKB)** do svých požadavků na dodavatele a poddodavatele a zpřesnit je podle metodiky k VZ a KB (např. doložení certifikátu podle normy ISO 27001, povinnost hlásit změny v dodavatelském řetězci, sankční ujednání).
2. **Stanovit mechanismus průběžného zákaznického auditu** – kontrolní právo zadavatele provést audit zaměřený na to, zda nedochází k předávání dat na Území.
3. **Použít tzv. negativní technické podmínky** (vyloučení určitých řešení nebo lokalit datových center) jen tam, kde to prokazatelně plyne z analýzy rizik.
4. **Opřít se o aktuální rozhodovací praxi ÚOHS a správních soudů.**

Tímto způsobem lze naplnit povinnost řídit rizika spojená s dodavateli (§ 8 odst. 1 písm. e) VKB) a zároveň minimalizovat riziko, že zadavatel poruší § 36 odst. 1 ZZVZ (zákaz bezdůvodných překážek hospodářské soutěže).

Obecně lze odkázat rovněž na dokument Úřadu „Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení“[4].

Uvedený materiál se týká varování ze dne 17. prosince 2018 před použitím technických a programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation (č. j. 3012/2018-NÚKIB-E/110, dále jen „varování HUA a ZTE”), avšak postupy a procesy spojené se zadávacím řízením na veřejnou zakázku lze použít obdobně.

Je však potřeba zvolit odpovídající postupy ve vztahu k tomu, v jaké fázi se dané výběrové řízení nachází:

- Fáze přípravy na veřejnou zakázku (příprava zadávací dokumentace/zadávacích podmínek vč. smluvních podmínek).

[4] https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/materialy-k-zakonu-o-kyberneticke-bezpecnosti/).

- Fáze probíhajícího zadávacího řízení.
- Fáze po skončení zadávacího řízení a zadání zakázky uchazeči.

6.1 Fáze přípravy na veřejnou zakázku

V souladu s § 8 odst. 1 písm. e) VKB musí povinná osoba řídit rizika spojená s dodavateli. Je tedy nutné provedení analýzy rizik podle § 5 VKB a následné zapracování jejího výsledku přímo do zadávací dokumentace.

Kritéria a scénáře, kdy může být účastník vyloučen nebo technologie nepřijata, musí být definovány už v zadávacích podmínkách (viz metodika k VZ a KB). Vhodné je použít např. technické podmínky (§ 37, § 89 ZZVZ), kvalifikační kritéria (§ 73 a násl. ZZVZ), nebo kritéria kvality (§ 116 ZZVZ) zaměřená na úroveň bezpečnosti.

6.2 Fáze probíhajícího zadávacího řízení

a) V rámci zadávacího řízení neuplynula lhůta pro podání žádosti o účast, předběžných nabídek nebo nabídek

V takovém případě lze po provedení analýzy rizik v souladu s ustanovením § 99 ZZVZ změnit nebo doplnit zadávací podmínky obsažené v zadávací dokumentaci. Změna nebo doplnění zadávací dokumentace musí být uveřejněna nebo oznámena dodavatelům stejným způsobem jako zadávací podmínka, která byla změněna nebo doplněna (zpravidla uveřejněním na profilu zadavatele, ve Věstníku veřejných zakázek, resp. Úředním věstníku Evropské unie).

Zde Úřad upozorňuje na povinnost vyplývající z druhého odstavce výše citovaného ustanovení ZZVZ, kdy je zadavatel povinen přiměřeně prodloužit lhůtu pro podání žádostí o účast, předběžných nabídek nebo nabídek. ZZVZ v tomto ustanovení dále ukládá zadavateli povinnost prodloužit lhůtu tak, aby od odeslání změny nebo doplnění zadávací dokumentace činila nejméně celou svou původní délku v případě takové změny nebo doplnění zadávací dokumentace, která může rozšířit okruh možných účastníků zadávacího řízení. Byť úpravou zadávacích podmínek podle varování dochází *de facto* spíše k omezení okruhu možných účastníků, Úřad vycházeje ze zásad uvedených v ustanovení § 6 ZZVZ doporučuje prodloužit lhůtu pro podání žádostí o účast, předběžných nabídek nebo nabídek tak, aby činila nejméně celou svou původní délku, a to z důvodu, že by uchazeči za změněných podmínek mohli nabídnout i jiné produkty, než původně zamýšleli, příp. z kterých vycházeli při zvažování, zda v daném zadávacím řízení podají žádost o účast, předběžnou nabídku nebo nabídku, a k učinění této úvahy je třeba uchazečům poskytnout adekvátních prostor.

b) V rámci zadávacího řízení již uplynula lhůta pro podání nabídek

Po provedení analýzy rizik lze buď pokračovat v zadávacím řízení a případně přijmout bezpečnostní opatření ke snížení rizika (aniž by tím byl dotčen postup v zadávacím řízení), nelze-li, pak zrušit zadávací řízení z důvodů podle § 127 odst. 2 písm. d) ZZVZ. Důvodem pro tento krok pak je, že v průběhu zadávacího řízení se podle názoru Úřadu vyskytly důvody hodné zvláštního

zřetele (bylo vydáno varování národní autoritou k tomu oprávněnou), pro které nelze po zadavateli požadovat, aby v zadávacím řízení pokračoval (nedostal by plnění odpovídající všem podmínkám, kterými je povinen se řídit vč. varování Úřadu) a nadto zadavatel tyto důvody nezpůsobil (je tak donucen činit na základě objektivních skutečností vzniklých vně zadavatele).

Úřad zde upozorňuje, že vydání varování nelze automaticky považovat za důvod pro vyloučení uchazeče ze zadávacího řízení. I nadále platí, že zadavatel je oprávněn vyloučit uchazeče ze zadávacího řízení pouze z důvodů stanovených v ZZVZ (zadavatel by tedy musel varování Úřadu, resp. důsledky plynoucí z jeho vydání, podřadit pod některý z důvodů uvedených v § 48 ZZVZ).

6.3 Fáze po skončení zadávacího řízení a zadání zakázky uchazeči

V souladu s § 8 odst. 1 písm. e) VKB musí povinná osoba řídit rizika spojená s dodavateli. Je tedy nutné provedení analýzy rizik podle § 5 VKB a na základě jejího výsledku provést jedno z následujících:

a) **V případě potřeby zvážit nasazení bezpečnostních opatření ke snížení rizik.**

Úřad v této souvislosti upozorňuje na ustanovení § 222 odst. 1 ZZVZ, podle něhož zadavatel nesmí umožnit podstatnou změnu závazku ze smlouvy na veřejnou zakázku po dobu jeho trvání bez provedení nového zadávacího řízení podle ZZVZ.

V případě plnění realizovaných na základě rámcové dohody Úřad upozorňuje na ustanovení § 131 ZZVZ, podle něhož zadavatel nesmí umožnit podstatnou změnu podmínek rámcové dohody po dobu jejího trvání bez provedení nového zadávacího řízení podle ZZVZ, přičemž zadavatel nesmí umožnit ani podstatnou změnu podmínek uvedených v rámcové dohodě při zadávání veřejných zakázek na základě této rámcové dohody.

Co je podstatnou změnou závazku podle ZZVZ, je třeba vždy posuzovat individuálně vzhledem k charakteru původní veřejné zakázky a jednotlivých učiněných změn, přičemž toto posouzení vždy přísluší zadavateli.

b) **V případě, že není možné přijmout bezpečnostní opatření ke snížení rizika, nahradit technické a programové prostředky na základě nového zadávacího řízení.**

V této souvislosti Úřad uvádí, že možnost ukončení smlouvy je v ZZVZ řešena v ustanovení § 223. Podle tohoto ustanovení může zadavatel závazek ze smlouvy na veřejnou zakázku vypovědět nebo od ní odstoupit v případě, že v jejím plnění nelze pokračovat, aniž by byla porušena pravidla uvedená v § 222 ZZVZ. Současně tím není dotčeno právo zadavatele ukončit závazek ze smlouvy na veřejnou zakázku podle jiných právních předpisů (typicky zákona č. 89/2012 Sb., občanský zákoník) či smluvních ujednání v uzavřených smlouvách.

Výše uvedené se vztahuje na zadavatele ve smyslu § 4 ZZVZ, tedy nejen na veřejné zadavatele, ale mimo jiné též na další osoby, které při výkonu relevantní činnosti zadávají sektorovou zakázku podle ustanovení § 151 a násl. ZZVZ, a to v míře dané jednotlivými ustanoveními ZZVZ.

6.4 Rozhodovací praxe

Z rozhodovací praxe ÚOHS lze pak poukázat na rozhodnutí vydaná v souvislosti s varováním HUA a ZTE. Například rozhodnutí ze dne 6. listopadu 2019 (sp. zn. ÚOHS-S0262/2019/VZ), kde zadavatel požadoval při dodání zařízení uvedených ve varování ještě duplicitní „nečínské“ řešení a jejich plnou společnou integraci tak, aby takové řešení plnilo funkci zajištění vysoké dostupnosti. Zadavatel provedl analýzu rizik lege artis, a sporné opatření tak bylo označeno za smysluplné a neexcesivní. Návrh společnosti Huawei Technologies (Czech) s.r.o. byl proto zamítnut.

Dále lze poukázat na rozhodnutí ÚOHS ze dne 19. února 2024 (sp. zn. ÚOHS-S0628/2023/VZ), kdy neregulovaný subjekt na základě správně provedené analýzy rizik vyloučil Huawei Technologies Co., Ltd. a ZTE Corporation, přičemž návrh Huawei Technologies (Czech) s.r.o. proti postupu tohoto zadavatele byl zamítnut, jelikož ÚOHS neshledal důvody pro uložení nápravného opatření.

Naopak lze poukázat i na rozhodnutí ÚOHS ze dne 25. srpna 2022 (sp. zn. ÚOHS-S0196/2022/VZ), kdy zadavatel vyloučil použití zařízení výrobců uvedených ve varování, avšak analýza rizik nebyla provedena lege artis, tj. v souladu s VKB a ZKB. Zadávací řízení tak bylo zrušeno.

Závěr z rozhodovací praxe plyne jasný – zadavatel musí provést analýzu rizik v souladu se ZKB a VKB, tj. lege artis, aby následné nastavení zadávacích podmínek bylo omezením hospodářské soutěže v souladu se ZZVZ.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
3. září 2025	1.0	Autor	Vytvoření dokumentu