NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

SPCSS

Státní pokladna
Centrum sdílených služeb

PRŮVODCE ŘÍZENÍM DODAVATELŮ VE VZTAHU K HODNOCENÍ RIZIK KB

Na tvorbě tohoto dokumentu se podílely týmy odborníků NÚKIB a SPCSS.
Tým NÚKIB byl složen ze členů Odboru kontroly a Odboru regulace.

Tým SPCSS byl složen ze členů:
Mgr. Ing. Ondřej Nekovář (vedoucí týmu)
Arnošt Sarvaš
Ing. Marcel Danilov
Mgr. Jaroslav Mach, DiS.

Obsah

1 Úvod

Základní proces řízení aktiv a rizik kybernetické bezpečnosti (dále jen „KB“) je přiblížen v dokumentu Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti (dále jen „Průvodce AR“, viz kapitola 5, kde jsou zmíněny relevantní podpůrné materiály). Tento samostatně stojící dokument rozšiřuje Průvodce AR o problematiku hodnocení rizik KB ve vztahu k řízení dodavatelů, zejména pak ve vztahu k zadávání veřejných zakázek (dále jen „VZ“). Ty jsou jedním ze způsobů řízení dodavatelů využívaných zejména veřejnými zadavateli. Soukromé společnosti, které nehospodaří s veřejnými financemi, se nemusí zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, řídit. Mohou však využít postupy v něm popsané dobrovolně, aniž by musely provádět všechny kroky podle tohoto zákona.

Řízení rizik spojených s dodavateli je jedna ze základních povinností určená vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VKB“). Pro ukázky procesu řízení dodavatelů je v tomto dokumentu jako modelová organizace identifikováno Ministerstvo pro certifikaci senzorů (dále jen „Ministerstvo“[1]), tedy stejně jako v Průvodci AR. Prostřednictvím hodnocení rizik předmětu veřejných zakázek (dále jen „HR VZ“) získá organizace podstatný nástroj pro předcházení rizik spojených s KB a bezpečností aktiv organizace. Zároveň zjistí, jaká bezpečnostní opatření nebo pravidla by bylo vhodné reflektovat v zadávací dokumentaci nebo ve smlouvě s dodavatelem.

Podpůrný materiál vychází zejména z praktických zkušeností s prováděním HR VZ a většina uvedených informací tak představuje dobrou praxi, která bude využitelná a bude reflektovat požadavky VKB. Dokument samotný pak obsahuje část teoretickou a praktickou a modelový příklad. V teoretické části jsou rozvedeny jednotlivé etapy HR VZ, doplněné o některé pojmy nebo ustanovení z VKB či vydaných opatření a metodických materiálů od Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB”). V praktické části jsou uvedeny příklady možného řešení, jak postupovat při zpracování a posuzování VZ. Modelové situace rovněž obsahují konkrétní vzor hodnocení rizik.

Nedílnou součástí zajištění KB organizace při správě a vyhodnocování VZ je kromě nastavení celého procesu také stanovení odpovědných osob, které v tomto procesu budou plnit svou roli. Za tímto účelem je zpracována modelová RACI matice[2] popisující možné pracovní role a jejich odpovědnosti v průběhu celého hodnotícího procesu (viz kap. 3.1, resp. Příloha 1 – Modelová RACI matice).

Účelem tohoto dokumentu není představit jediný správný postup HR VZ v souladu s VKB. Na průvodce je potřeba nahlížet jako na podpůrný materiál, který lze aplikovat při zvážení všech okolností, které mohou mít vliv na finální výstup u daného hodnocení. Modelové situace představují pouze varianty postupů pro pochopení základního rozlišování a členění. Cílem je tak představit základní principy, které je nutné přizpůsobit prostředí organizace. Tento podpůrný materiál byl vytvořen proto, aby přiblížil problematiku HR VZ především těm, kteří s ní nemají žádné nebo minimální zkušenosti. Jedná se pouze o doporučení nevymahatelné podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZKB“).

[1] Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti, kap. 1.4, str. 9 až 15.
[2] RACI tabulky a jak na ně – CleverAndSmart Management Consulting. *CleverAndSmart Management Consulting* [online]. Copyright © 2008. Dostupné z: https://www.cleverandsmart.cz/raci-tabulky-a-jak-na-ne/

Kvůli názornosti byl pro modelový příklad v rámci Ministerstva zvolen informační systém kritické informační infrastruktury (dále jen „IS KII“), na kterém budou demonstrovány příslušné postupy hodnocení. Stejné povinnosti platí také pro informační systémy základní služby (dále jen „ISZS“) a významné informační systémy (dále jen „VIS“). V případě využití tohoto materiálu nepovinnými osobami nebo pro informační a komunikační systémy (dále jen „IS“), které nespadají pod ZKB, je vhodné zavádět postupy přiměřeně.

K lepšímu přehledu při procházení dokumentu jsou využívány symboly viz tabulka č. 1.

Tabulka 1 - Symboly

Symbol	Popis
	Modelový příklad
	Tip
	Upozornění

1.1 Jak pracovat s podpůrným materiálem

Podpůrný materiál je zaměřen obecně (vymezení předmětu plnění, procesní náležitosti) a modulově (konkrétní VZ prostupující celým průvodcem). Další modelové příklady (zejména ty, které se mírně liší od hlavního příkladu VZ) jsou uvedeny v samostatné kapitole (kapitola 4). Jedná se však pouze o ukázku sloužící pro pochopení principů vysvětlovaných v rámci tohoto podpůrného materiálu. Skutečnosti uvedené v dokumentu nebo v přílohách slouží pouze jako příklady a nejedná se tedy o jejich kompletní výčet, např. hodnocení rizik provedené v jednotlivých organizacích bude obsahovat odlišná primární aktiva nebo přístup k některým zakázkám, než jak je uvedeno v tomto ukázkovém materiálu modelové organizace. Všechny přílohy tohoto podpůrného materiálu pak slouží pouze jako inspirace pro práci a při jejich použití je nutné je upravit pro potřeby konkrétní organizace.

Pro snazší pochopení jsou postupy doplněny konkrétním příkladem VZ v prostředí modelového Ministerstva. Oproti Průvodci AR se zde naopak předpokládá jedno provedené hodnocení rizik, které by mělo být provedeno vždy u konkrétní VZ (například na IS, a to v případě, že VZ do IS svou povahou zasahuje). Při samotném hodnocení rizik je tedy potřeba postupovat podle toho, na jaký konkrétní předmět zakázka cílí, tj. vysokou prioritu bude mít například zajištění ochrany primární služby, kterou identifikovaný IS poskytuje, tzn. např. IS podporující výrobu a distribuci elektřiny, IS podporující provoz letecké dopravy atd. Naopak nižší prioritu bude mít zakázka cílící na méně významný IS organizace, popř. na dodávky nesouvisející s KB, např. zakázka na sekačku travního porostu v areálu organizace. Dále bude také záležet, zda se VZ bude realizovat na dodávky (zejména HW), na služby (podpora, rozvoj) nebo na stavební práce.

Hodnocení rizik je pak obecně požadováno jen v souvislosti s významnými dodavateli dle § 8 odst. 2 písm. a) a c). Ostatní dodavatelé jsou řízeni podle § 8 odst. 1 písm. e) VKB (viz kap. 2).

1.2 Představení modelové organizace

Jak již bylo zmíněno v úvodu, modelovou organizací i v tomto případě bude Ministerstvo. Průvodce hodnocením rizik KB ve vztahu k veřejným zakázkám dle VKB (dále jen „Průvodce VZ“) navazuje na Průvodce AR. Snahou je provázat oba průvodce tam, kde to situace a možnosti dovolí, aby byla zachována maximální kontinuita a využitelnost informací v samotných kapitolách nebo při jednotlivých modelových příkladech. Modelová organizace Ministerstva tedy vychází z Průvodce AR s dodatečnými úpravami v podobě nových oddělení, která jsou relevantní pro proces HR VZ.

Ministerstvo ověřuje, zda předložené senzory splňují všechny požadavky na ně kladené a vyhovujícím zařízením uděluje tříletou certifikaci. Kromě kontroly dokumentace provádí také testování předložených senzorů ve vlastní laboratoři. Ministerstvo je jediným orgánem provádějícím certifikaci senzorů na území státu a příslušné subjekty mají povinnost používat pouze certifikovaná zařízení. Ministerstvo vede neveřejnou detailní evidenci informací o všech senzorech, které byly k certifikaci předloženy. Současně má na svých webových stránkách veřejně dostupný seznam certifikovaných senzorů. Celkem má 2 000 zaměstnanců.

Proces certifikace je zpracován v IS pro evidenci a zpracování procesu certifikace senzorů (dále také jako „agendový systém“). Tento IS byl určen jako prvek KII. Výrobci mohou žádosti o certifikace podávat prostřednictvím webové aplikace Ministerstva, která je součástí tohoto IS a slouží pro externí uživatele, je ale nutná předchozí registrace. Veškerou dokumentaci potřebnou pro proces certifikace výrobci nahrávají do aplikace ve formátu pdf. Ministerstvo má lhůtu 30 dní, aby na podanou žádost reagovalo. S IS pracuje 1 400 interních uživatelů Ministerstva a 300 externích uživatelů.

Webová aplikace slouží výrobcům k podávání žádostí o certifikaci senzorů. Žádost obsahuje formulář, jehož přílohou je technická dokumentace senzoru. Zároveň prostřednictvím této aplikace výrobce daný senzor registruje na laboratorní testy a zajistí jeho fyzické doručení na Ministerstvo. IS slouží jako podpůrný nástroj zaměstnancům Ministerstva, kteří jsou odpovědní za proces certifikace včetně jeho zdokumentování. Průběh jednotlivých kroků procesu je logován. IS také hlídá dodržování zákonných lhůt. Webová aplikace slouží široké veřejnosti k zobrazení informací o tom, které senzory byly Ministerstvem certifikovány. Certifikáty jsou automaticky po třech letech zrušeny a senzory odebrány z veřejného seznamu certifikovaných zařízení. IS je vyvíjen dodavatelskou firmou.

1.2.1 Popis jednotlivých rolí a úseků

Průvodce AR zmiňuje ve svém Úvodu jako nedílnou součást procesu také aktivní podporu a zapojení vedení organizace. V případě prováděného hodnocení rizik se pak může jednat z pozice vedení společnosti např. o osobu v roli garanta primárního aktiva. Po definování kontextu Ministerstva (agend, služeb, aktiv apod.) je potřeba přistoupit k identifikaci jednotlivých úseků a pracovních rolí, které se na celém procesu podílejí. Tím bude zajištěna kontinuita celého procesu a zaručena plynulost předávání informací mezi jednotlivými úseky a jejich zaměstnanci.

Jedním z důležitých kroků je tak např. určení odpovědného zaměstnance pro každého jednotlivého dodavatele, tzv. zaměstnanec odpovědný za smluvní vztah. Tento zaměstnanec musí určit a řídit všechny odborné záležitosti související s předmětnými dodávkami nebo službami. Měl by tedy disponovat odborným povědomím o věcném plnění zakázky, a zároveň také případnou právní podporou. Nedílnou součástí těchto aktivit je i zajištění odpovídající úrovně bezpečnosti informací. V procesu HR VZ je však aktivní účast zaměstnance odpovědného

za smluvní vztah značně omezená a není většinou nutná přímá komunikace. Ke komunikaci může docházet až v případech, kdy je potřeba vyjasnit konkrétní dopady nebo další obdržené informace vycházející např. ze zadávací dokumentace. Obdobně to platí také u dalších osob, mezi které kromě zaměstnance odpovědného za smluvní vztah patří kupříkladu bezpečnostní role dle VKB (§ 6 odst. 3, mimo auditora KB) a další role podílející se na výběrovém řízení nebo na jeho průběhu.

Pro účely tohoto dokumentu je přiblíženo také Oddělení veřejných zakázek Ministerstva (dále jen „OVZ“), které je popsáno níže.

Sekce provozní:

- Odbor právní
    - Oddělení veřejných zakázek
        - Zajištění koordinace, metodického řízení, poradenské činnosti a kontroly v oblasti zadávání veřejných zakázek
        - Zpracování a posouzení návrhů investičních programů a koncepcí dlouhodobého vývoje pro Ministerstvo
        - Zajištění plnění procesních náležitostí dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek
        - Zpracování veškeré potřebné dokumentace a související administrace
        - Spolupráce s dalšími odbory nebo odděleními v rámci předmětné agendy

2 Hodnocení rizik v kontextu platné legislativy

Tato kapitola se zaměřuje na zasazení hodnocení rizik do platné legislativy a přiblížení jednotlivých dílčích podkapitol, které mají oporu v relevantní legislativě. Je zde vysvětleno, na základě jaké legislativy je nutno provádět VZ a také povinnost řídit dodavatele v oblasti KB. V kapitole jsou také nastíněny opatření dle § 11 ZKB a metodika hodnocení aktiv a rizik, která vychází z platné legislativy. Hodnocení rizik je jedna ze základních povinností požadovaná VKB (viz § 4 a 5 VKB). Bez znalosti toho, jaká má organizace aktiva a jaká rizika ji ohrožují, nelze efektivně plnit většinu dalších povinností daných VKB. Organizace zjistí, co je pro ni důležité a co musí chránit i v souvislosti s hodnocením rizik při řízení dodavatelů dle § 8 VKB. V návaznosti na to dokáže identifikovat významné dodavatele a stanovit jim příslušné povinnosti ve smluvním ujednání. Řízením rizik organizace zjistí, jakým způsobem je potřeba aktiva chránit a jaká bezpečnostní opatření je nutné zavést.

Mezi základní pojmy, se kterými VKB pracuje, řadíme hodnocení a řízení rizik. Tyto pojmy jsou vymezeny ve VKB. V § 2 písm. d) se uvádí, že **hodnocením rizik** se rozumí *„celkový proces identifikace, analýzy*[3] *a vyhodnocení rizik*". V písm. i) se pak uvádí, že **řízením rizik** se rozumí *„činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik*". Pro doplnění může být vhodné také zmínit písm. h), které rozvádí samotný pojem **riziko**, a tedy, že rizikem je *„možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu"*. Při HR VZ je však potřeba nahlížet na aktiva a rizika trochu odlišněji, než jak k nim přistupuje Průvodce AR (základní seznámení s pojmem riziko na str. 75). Neméně důležitým pojmem souvisejícím s procesem hodnocení rizik u VZ je **významný dodavatel**, kterým se dle § 2 písm. n) VKB rozumí *„provozovatel informačního nebo komunikačního systému (dále jen „provozovatel") a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému*". Právě určení významného dodavatele často rozhoduje o tom, jak celý proces hodnocení rizik bude dále probíhat (viz kap. 2.2 a 2.3).

2.1 Legislativní rámec

Povinnost hodnocení rizik v souvislosti se zadáváním VZ je třeba normativně vymezit. Jedním ze vstupních právních předpisů, kterým je nutno se v tomto případě řídit je zákon č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ"). ZZVZ určuje základní pravidla pro zadávání VZ a další náležitosti související s touto problematikou. Dalším právním předpisem, který tuto oblast reguluje je ZKB. ZZVZ i ZKB jsou předpisy stejné právní síly a nenacházejí se ve stavu podřízenosti či nadřízenosti. Zadavatel VZ je vždy povinen se při zadávání VZ řídit oběma zmíněnými zákony. Kromě ZZVZ a ZKB problematiku hodnocení rizik dále upravuje také VKB. Na organizace s účastí zahraničních investorů se vztahuje také zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic)[4].

Stěžejní povinností zadavatele je podle ZZVZ řádné odůvodnění všech požadavků, které hospodářskou soutěž omezují (§ 36 odst. 1 ZZVZ). Ze ZKB vyplývá zadavateli povinnost provádět

[3] V praxi se však pojem analýza rizik používá pro celý proces a jedná se tak de facto o synonymum pojmu hodnocení rizik, a ne jeho podmnožinu.

[4] V kontextu zadávání VZ konkrétně § 7 písm. c), podle kterého: „Bez povolení podle § 14 odst. 1 nebo podmíněného povolení podle § 15 odst. 3 nesmí být uskutečněna zahraniční investice do cílové osoby, která je správcem informačního systému kritické informační infrastruktury, správcem komunikačního systému kritické informační infrastruktury, správcem informačního systému základní služby nebo provozovatelem základní služby (viz § 3 ZKB)".

bezpečnostní opatření za účelem zajištění KB IS a povinnost zanášet požadavky vyplývající z přijatých bezpečnostních opatření do smluv s dodavateli (§ 4 ZKB). **Bezpečnostními opatřeními** se podle § 5 ZKB rozumí organizační a technická opatření, která je nutné v souvislosti s konkrétní VZ přijímat, vyžaduje-li to povaha samotné zakázky. Zohlednění požadavků vyplývajících z bezpečnostních opatření v míře nezbytné pro splnění povinností podle ZKB při výběru dodavatele nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěže (§ 4 odst. 4 věta druhá a § 4 odst. 7 ZKB). Zadavatel VZ je povinen zanést do zadávacích podmínek požadavky, kterými bude splňovat povinnosti vyplývající ze ZKB. Tyto zadávací podmínky musí reflektovat výsledky, kterých zadavatel dosáhl po hodnocení rizik, a obsahovat výčet konkrétních bezpečnostních opatření, které chce zadavatel VZ implementovat za účelem snížení rizika na akceptovatelnou hodnotu či jeho úplnou eliminaci. Při procesu hodnocení rizik je rovněž nutno zohlednit všechna opatření podle § 11 ZKB vydaná NÚKIB, zejména varování, která vydal v období před zahájením zadávacího řízení (§ 5 odst. 1 písm. h) bod 3. VKB). Problematika opatření je blíže představena v podkapitole 2.4.

V rámci vydávaných opatření je potřeba též zmínit propojení ZZVZ a ZKB, konkrétně pak § 36 odst. 1 ZZVZ uvádí, že „*zadávací podmínky nesmí být stanoveny tak, aby určitým dodavatelům bezdůvodně přímo nebo nepřímo zaručovaly konkurenční výhodu nebo vytvářely bezdůvodné překážky hospodářské soutěže*“. Zadavatelé tak smí v souladu se ZZVZ hospodářskou soutěž omezit pouze v odůvodněných případech. Příslušnou zadávací podmínku je třeba vnímat jako legitimní a odůvodněnou, jestliže vychází z povinností, které byly zadavateli uloženy jiným zákonem a tato podmínka zrcadlí potřebu zadavatele a splnění zákonné povinnosti. V tomto případě se jedná o právní akt vydaný na základě § 22 písm. b) ZKB, kterým NÚKIB v rámci svých kompetencí vydává opatření (např. zmíněná varování) a povinné osoby je musí zohlednit.

Bezpečnostní opatření, která ZKB stanovuje a VKB upravuje, lze aplikovat jak na předmět VZ, tak na osobu dodavatele. Do zadávacích podmínek mohou být zadavatelem zaneseny jakékoliv požadavky, které jsou náležitě odůvodněny a které současně splňují základní zásady § 6 ZZVZ. Veškerá bezpečnostní opatření z VKB jsou podřaditelná pod některý z institutů upravených ZZVZ. Může jít například o kritéria pro hodnocení nabídek, požadavky na předmět plnění nebo požadavky na kvalifikaci[5] dodavatele. Za předpokladu vhodného a dostatečného vymezení zadávacích podmínek je tedy zadavatel schopen vyloučit účastníky zadávacího řízení, kteří stanovené zadávací podmínky nesplňují.

Přesný způsob zahrnutí bezpečnostních požadavků do zadávacích podmínek je zcela v gesci zadavatele VZ. Jednotlivá bezpečnostní opatření, která jsou požadována v zadávacím řízení, by měla mít kvalitu a úroveň odpovídající výsledku hodnocení a řízení rizik.

Problematika řízení dodavatelů a zadávání VZ v oblasti KB je více přiblížena v podpůrných materiálech zveřejněných na webových stránkách NÚKIB:

- Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost,
- Požadavky na smlouvy s dodavateli,
- Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení a
- Metodika řízení dodavatelů.

[5] Požadavky na kvalifikaci dodavatele jsou omezeny. Zadavatel musí na osobu dodavatele nebo subdodavatele vznést pouze takové kvalifikační požadavky, které mu ZZVZ umožňuje. V případě, že existují jiné kvalifikační požadavky, musí dojít k jejich přetransformování na požadavky na předmět plnění. Tím se zamezí vázání požadavků na osobu dodavatele nebo subdodavatele.

Podpůrný materiál „Zadávání veřejných zakázek v oblasti ICT a kybernetické bezpečnosti“ popisuje a více rozvádí problematické oblasti, ke kterým zároveň doplňuje i možné varianty řešení v souladu s pravidly hospodářské soutěže. Podpůrný materiál „Požadavky na smlouvy s dodavateli“ vysvětluje jednotlivé požadavky přílohy č. 7 VKB a vysvětluje jednotlivá smluvní ustanovení, která musí být zahrnutá do smlouvy mezi povinnou osobou a významným dodavatelem. V metodice „Zohlednění varování ze dne 17. prosince 2018“ je vysvětlen institut varování a popsán princip řízení rizik. Vedle toho metodika předkládá možnosti pro zajištění plnění povinností podle ZKB, které jsou v souladu s předpisy regulujícími zadávání VZ. „Metodika řízení dodavatelů” se zabývá procesem řízení dodavatelů v průběhu celého životního cyklu dodávky s důrazem na obsah politiky řízení dodavatelů podle přílohy č. 5 k VKB.

2.2 Požadavky § 8 VKB

Kromě ZZVZ a ZKB problematiku hodnocení rizik legislativně upravuje také VKB, konkrétně se jedná o § 8 VKB, který se dále zabývá určením základních bezpečnostních pravidel pro řízení dodavatelů a pro uzavírání dodavatelských smluv. Jeho hlavním cílem je stanovit pravidla pro dodavatele, která vychází z požadavků systému řízení bezpečnosti informací, seznámit dodavatele s těmito pravidly a následně vyžadovat jejich plnění.

VKB ve spojitosti s problematikou řízení dodavatelů pracuje s pojmy **dodavatel**, **významný dodavatel** a **provozovatel**. Dodavatelé se řídí podle § 8 VKB a pro skupinu významných dodavatelů (součástí které jsou i provozovatelé) vyplývají navíc další povinnosti, které je třeba splňovat.

S každým dodavatelským vztahem se pojí řada povinností. Mezi ty obecné, které platí pro všechny dodavatele se řadí:

- stanovení pravidel, která zohledňují požadavky systému řízení bezpečnosti informací (§ 8 odst. 1 písm. a) VKB),
- seznámení dodavatelů se stanovenými pravidly a jejich vyžadování (§ 8 odst. 1 písm. d) VKB) a
- řízení rizik spojených s daným dodavatelem (§ 8 odst. 1 písm. e) VKB).

Zadavatelé VZ musí provádět hodnocení rizik v pravidelných intervalech a dále:

- při významných změnách ve vztahu k aktivům existujících informačních nebo komunikačních systémů (§ 5 VKB a § 8 odst. 2 písm. c) VKB),
- u významných dodavatelů ve vztahu k plnění předmětu výběrového řízení, a to v rámci tohoto výběrového řízení (§ 8 odst. 2 písm. a) VKB),
- v souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému (§ 13 písm. a) VKB).

2.3 Významní dodavatelé a povinnosti s nimi spojené

Jak již bylo zmíněno, mimo obecných povinností, které jsou společné pro všechny typy dodavatelů, se ke skupině významných dodavatelů vztahuje soubor dalších povinností. Ve chvíli, kdy konkrétního dodavatele povinná osoba (v tomto případě samotný zadavatel VZ) určí jako významného, je nutno jej zaevidovat do evidence významných dodavatelů (§ 8 odst. 1 písm. b) VKB). Jakmile bude uvedený dodavatel do této evidence zařazen, je potřeba ho písemnou formou prokazatelně o jeho zařazení informovat (§ 8 odst. 1 písm. c) VKB). Náležitosti prokazatelného informování jsou uvedeny v (§ 8 odst. 3 VKB). V případě, že je významný dodavatel zároveň i provozovatelem, je nutno tuto skutečnost v prokazatelném informování zohlednit (§ 8 odst. 3

písm. d) VKB). Pokud se jedná o významného dodavatele, který je zároveň provozovatelem, a byl o této skutečnosti prokazatelně písemně informován, tak se k jeho povinnostem řadí také hlášení kontaktních údajů formou uvedenou v § 34 VKB. Dále je ze strany zadavatele VZ nutné zajistit, že smlouvy uzavírané s významnými dodavateli obsahují veškeré (pro vztah s daným dodavatelem relevantní) oblasti, které jsou uvedeny v následujícím výčtu dle Přílohy č. 7 VKB (§ 8 odst. 1 písm. f) VKB).

Příloha č. 7 VKB – Obsah smlouvy uzavírané s významnými dodavateli:

- ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),
- ustanovení o oprávnění užívat data,
- ustanovení o autorství programového kódu, popřípadě o programových licencích,
- ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),
- ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,
- ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,
- ustanovení o řízení změn,
- ustanovení o souladu smluv s obecně závaznými právními předpisy,
- ustanovení o povinnosti dodavatele informovat povinnou osobu o
    - kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
    - způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,
    - významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem,
- specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),
- specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),
- specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,
- pravidla pro likvidaci dat,
- ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy,
- ustanovení o sankcích za porušení povinností.

V souladu s § 8 odst. 2 písm. a) VKB musí zadavatel VZ u významného dodavatele v rámci výběrového řízení a před uzavřením smlouvy provést hodnocení rizik souvisejících s plněním předmětu výběrového řízení. Toto hodnocení rizik vychází z § 5 VKB a má být provedeno přiměřeně podle přílohy č. 2 VKB. Pokud dojde při hodnocení rizik k identifikaci neakceptovatelných rizik, musí zadavatel zajistit zavedení přiměřených bezpečnostních opatření (viz kap. 2.1). V případě uzavření smluvního vztahu mezi dodavatelem a zadavatelem VZ, musí

být ve smlouvě jasně definováno a rozděleno stanovení způsobu a úrovně realizace příslušných bezpečnostních opatření a následně určení odpovědností za zavedení a kontrolu těchto bezpečnostních opatření (§ 8 odst. 2 písm. b) VKB). Zadavatel je dále povinen provádět pravidelný přezkum hodnocení rizik a také pravidelně kontrolovat zavedená bezpečnostní opatření u poskytovaných plnění. V některých případech může dojít k přenesení povinnosti kontroly dodavatelů na třetí stranu (např. na nezávislého auditora). Pokud dojde při přezkumu hodnocení rizik nebo při kontrole bezpečnostních opatření k identifikaci nedostatků, musí zadavatel zajistit jejich řešení dle § 8 odst. 2 písm. d) VKB. Po uzavření smluv a v průběhu smluvního vztahu je nutné zajistit pravidelné přezkoumávání plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací (§ 8 odst. 1 písm. g) VKB).

2.4 Opatření NÚKIB

V souladu s § 11 ZKB vydává NÚKIB opatření, kterými jsou **varování**, **reaktivní opatření** a **ochranné opatření**. Je důležité zmínit, že povinné osoby musí zohlednit všechna relevantní opatření, tedy i ta, která **budou vydána v budoucnu**, a tento podpůrný materiál je neobsahuje. Nově určené povinné osoby musí pracovat s relevantními varováními, která jsou **stále platná** a byla vydána ještě před jejich určením.

Varování slouží k ochraně informačních systémů před hrozbami v oblasti KB a jsou vydávána podle § 12 odst. 1 ZKB v případě, kdy se o hrozbě NÚKIB dozví z vlastní činnosti nebo z podnětu provozovatele národního CERT, či jiných orgánů vykonávajících působnost v oblasti KB. Všechna varování jsou zveřejněna na úřední desce NÚKIB[6], který následně informuje povinné osoby. Ty jsou povinny na hrozbu vyplývající z varování reagovat a zohlednit ji v hodnocení rizik podle § 5 odst. 1 písm. h) bod 3 VKB.

Doposud vydaná **varování** poukazují na hrozby a zároveň je hodnotí. Povinná osoba může použít pro hodnocení hrozeb odlišnou stupnici než dle přílohy č. 2 tabulky č. 1 VKB (jak umožňuje § 5 odst. 3 VKB), nicméně je nutno tuto hrozbu ohodnotit způsobem odpovídajícím příslušné úrovni podle VKB. Například pokud je hrozba dle varování hodnocena nejvyšším stupněm (tzn. jako kritická), povinná osoba musí použít v rámci svých stupnic rovněž nejvyšší stupeň (v našem případě hodnotu 4). Uvedené je blíže rozvedeno v kapitole 3.5.

Povinné osoby dle § 3 písm. c) až f) ZKB (v některých případech i povinné osoby podle § 3 písm. a) a b)) musí dále zohlednit reaktivní a ochranná opatření vydaná NÚKIB podle § 13 § 14 ZKB. Reaktivní opatření reaguje na vzniklý kybernetický bezpečnostní incident, nebo slouží k zabezpečení IS před kybernetickým bezpečnostním incidentem, a je nutno jej provést ve stanovené lhůtě. Ochranné opatření je opatřením obecné povahy, které je vydáno za účelem ochrany IS na základě již vyřešeného kybernetického bezpečnostního incidentu. V současné době jsou vydána tři reaktivní opatření na Exchange, SolarWinds a Apache Log4j a také jedno ochranné opatření týkající se zabezpečení e-mailů. Dosud vydaná reaktivní a ochranná opatření však nejsou pro tento podpůrný materiál relevantní.

Organizace, které nespadají pod regulaci ZKB mohou opatření brát pouze jako doporučení a nejsou povinny jej zohledňovat.

Níže je uveden přehled varování vydaných NÚKIB, které musí povinné osoby zvážit na základě relevantnosti. To platí o všech ostatních opatřeních, které povinné osoby zvažují. **Vždy je potřeba zvážit relevantnost daného opatření, i vydaných v budoucnu, a to pak dále aplikovat při**

[6] Národní úřad pro kybernetickou a informační bezpečnost – Úřední deska (nukib.cz)

hodnocení rizik. Nerelevantní opatření nemusí povinné osoby při hodnocení rizik zohledňovat. Povinná osoba si musí vždy ověřit, která varování jsou aktuálně platná. Jednotlivá varování využitá v tomto materiálu jsou uvedena u jednotlivých modelových příkladů.

Varování před použitím technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation

NÚKIB 17. prosince 2018 vydal varování před použitím technických a programových prostředků společností Huawei Technologies Co., Ltd. a ZTE Corporation a současně jejich dceřiných společností. Poznatky bezpečnostní komunity, které jsou NÚKIB dostupné, o aktivitách uvedených společností v České republice i ve světě vytváří důvodné obavy z existence potenciálních rizik při využívání technických a programových prostředků, které tyto společnosti poskytují svým zákazníkům. Povinné osoby uvedené v § 3 písm. c) až f) ZKB jsou povinny podle § 4 odst. 4 ZKB při výběru dodavatele zohlednit požadavky, které vyplývají z bezpečnostních opatření a zahrnout tyto požadavky do smlouvy s dodavatelem.

NÚKIB hrozbu hodnotí na úrovni **Kritická – Hrozba je velmi pravděpodobná až více méně jistá.**

V rámci vydaného podpůrného materiálu je přehledová tabulka, která uvádí příklady hrozeb. Jedná se o seznam hrozeb, který musí být následně organizací přizpůsobený pro její prostředí a potřeby. Uvedený seznam hrozeb doplňuje hrozby uvedené ve VKB.

Tabulka 2 - Přehledová tabulka hrozeb

Výskyt hrozby	Projev hrozby
na úrovni telekomunikačních komponent	zaznamenávání hovorů
	kontrola nad obsahem přenášených dat
	lokalizace uživatelů
	deaktivace telekomunikačních služeb (nefunkční hlasové a datové služby)
na úrovni serverových řešení a infrastruktury	přístup k veškerým datům
	kontrola nad obsahem přenášených dat
	možnost odepření služby
na koncových zařízeních	přístup k uloženým datům (šifrování na zařízení není ochranou)
	pořizování záznamu (audio, video)
	získání geolokačních dat
	podvrhnutí identity

Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací

Varování ze dne 21. března 2022 souvisí s hrozbou nedodržení smluvních závazků ze strany dodavatelů ICT služeb a produktů s významným vztahem k Ruské federaci. Hrozba je založena na možných dopadech ekonomických sankcí týkajících se Ruské federace, které mohou vést k nedodržení smluvních závazků ze strany ICT dodavatelů a ovlivnit funkčnost jimi spravovaných

systémů. Jedná se o hrozbu, která je definována v příloze č. 3 VKB, přesněji typová hrozba č. 10 „*nedodržení smluvního závazku ze strany dodavatele*“. Zadavatelé regulovaní dle ZKB by měli dále s danou hrozbou pracovat v hodnocení rizik a v dalších procesech souvisejících se zakázkou. Je doporučeno danou hrozbu zohlednit v plánech kontinuity činností. K tomuto varování je na internetových stránkách NÚKIB uveřejněno doplnění[7] obsahující otázky a odpovědi relevantní pro povinné osoby.

NÚKIB hrozbu hodnotí na úrovni **Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná.**

Varování před hrozbou kybernetických útoků na IS veřejné správy

Dne 25. února 2022 bylo vydáno varování, které upozorňuje na kybernetické útoky zaměřené na IS veřejné správy a další strategické organizace. Součástí varování je sada doporučení.

NÚKIB tuto hrozbu hodnotí na úrovni **Kritická – Hrozba je velmi pravděpodobná až téměř jistá.**

Varování před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím

Vydané varování ze dne 30. května 2022 je zaměřeno na možnou hrozbu při použití chytrých elektroměrů pocházející ze zemí s nedůvěryhodným právním prostředím. Jedná se o technické nebo programové prostředky, které nepochází ze států Evropské unie, Evropského hospodářského prostoru, Organizace pro hospodářskou spolupráci a rozvoj či Severoatlantickou alianci, pro implementaci technologií umožňujících požadovanou úroveň přímého měření typu B, C1, C2 nebo C3 dle vyhlášky o měření elektřiny.

NÚKIB tuto hrozbu hodnotí na úrovni **Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná.**

Varování před hrozbou spočívající v instalaci a používání aplikace TikTok

Vydané varování ze dne 8. března 2023 upozorňuje na hrozbu spočívající v instalaci a použití aplikace TikTok na zařízení, která jsou používaná k přístupům k IS KII, ISZS a VIS. Na základě zjištění a poznatků NÚKIB sbírá TikTok velké množství uživatelských dat, která jsou následně ukládána. Aplikace TikTok je provozována společností ByteDance, která spadá do působnosti čínské národní legislativy. Na základě čínské legislativy a podle pravidel pro nahlašování zranitelností v síťových zařízeních se může na aplikaci TikTok vztahovat povinnost předání uložených dat. Z tohoto důvodu vznikají obavy, že zájmy Čínské lidové republiky mohou být stavěny nad zájmy uživatelů technologií společností, které jsou podřízeny právnímu prostředí Čínské lidové republiky. Hrozbou je tedy možnost cílených kybernetických útoků na konkrétní osoby, možnost využití dat k vydírání cílených osob a narušení bezpečnosti České republiky.

NÚKIB tuto hrozbu hodnotí na úrovni **Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná.**

2.5 Metodika hodnocení rizik

Podle § 4 odst. 1 písm. a) a § 5 odst. 1 písm. a) VKB je před zahájením procesu hodnocení rizik nutné mít zpracovanou metodiku pro hodnocení aktiv a rizik, na jejímž základě bude celý proces proveden. V metodice musí být uvedeny základní informace, jako je zvolená metoda, která bude použita, stupnice pro hodnocení aktiv i rizik, výpočet pro získání hodnot rizik apod. Metodika musí být dostatečně návodná, srozumitelná a jednoznačná, aby bylo zaručeno, že bude celý

[7] Národní úřad pro kybernetickou a informační bezpečnost – Doplnění informací k varování NÚKIB v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací (nukib.cz)

proces hodnocení rizik opakovatelný, přezkoumatelný a povede za stejných podmínek ke stejným výsledkům. Hodnocení rizik nelze provést bez toho, aniž by bylo provedeno hodnocení aktiv podle § 4 VKB. Povinná osoba identifikuje jednotlivá aktiva a určí, zdali se jedná o primární nebo podpůrná aktiva. Mezi primární aktiva se dle § 2 písm. g) VKB řadí informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém. Mezi podpůrná aktiva se podle § 2 písm. f) VKB řadí technické aktivum, zaměstnanci a dodavatelé, kteří se podílejí na provozu, rozvoji, správě nebo bezpečnosti IS. Řízením aktiv v oblasti KB se podrobněji zabývá podpůrný materiál Průvodce AR.

Samotná metodika hodnocení rizik by měla nejen definovat proces hodnocení rizik, ale také stanovit kritéria pro akceptovatelnost rizik a definovat role, které budou za jednotlivé činnosti odpovědné, případně které budou na hodnocení rizik spolupracovat. Řízení rizik je činnost, která zahrnuje hodnocení rizik, výběr a zavedení bezpečnostního opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik. S ohledem na vymezená aktiva se identifikují relevantní hrozby a zranitelnosti. Povinná osoba by měla především zvažovat relevantní kategorie hrozeb a zranitelností, které jsou uvedeny v příloze č. 3 VKB a mohou mít dopad na identifikovaná aktiva povinné osoby.

Hodnocení rizik by mělo probíhat v rámci výběrového řízení a před uzavřením smlouvy podle § 8 odst. 2 písm. a) VKB s významným dodavatelem, přiměřeně podle přílohy č. 2 VKB s ohledem na řízení aktiv a rizik v organizaci dle § 4 a 5 VKB. Hodnota rizika je v praxi nejčastěji definována jako funkce, která je ovlivňována dopadem, hrozbou a zranitelností. Tato funkce je nezbytnou součástí metodiky. VKB konkrétně uvádí funkci:

Riziko = dopad x hrozba x zranitelnost

Dopad představuje hodnotu škody, která by vznikla v případě narušení bezpečnosti informací (důvěrnosti, integrity, dostupnosti). Pro hodnocení dopadu je využito hodnocení aktiv podle § 4 VKB.

Hrozba je podle § 2 písm. e) VKB *„potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu*". Hodnocení hrozby vychází z možnosti její existence a pravděpodobnosti její realizace. Její hodnota může být předem určena, a to v případě, kdy se jedná o hrozbu uvedenou ve varování, která vydává NÚKIB a kterými se blíže zabývá kapitola 2.4. Povinná osoba musí následně klasifikovat danou hrozbu hodnotou odpovídající úrovni uvedené ve varování.

Zranitelnost je definována v § 2 písm. p) VKB jako *„slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami*". Hodnota zranitelnosti je odvozována dle pravděpodobnosti jejího výskytu, či jejího zneužití a dle úrovně zavedení vhodných bezpečnostních opatření.

Pro hodnocení rizik může každá povinná osoba použít svoji funkci a vlastní metodiku, ale musí zajistit, že hodnocení rizik bude na stejné nebo vyšší úrovni, než je uvedeno ve VKB. Stanovené výsledné hodnoty rizika musí být porovnány s kritérii pro akceptovatelnost a musí být rozhodnuto, jak bude riziko ošetřeno. Podrobný popis a ukázka zpracování hodnocení rizik je ve vydaném podpůrném materiálu Průvodce AR.

Rizika, která organizace identifikovala v hodnocení rizik, by měla být následně ošetřena jedním ze způsobů uvedených v kapitole 3.3.

3 Postup HR VZ

Povinná osoba musí v souladu s § 8 odst. 1 písm. e) VKB řídit rizika spojená s dodavateli, a dále u těch, které určí jako významné, provádět hodnocení rizik. Hodnocení rizik je v této kapitole popsáno v širším kontextu. Není zde popsána pouze povinnost zpracovat hodnocení rizik dle VKB, nýbrž celý proces VZ – od obdržení dokumentace k VZ, přes nutnost do organizace zavést metodiku hodnocení, až po zapracování bezpečnostních opatření vzešlých z hodnocení rizik. To přibližuje níže uvedený příklad.

V rámci rozšíření kapacit úložišť rozhodlo Ministerstvo nakoupit nová aktiva, a to konkrétně páskové knihovny. V obecném vymezení Ministerstvo tato úložiště používá pro ukládání dat v rámci chodu systému pro evidenci a zpracování procesu certifikace senzorů. V současné době poptává Ministerstvo prostřednictvím veřejné zakázky pět kusů diskových polí. Vzhledem k povaze dodávky bude potenciální dodavatel určen jako významný.

Jakožto veřejný zadavatel podle § 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, bude postupovat prostřednictvím veřejné zakázky. Vzhledem k předmětu VZ, který byl zvolen pro modelový příklad a průzkumu v rámci trhu, Ministerstvo předpokládá přihlášení dodavatele, který dodává technické prostředky, které jsou předmětem varování NÚKIB (kapitola 2.4). Pro tyto účely a pro plnění povinností VKB vypracovalo Ministerstvo hodnocení rizik, které je obsahem této kapitoly a jehož postup je popsán v dalších krocích.

Kategorizace tohoto procesu je definována v podkapitolách 3.1 až 3.7. Jednotlivé kroky celého procesu a možné způsoby, jak k nim přistupovat, jsou konkrétně popsány na modelové organizaci – Ministerstvu.

3.1 Pracovní role (RACI matice)

Pro samotný proces HR VZ je klíčové hned v úvodu definovat pracovní role, které se na něm budou podílet, budou ho utvářet a dále rozvíjet. Tyto pracovní role jsou vykonávány konkrétními odbornými pracovníky a vyžadují své specifické odpovědnosti, znalosti a zkušenosti. V některých případech pak můžeme hovořit také o bezpečnostních rolích, které jsou více rozvedeny v § 7 VKB, popř. v příloze č. 6 VKB.

Za jednu z bezpečnostních rolí (a v rámci procesu HR VZ i rolí stěžejní) je považován **Manažer kybernetické bezpečnosti** (dále jen „MKB“). Pro potřeby tohoto dokumentu je současně v rámci Ministerstva definován i MKB na pozici junior (dále jen „MKBJR“) z důvodu rozdělení množství práce mezi více osob. Zahrnutí této role rovněž demonstruje fakt, že proces HR VZ lze rozdělit mezi větší množství osob. Mezi další bezpečnostní role, které mohou být v procesu HR VZ zahrnuty, patří např. **Architekt kybernetické bezpečnosti** (dále jen „ARCHKB“) nebo **Garant aktiva** (dále jen „GA“). GA v tomto procesu by měl pomoci s hodnocením daného aktiva, resp. působí jako ručitel za dané aktivum, kterého se soutěžená VZ týká. Ostatní bezpečnostní role mohou s MKB spolupracovat a poskytovat mu na vyžádání podporu. GA je následně informován o konečném výstupu v celé věci (tj. včetně výsledku diskuse a rozhodnutí MKB prostřednictvím jeho vydaného stanoviska k VZ).

Tyto a další činnosti pak ve svém souhrnu sumarizuje RACI matice. Ta ve své podstatě stanovuje odpovědnosti jednotlivých osob, které plní v kontextu daného procesu svou pracovní roli. K ní mají přiřazenu určitou činnost podle fáze, ve které se proces nachází. Ideální formou je pak tabulka, ve které jsou uvedeny v jednotlivých řádcích činnosti, které je potřeba provést, a sloupce popisující role, které se celého procesu účastní. Jakou konkrétní odpovědnost pak každá role má,

je v tabulce označeno písmeny „R“, „A”, „C“ nebo „I“. Důležité je také zmínit, že jedna osoba může (ale nemusí) vykonávat více těchto rolí. Modelová matice je uvedena v příloze č. 1.

Níže jsou uvedeny charakteristiky jednotlivých písmen tvořících zkratku RACI.

Tabulka 3 - Role v RACI matici

R	Responsible	Osoby, které jsou zodpovědné za zpracování nebo vykonání určitých dílčích činností nebo za zpracování výstupů v dané věci.
A	Accountable	Osoby, které kontrolují postup v celém procesu a zodpovídají za jeho celkový výsledek.
C	Consulted	Osoby, které přispívají znalostmi ze svého oboru, plní roli konzultanta a podávají vyjádření k určitému postupu nebo činnosti v průběhu celého procesu.
I	Informed	Osoby, které mají být informovány o některých skutečnostech, které se objevily nebo byly zjištěny, a je žádoucí, aby o nich věděly.

Pro přehlednost celé tabulky, jasné vymezení odpovědností a snadnější řízení procesu i komunikace je vhodné ke každé pracovní roli přiřadit jednu konkrétní odpovědnost (písmeno) za danou činnost. Pokud budeme uvádět více takových odpovědností, pak se doporučuje nepřesahovat počet dvou písmen, a zároveň písmeno „A“ zachovat pouze pro jednu takovou pracovní roli. Není ani chybou, pokud u některých činností nebude u jedné či více osob pole vyplněno, pokud jejich účast v této části procesu není nutná.

RACI matice na Ministerstvu tak naplňuje procesně orientovaný přístup, jehož nezbytným kritériem k zajištění plnění všech podstatných úkonů je právě jednoznačné stanovení odpovědností a informačního toku.

3.2 Nastavení interních postupů

Nutnou podmínkou pro úspěšnou a efektivní implementaci požadavků § 8 VKB vztahujících se k řízení rizik je nastavení interních postupů a odpovědností v rámci organizace. Interními postupy jsou zde chápány různé administrativní činnosti vedoucí k efektivnímu průběhu celého procesu.

Interní postupy v různých organizacích mohou být odlišné v závislosti na nastavených procesech. Níže uvedený postup je tedy pouze doporučující a jeho implementace tak závisí na kontextu konkrétní organizace.

Klíčovým interním postupem je nutnost ustanovení komunikace a definice vzájemných potřeb mezi rolí MKB a útvarem zaštiťujícím problematiku VZ v rámci organizace. V případě Ministerstva se jedná o OVZ. Je nutné ustanovit, že problematika řízení dodavatelů a výstupy od MKB budou nedílnou součástí procesu zveřejňování VZ a dalšího smluvního řízení s dodavateli. K úspěšnému řízení rizik dle § 8 VKB musí mít MKB k dispozici veškerou dokumentaci k VZ a je žádoucí si tak vydefinovat, jakým způsobem a v jakém rozsahu bude zajištěno předávání dokumentace MKB a další charakteristiky tohoto podprocesu.

Zjednodušeně řečeno tedy bude nutné se nejprve domluvit na následujících krocích:

1. kanály použité pro předání/zaslání dokumentace k posouzení MKB,
2. lhůty pro posouzení:
    a. dokumentace VZ (rozhodnutí o významnosti dodavatele),
    b. následné zpracování HR VZ (v případě rozhodnutí o významném dodavateli),
3. forma stanoviska MKB (samostatný dokument nebo zapracování do zaslané dokumentace),

4. nutnost zapracování výstupů hodnocení rizik do zadávací dokumentace.

V rámci dokumentace je stěžejní si s OVZ ustanovit, že posuzování VZ, příp. HR VZ se provádí před vypsáním VZ, ale již nad finální zadávací dokumentací. V případě pozdější změny dokumentace (a tím pádem VZ) je nutné vyvolat celý proces posouzení VZ, resp. HR VZ znovu.

Zadávací dokumentací se v kontextu posouzení VZ a zpracování HR VZ nemá na mysli poskytnutí celé komplexní dokumentace k VZ, ale pouze relevantních dokumentů, které postačují pro potřeby provedení samotného hodnocení.

V obdržené dokumentaci se pak může objevit kombinace níže uvedených dokumentů:

- Žádost o zadání veřejné zakázky,
- Zadávací dokumentace, včetně příloh (technické specifikace atd.),
- Průzkum trhu,
- Objednávka,
- Poptávka,
- Smlouva,
- Servisní smlouva.

Na základě této dokumentace MKB provede posouzení významnosti dodavatele, resp. zda bude předmět plnění VZ významný z pohledu KB a tím pádem bude jeho dodavatel významným dodavatelem. V tomto momentě zpracuje HR VZ, jehož výstupem jsou podmínky, ve kterých se promítají stanovená bezpečnostní opatření, jejichž účelem je mitigace (zmírnění) identifikovaných rizik. Navrhnutá bezpečnostní opatření v rámci hodnocení rizik je potřeba zapracovat do Zadávací dokumentace a také do smlouvy. Toto je opět nutné nastavit interně se subjektem, který v rámci organizace řídí VZ (pro potřeby tohoto dokumentu OVZ).

Důležité je, v rámci definice a popisu interních postupů, i založení úložiště/diskusního fóra, kam mají zřízen přístup osoby mající vliv na posouzení zakázky. MKB při formování stanoviska může svůj názor konzultovat s dalšími bezpečnostními rolemi či odborníky na bezpečnost nebo jinými relevantními osobami. Dokumentace musí být náležitě sdílena a jednotlivým stranám by měl být poskytnut prostor vyjádřit svůj názor. Ve stejné struktuře je poté potenciálně zpracováno i hodnocení rizik. Výsledný dokument tak může být opět konzultován s jednotlivými zúčastněnými stranami v rámci bezpečnosti ještě před tím, než bude oficiálně zaslán na OVZ.

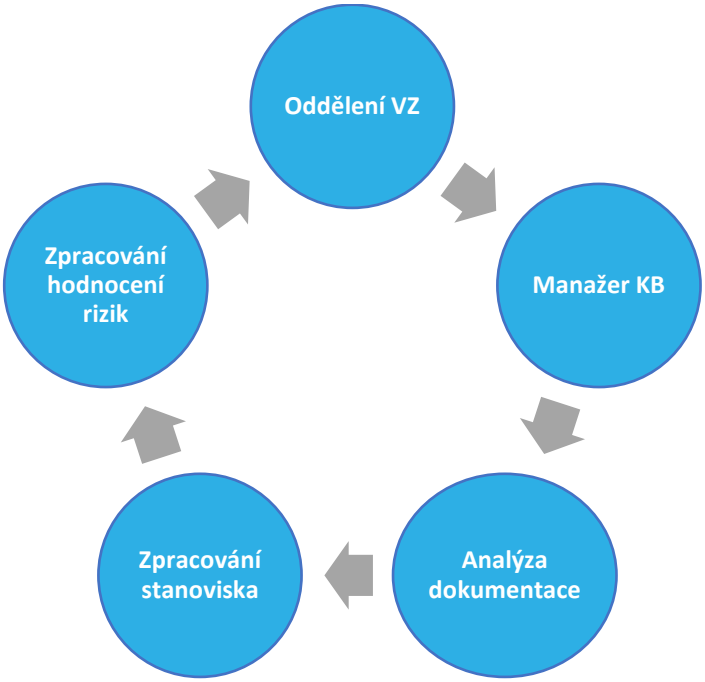
Nedílnou součástí interních postupů je i nutnost evidence již posouzených VZ, příp. zpracovaných hodnocení rizik. V závislosti na velikosti organizace může MKB za jeden kalendářní rok posoudit nízké jednotky VZ ale i podstatně více. Pro potřeby např. auditů KB je nutné zvolit vhodnou evidenční strukturu tak, aby konkrétní VZ a závěry posouzení byly vždy jednoduše dohledatelné.

Důležité je rovněž v interních procesech zakotvit, že zpracované hodnocení rizik je obecně považováno za citlivou informaci, kterou není vhodné zveřejňovat a není ani určena k nahlédnutí dodavatelům. Jedná se o interní dokument určený pouze pro potřeby Ministerstva a dle dalších okolností pro odpovídající autority, jakými jsou Úřad pro ochranu hospodářské soutěže (dále jen „ÚOHS") nebo NÚKIB.

3.2.1 Interní postupy v procesu HR

Na Ministerstvu je tedy interně zahájen proces, který je znázorněn na grafu níže. První etapa je odpovědností OVZ a týká se dokumentace k VZ a komunikace s MKB. Další etapy jsou již odpovědností MKB.

Obrázek 1 - Vzorový postup v procesu HR



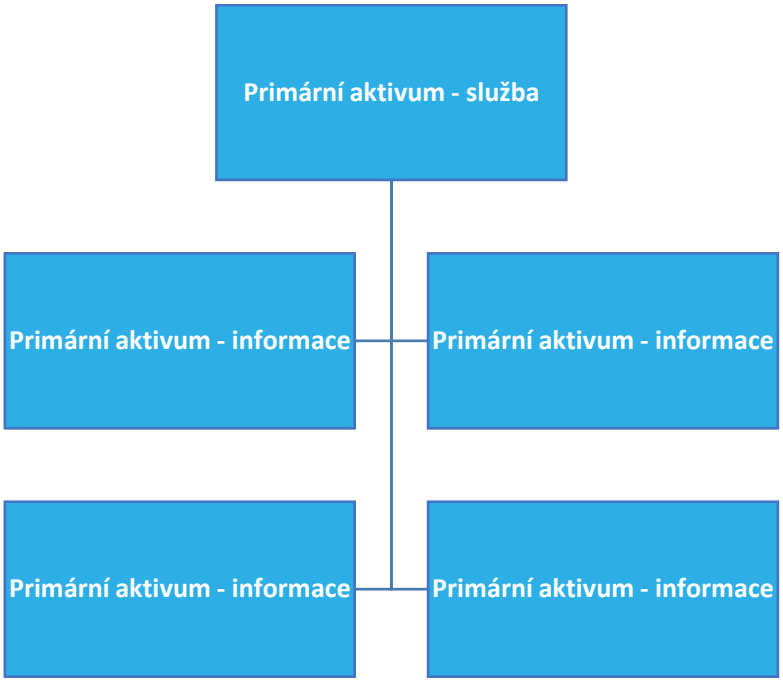
3.3 Metodika HR VZ, přizpůsobení organizaci

Prvotním krokem organizace je vytvoření metodiky pro HR VZ. Nezbytnou součástí je také katalog zranitelností a hrozeb, včetně stanovení stupnic pro jejich hodnocení. Další důležitý bod, co musí metodika obsahovat, je stanovení kritérií pro akceptovatelnost rizik a postupů pro jejich vypořádání. V následujících podkapitolách jsou jednotlivé pojmy popsány. Všechny informace níže uvedené, vyjma informací o podpůrných aktiv, jsou převzaty z Průvodce AR a z vydané metodiky k varování NÚKIB ze dne 17. prosince 2018, která je dostupná na webových stránkách NÚKIB.

3.3.1 Primární aktiva

Za hlavní primární aktivum jsou považovány **služby**, které pracují s dalšími primárními aktivy typu **informace**. Viz následující obrázek:

Obrázek 2 - Hierarchie primárních aktiv



Primární aktiva jsou ohodnocena z pohledu důvěrnosti, integrity, dostupnosti a ztráty dat. Při posuzování hodnoty aktiv je nutné uvažovat o nejhorším možném scénáři a nebrat v úvahu zavedená bezpečnostní opatření. Musí být evidovány jak vazby mezi primárními aktivy, tak i vazby mezi primárními a podpůrnými aktivy. Hodnocení primárních aktiv probíhá na základě dopadové tabulky.

Hodnocení primárních aktiv může dosahovat těchto hodnot pro každý jednotlivý atribut (důvěrnost, integrita, dostupnost, ztráta). Kompletní tabulka hodnot je uvedena v metodice v Průvodci řízení aktiv a rizik dle VKB, přesněji v příloze 2 - Vzorová metodika pro identifikaci a hodnocení rizik.

Tabulka 4 - Stupnice pro hodnocení primárních aktiv

Stupnice pro hodnocení primárních aktiv	
1	Nízká
2	Střední
3	Vysoká
4	Kritická

3.3.2 Podpůrná aktiva

Za podpůrné aktivum je v rámci HR VZ považován předmět VZ. Dle povahy VZ se tak může jednat o technické aktivum (HW, SW) nebo např. služby podpory. Podpůrná aktiva jsou stejně jako primární aktiva hodnocena z pohledu důvěrnosti, integrity, dostupnosti a ztráty dat. Výsledné hodnoty jsou poté chápány jako dopad, který vstupuje do vzorce výpočtu rizik.

3.3.3 Katalog hrozeb a zranitelností

Hrozbou se rozumí událost či aktivita, která má vliv na bezpečnost a může zapříčinit škodu. Hrozba může být úmyslná, neúmyslná či na základě vyšší moci. Zranitelností se rozumí vlastnost

aktiva, jeho slabina či nedostatek, který může být zneužit jednou či více hrozbami a generovat tak nežádoucí vliv. Jedná se o citlivost aktiva vzhledem ke konkrétní hrozbě.

Dle § 5 odst. 1 písm. b) VKB je nutné, aby byl vytvořen katalog hrozeb a zranitelností. Katalog by měl vycházet z kategorií popsaných v příloze č. 3 VKB a následně může být také využita metodika k varování NÚKIB ze dne 17. prosince 2018, která je dostupná na webových stránkách NÚKIB. Vytvořený katalog by měl být upraven pro potřeby konkrétní organizace.

Tabulka 5 - Katalog zranitelností

Zranitelnost
nedostatečná údržba aktiv
zastaralost aktiv
nedostatečná ochrana perimetru
nedostatečné bezpečnostní povědomí lidských zdrojů
nevhodné nastavení přístupových oprávnění
nedostatečné monitorování činnosti lidských zdrojů, neschopnost odhalit jejich pochybení, nevhodné nebo závadné způsoby chování
nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů
nedostatečná ochrana aktiv
nevhodná bezpečnostní architektura
nedostatečná míra nezávislé kontroly
nedostatek zaměstnanců s potřebnou odbornou úrovní

Tabulka 6 - Katalog hrozeb

Hrozba
porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů
poškození nebo selhání technického nebo programového vybavení
zneužití identity fyzické osoby
užívání programového vybavení v rozporu s licenčními podmínkami
působení škodlivého kódu (například viry, spyware, trojské koně)
narušení fyzické bezpečnosti
přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie
zneužití nebo neoprávněná modifikace údajů
ztráta, odcizení nebo poškození aktiva
nedodržení smluvního závazku ze strany dodavatele
pochybení ze strany zaměstnanců a administrátorů

zneužití vnitřních prostředků, sabotáž
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik
zneužití vyměnitelných technických nosičů dat
napadení elektronické komunikace (odposlech, modifikace)

3.3.4 Hodnocení hrozeb a zranitelností

U hrozby se hodnotí pravděpodobnost, s jakou nastane, viz tabulka 7.

Tabulka 7 - Stupnice pro hodnocení hrozeb

Stupnice pro hodnocení hrozeb		
1	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za pět let.
2	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od jednoho roku do pěti let.
3	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od jednoho měsíce do jednoho roku.
4	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

U zranitelnosti se hodnotí, jak je pravděpodobné její zneužití a jestli existují bezpečností opatření, která by vedla ke snížení možnosti jejího zneužití.

Tabulka 8 - Stupnice pro hodnocení zranitelností

Stupnice pro hodnocení zranitelností		
1	Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
2	Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
3	Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována, nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

3.3.5 Hodnocení rizik

Identifikace rizik je vytváření relevantních kombinací aktivum-zranitelnost-hrozba. Jejím účelem není vytvoření kombinací všeho se vším. Např. u aktiv typu lidské zdroje nemá smysl vytvářet

kombinace obsahující zranitelnosti typu nedostatečná údržba a hrozby typu poškození nebo selhání technického nebo programového vybavení. Je potřeba zvážit všechny relevantní varianty s ohledem na celou trojici aktivum-zranitelnost-hrozba.

Pro výpočet rizika jsou nejčastěji využívány funkce, které ovlivňuje dopad, hrozba a zranitelnost:

Riziko = dopad x hrozba x zranitelnost

Analýza rizik je v souladu s VKB ohodnocení relevantních kombinací aktivum-zranitelnost-hrozba a výpočet výsledné hodnoty rizika podle příslušného vzorce.

Vyhodnocení znamená porovnání výsledné hodnoty rizika s kritérii pro akceptovatelnost a rozhodnutí, zda bude riziko akceptováno nebo bude snižováno.

Tabulka 9 - Stupnice pro hodnocení rizik a kritéria pro akceptovatelnost

Stupnice pro hodnocení rizik			Proces zvládání rizik
1-16	Nízká	Riziko je považováno za přijatelné – akceptovatelné.	Riziko akceptuje MKB ve spolupráci s GA. Dále riziko monitorují. V případě zájmu se výbor KB může o těchto rizicích informovat.
17-31	Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.	V případě způsobu zvládání rizika „Akceptovat“ riziko akceptuje MKB ve spolupráci s GA. V případě způsobu zvládání rizika „Snížit“ navrhuje bezpečnostní opatření ARCHKB ve spolupráci s MKB. Navržený způsob zvládání rizik včetně bezpečnostního opatření prezentuje MKB Výboru pro KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládání.
32-47	Vysoká	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	Způsob zvládání rizika navrhuje MKB ve spolupráci s GA. V případě návrhu způsobu zvládání rizika „Snížit“ navrhuje bezpečnostní opatření ARCHKB ve spolupráci s MKB. Navržený způsob zvládání rizik včetně bezpečnostního opatření prezentuje MKB Výboru pro KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládání.
48-64	Kritická	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	Způsob zvládání rizika navrhuje MKB ve spolupráci s GA. V případě návrhu způsobu zvládání rizika „Snížit“ navrhuje bezpečnostní opatření ARCHKB ve spolupráci s MKB. Navržený způsob zvládání rizik včetně bezpečnostního opatření prezentuje MKB Výboru pro KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládání. V případě naléhavosti zvládnutí rizika lze postupovat způsobem popsaným v metodice.

Identifikovaná a ohodnocená rizika je potřeba vhodným způsobem ošetřit tak, aby nebyla organizací ignorována. V závislosti na výstupu z hodnocení rizik je potřeba určit způsob jejich zvládnutí.

Tabulka 10 - Způsoby zvládání

Zvládání	Popis
Akceptace	S rizikem jako takovým se již nic dále nedělá, pouze se přijme, tedy dochází k podstoupení rizika. Používá se pro rizika nízké až střední úrovně.

Sledování	Riziko již není dále snižováno, ale je pečlivě sledováno v čase. Zejména zda nedochází k navýšení v oblasti dopadu, pravděpodobnosti hrozby, nebo míry zranitelnosti s rizikem spojeným. Používá se pro rizika střední úrovně.
Redukce	Dochází k aplikování vhodných bezpečnostních opatření za účelem snížení rizika na nižší úroveň (v ideálním případě akceptovatelnou). Je možné využít pro všechny úrovně rizik, zejména se používá pro rizika střední až kritické úrovně.
Eliminace	Spočívá v nalezení jiného řešení dané situace, které rizikovou událost neobsahuje.
Vyhnutí	Utlumení (velmi omezené využití), nebo vypnutí (nepoužívání) daného aktiva.
Přenos a sdílení	S rizikem jako takovým se nic neděje, pouze dochází k jeho přenesení (resp. dopadu, který může nastat) na třetí stranu (např. pojišťovnu), která je s tímto přenosem ztotožněna a souhlasí s ním. Je možné využít pro všechny úrovně rizik, zejména se používá pro rizika střední až kritické úrovně.

Zvládání rizik navrhuje MKB ve spolupráci s architektem KB a garantem aktiva. Všechna rizika musí být monitorována a přezkoumávána, přinejmenším **jednou ročně** v rámci celkového hodnocení rizik.

Pro zvládání rizik slouží navržená bezpečnostní opatření, která je nutné v rámci organizace evidovat. Dle VKB se jedná o plán zvládání rizik, který je povinným dokumentem při řízení rizik podle § 5. V něm organizace také zohlední například významné změny nebo změny rozsahu systému řízení bezpečnosti informací. V rámci § 8 VKB, resp. při procesu HR VZ mohou organizace využít obdobné dokumenty, které potřebné údaje obsahují. Cílem tohoto kroku je nalézt systematický přístup k zavádění navrhovaných bezpečnostních opatření, stanovení jejich prioritizace, a v neposlední řadě také efektivní plánování finančních, lidských a technických zdrojů. Stejně tak je potřeba stanovit odpovědné osoby za splnění jednotlivých bezpečnostních opatření, včetně termínů pro jejich zavedení. S dokumentací by mělo být aktivně pracováno (tj. měla by být pravidelně aktualizována).

3.4 Proces posouzení VZ

Účelem této kapitoly je přiblížení klíčového procesu posouzení VZ na Ministerstvu, který je zaveden pro hodnocení rizik v souvislosti s předmětem výběrového řízení. Právě v této kapitole bude v jednotlivých krocích nastíněn možný postup, který je potřeba přizpůsobit kontextu každé organizace.

3.4.1 Účel posouzení

HR VZ nespočívá pouze v tom, aby bylo vyhověno legislativě (viz kap. 2), ale rovněž aby na Ministerstvu byla mapována rizika spojená s KB, jež se mohou vztahovat nebo vztahují k výběrovým řízením. Je samozřejmě možné nastavit si interně scénáře, které budou automaticky vylučovat některé předměty VZ za přesně daných podmínek, aby nemusely být posuzovány zakázky nerelevantního typu. Na druhou stranu, posouzení každé zakázky dává určitou míru lepší kontroly před možným pochybením, čemuž se někdy také říká tzv. kontrola čtyř očí (stejnou věc zkontrolují dvě osoby).

Pokud tedy bude Ministerstvo provádět i nadále posuzování VZ ve vztahu ke KB, bude nejen v souladu s legislativními požadavky, ale zejména bude monitorovat možné negativní vlivy zasahující do vnitropodnikových systémů či procesů a bude schopno minimalizovat s tím spojená rizika. V návaznosti na to navrhne, a poté nasadí patřičná opatření, která sníží možný dopad na

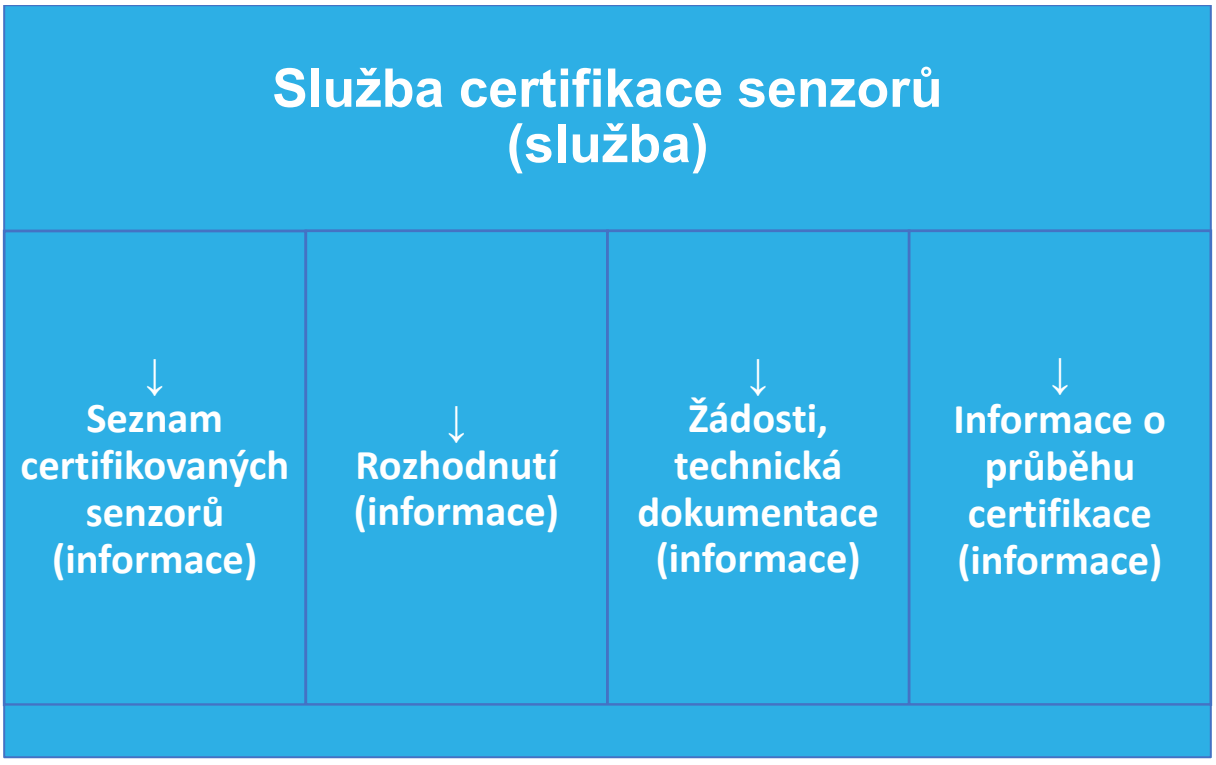
Ministerstvo v rámci jeho provozu, poskytování služeb apod. Dopad opatření samozřejmě nemusí být pouze externí, ale také interní, pokud bude potřeba aplikovat nákladnější opatření, o čemž poté rozhoduje příslušný garant primárního aktiva, ke kterému se předmětná VZ ve formě podpůrného aktiva vztahuje.

3.4.2 Primární a podpůrné aktivum

Ministerstvo má již primární aktiva identifikována a ohodnocena (z pohledu důvěrnosti, integrity, dostupnosti a ztráty), a proto při HR VZ zvažuje již primární aktivum s konkrétními hodnotami. Na Ministerstvu je takovým aktivem s nejvyššími hodnotami bezpečnostních atributů **Služba certifikace senzorů**. Bez této služby by nebyl naplňován záměr fungování Ministerstva, které by tak nemohlo plnit své závazky v rámci vydávání certifikací, a tím by jeho činnost prakticky zanikla. Při HR VZ je proto nezbytné vědět, jaká primární aktiva Ministerstvo spravuje, aby bylo zřejmé, které z těchto primárních aktiv je prioritní k zachování jeho důvěrnosti, integrity a dostupnosti (CIA). Na toto prioritní aktivum jsou navázána podpůrná aktiva, kterými v tomto případě jsou jednotlivé předměty VZ. Předmětem VZ tak bude např. „Nákup komunikačních prostředků a technického vybavení (HW) pro agendový IS pro evidenci a zpracování procesu certifikace senzorů“.

Posuzování VZ skrze ovlivněná primární aktiva je pouze jedním z možných přístupů. Organizace si může zvolit jiný postup pro stanovení toho, které VZ jsou vhodné pro provedení hodnocení rizik a které nikoliv.

Obrázek 3 - Vazby mezi primárními aktivy



3.4.3 Posouzení VZ

Velký díl zodpovědnosti nese již prvotní posouzení dokumentace VZ, která byla OVZ umístěna na sdílené úložiště, a tím dána k dispozici MKB k nastudování. O poskytnutí dokumentace je zároveň informován také zaměstnanec odpovědný za smluvní vztah. MKB, případně jím pověřený MKBJR, bude muset zvažovat rizika spojená s touto VZ, včetně jejich dopadu do prostředí Ministerstva,

ale zejména do předmětné Služby certifikace senzorů. Zde dochází ke klíčovému rozřazování VZ. Některé jsou bez významného dodavatele a bez potřeby zpracování další analýzy. Jiné zase svými rysy naplňují potřebu dalšího analytického posouzení. Takové analytické posouzení bude muset přijít v případě, kdy bude u příslušné VZ identifikován **významný dodavatel** (tato povinnost přímo vyplývá z § 8 odst. 2 VKB, viz kapitoly 2.1 a 2.2).

Obecně je však možné provést další hodnocení rizik i na základě odst. 1 písm. e) tohoto ustanovení, kdy je potřeba řídit rizika spojená s dodavateli. Pro Ministerstvo to v praxi znamená, že může hodnocení rizik v této fázi provádět také tehdy, pokud to uzná za vhodné. Organizace si sama musí určit, jak k samotnému procesu posouzení přistoupí a zda bude striktně dodržovat postup, kdy se hlubší analýza provádí pouze u významného dodavatele, popř. u vydaných varování. Významnost dodavatele pro konkrétní aktivum by se však měla posuzovat vždy.

Aby mohlo být výše uvedené řádně vyhodnoceno, nepodílí se na procesu posouzení pouze MKB, popř. MKBJR, ale také další osoby, které na vyžádání s rozhodnutím mohou pomoci. Těmito osobami jsou pak např. ARCHKB, GA. Konzultační roli mohou zastoupit i jiné osoby určené jako poradní v těchto záležitostech, které budou mít dostatečný vhled do problematiky KB. Určené osoby je poté vhodné zařadit do RACI matice (viz kap. 3.1), která bude charakterizovat jednotlivé pracovní role a jejich odpovědnosti v probíhajícím procesu.

Konzultantem v těchto věcech by neměl být AUDKB z důvodu zachování jeho nestrannosti.

Ministerstvo se při rozlišování toho, kdy má nebo nemá provádět další detailnější hodnocení rizik, řídí například níže uvedenými principy, které charakterizují, kdy se provedení detailnějšího hodnocení rizik vyžaduje nebo alespoň doporučuje.

- Jedná se o významného dodavatele,
- jedná se o klíčový nebo důležitý proces či službu,
- ve VZ není požadován konkrétní výrobce a Ministerstvo si není jisté, zda společnosti uvedené ve varování[8] poptávané technické či programové prostředky také nevyrábí,
- aplikace nebo systém je relevantní pro vztahy s osobami navázanými k primárnímu aktivu ke Službě certifikace senzorů.

Naproti tomu zde níže uvedené body popisují, kdy provedení dalšího hodnocení rizik zpravidla není nutné.

- Nejedná se o významného dodavatele,
- VZ nemá dopad na primární aktiva Ministerstva (Služba certifikace senzorů a informace v ní obsažené),
- jedná se o zakoupení technické podpory k již zakoupeným zařízením/licencím výrobce, které nejsou zahrnuty ve varování,
- jedná se o konzultační služby,
- jedná se o VZ na služby, kdy předmět VZ není relevantní ve vztahu ke KB,

[8] Varování NÚKIB ze dne 17. prosince 2018 před použitím technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation, viz také kapitola 2.4.

- dodavatel nebude mít ke svému produktu vzdálený přístup nebo zařízení nic nereferuje mimo perimetr Ministerstva.

Jedná se o příkladový výčet, který je fakticky mnohem širší a je potřeba vždy zvažovat konkrétní dopady každé zakázky do prostředí Ministerstva, stejně tak to, zda zakázka má relevanci vůči KB, a pokud ano, jak vážnou.

3.4.4 Významný dodavatel

V případě významného dodavatele (viz kapitoly 2.2 a 2.3) se jedná o každého dodavatele, který s Ministerstvem vstupuje do právního vztahu a jehož dodávka služeb nebo výpadek těchto služeb může mít vliv na primární aktiva, které Ministerstvo identifikovalo, resp. na KB. To znamená, že se v rámci VZ pro Ministerstvo soutěží dodavatel, který bude mít podstatný vliv nebo dopad na fungování Služby certifikace senzorů. Takový dodavatel bude mít pro Ministerstvo klíčovou roli (ať již v dodávce materiálu, techniky, služby), bez které by provoz informačního systému zajišťujícího Službu certifikace senzorů nebyl možný, byl ztížený nebo jinak negativně ovlivněný. Zároveň se může jednat o dodavatele, který je jedinečný na trhu (nemohla by za něj být nalezena náhrada, anebo jen velmi obtížně). Zcela jistě by šlo uvést další příklady. Smyslem uvedeného je však zmínit, že tento dodavatel má vliv na identifikované primární aktivum, který není pro Ministerstvo zanedbatelný. Průvodce AR o uvedeném pojednává např. v kapitole 4.2.2.

V případě identifikování dodavatele jako významného fakticky nastává pro Ministerstvo další krok v procesu HR VZ, kterým je zpracování hlubší analýzy (viz kap. 3.5). Zároveň je potřeba neopomenout, že v procesu řízení dodavatelů je nutné v souvislosti s řízením rizik spojených s významnými dodavateli zajistit, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 VKB. Zapracování tohoto požadavku v prostředí Ministerstva provádí právník zabývající se zapracováním výstupů hodnocení rizik do zadávací dokumentace k VZ. V souvislosti s významnými dodavateli vede Ministerstvo rovněž jejich evidenci. Další povinnosti spojené s dodavateli jsou popsány v kapitole 2.

3.4.5 Opatření NÚKIB

S HR VZ je na Ministerstvu spjata také povinnost dbát veškerých opatření (viz kapitola 2.4) vydaných ze strany NÚKIB. Co je jejich předmětem, je již uvedeno v předchozím textu. V tomto případě MKB musí reflektovat, na co které opatření cílí, a přizpůsobit tomu proces hodnocení rizik. V případě modelového příkladu bude potřeba přistoupit ke zpracování analýzy a tato opatření zohlednit. Každé opatření podle § 11 ZKB má svá specifika a je potřeba je zvažovat společně, na konkrétní typ organizace. Pakliže je možnost, že se do výběrového řízení přihlásí dodavatel, který bude mít vazby na osoby/instituce/technologie/atd. podléhající opatření, musí to být zohledněno v další analýze při hodnocení rizik s příslušným bezpečnostním opatřením, které bude předcházet riziku plynoucímu z relevantních opatření NÚKIB.

3.4.6 Stanovisko pro OVZ

Posledním krokem v této fázi je vydání stanoviska od MKB, ve kterém rozhoduje, zda se **jedná či nejedná o významného dodavatele** a zda se **bude či nebude zpracovávat obsáhlejší analýza.** Předmětné stanovisko může být samostatné, nebo být součástí zaslané dokumentace jako část formuláře k vyplnění. Dokumentace spolu se stanoviskem bude zaslána zpět na OVZ a v kopii také na zaměstnance odpovědného za smluvní vztah. O stanovisku jsou však na Ministerstvu informováni rovněž garanti VZ, kteří budou ručit za následná bezpečností opatření vyplývající z provedené analýzy. Veškerá provedená posouzení dokumentace k připravovaným VZ se na Ministerstvu zapisují do evidence posouzených VZ (viz Tabulka 4 Evidenční list), kde se rovněž

uvádí, zda byla či nebyla zpracována další dílčí část procesu HR VZ, tedy hlubší analýza dané VZ. Poté, co MKB odešle své stanovisko (s ostatní dokumentací) na OVZ, nastávají dvě možné situace:

- VZ byla posouzena a nebyla vyhodnocena nutnost dalšího rozboru.
  - Je zasláno stanovisko na OVZ, VZ zapsána do evidence u MKB, práce na posuzování končí.
- VZ byla posouzena a bylo vyhodnoceno provedení další analýzy na VZ.
  - Je zasláno stanovisko na OVZ, VZ zapsána do evidence u MKB, počíná běžet další lhůta na zpracování hodnocení rizik k VZ, které MKB zpracuje a které bude sloužit jako podklad pro další rozhodování při aplikaci vzešlých bezpečnostních opatření a při tvorbě smluvního ujednání.

3.5 Zpracování HR VZ

Jakmile proběhne proces posouzení VZ, na jehož základě se rozhodne o tom, že dodavatel předmětné VZ bude určen jako významný, přistupuje se ke zpracování HR VZ. Tento proces zahrnuje identifikaci, analýzu a ohodnocení potenciálních bezpečnostních rizik vztažených na primární aktiva a informační systémy organizace (v případě tohoto dokumentu Ministerstva). Účelem tohoto procesu je rozpracování a shrnutí výsledků provedeného hodnocení rizik předmětu VZ. Vzniklý dokument je podkladem pro další fáze výběrového řízení. Jednotlivé kroky HR VZ jsou popsány v níže uvedených podkapitolách. U každého kroku jsou následně uvedeny konkrétní modelové situace v rámci Ministerstva. Důležité je také zmínit, že se jedná pouze o jeden z možných přístupů, který může být podle potřeby organizace upraven.

Doporučením při prováděném HR VZ je v rámci ekonomického přístupu stanovit jedno klíčové primární aktivum, které je zakázkou ovlivněno, dále podpůrné aktivum nebo aktiva dle předmětu plnění VZ a následně nezbytnou míru navazujících hrozeb a zranitelností.

Je pravděpodobné, že u dotčeného IS, na nějž je směřována VZ, bude v rámci hodnocení rizik (dle § 5) identifikována vazba hned na několik primárních aktiv. Klíčové primární aktivum v kontextu HR VZ lze tak identifikovat např. jako aktivum s nejvyššími hodnotami bezpečnostních atributů (důvěrnost, dostupnost, integrita) z množiny všech již identifikovaných primárních aktiv.

Identifikovaná podpůrná aktiva by vždy měla odpovídat předmětu plnění VZ. U jednodušších VZ lze identifikovat pouze jednotky podpůrných aktiv, u složitějších VZ jich zpravidla bude více. Množství podpůrných aktiv také ovlivňuje míra detailu, kterou zadavatel má o výsledném řešení, např. zda kupuje zařízení, systém nebo službu bez znalosti přesných technických specifikací nebo procesů, nebo konkrétní zařízení, u kterého zná všechny podrobnosti.

Identifikované hrozby a zranitelnosti by měly být relevantní pro daný předmět VZ. Jejich identifikace je závislá na konkrétním předmětu plnění VZ a dalších okolnostech, jako jsou např. platná varování NÚKIB a k nim vydaná doporučení.

3.5.1 Identifikace a ohodnocení aktiv

Prvním krokem je identifikace ohroženého primárního aktiva (služby nebo informace), které je v kontextu hodnocení VZ klíčové nebo důležité pro danou organizaci (pro jeho chod, dodržení závazků apod.). Doporučením je identifikovat jedno klíčové aktivum. Vstup pro tuto identifikaci již existuje, a to konkrétně v rámci procesu posouzení VZ (kapitola 3.4), kde je analýza možných dopadů na primární aktiva jedním z kroků, podle kterého se organizace rozhoduje, zda dodavatele určí jako významného a bude tak platit povinnost zpracovat HR VZ.

Za podpůrné aktivum je zpravidla považován předmět VZ, nicméně v potaz by vždy měla být brána složitost VZ.

Pro hodnocení aktiv se používá metodika, která musí být v souladu s VKB (viz kapitola 2.5).

Modelový příklad:

Ministerstvo v kontextu VZ identifikovalo pět relevantních primárních aktiv PA1 až PA5 (viz tabulka). K těmto aktivům má identifikované garanty, kteří zodpovídají za jejich bezpečnost a s jejichž pomocí stanovilo hodnoty jednotlivých atributů bezpečnosti informací. Tato aktiva by měla být na Ministerstvu již identifikována a ohodnocena v rámci celkového řízení aktiv a rizik dle § 4 a 5. Nejedná se tak o procesní krok, který probíhá až při HR VZ. Organizace by měla mít veškerá aktiva již identifikována dle § 4 VKB a při HR VZ se tato data přebírají pouze jako vstup. Pro modelový příklad bylo vybráno aktivum PA1, jehož hodnoty budou vstupními hodnotami pro další kalkulaci.

Tabulka 11 - Modelový příklad – Primární aktiva I.

ID	Název	Popis	Dostupnost	Ztráta	Důvěrnost	Integrita
PA1	Služba certifikace senzorů	Zajištění procesu certifikace a evidence senzorů	3	4	3	3
PA2	Seznam certifikovaných senzorů	Seznam všech úspěšně certifikovaných senzorů i certifikátů samotných	2	1	1	3
PA3	Rozhodnutí	Výsledné rozhodnutí certifikačního procesu – negativní i pozitivní	2	3	3	3
PA4	Žádosti, technická dokumentace	Technická dokumentace a žádost o certifikaci, kterou zasílají jednotliví výrobci ke svým senzorům	3	3	3	3
PA5	Informace o průběhu certifikace	Informace o průběhu certifikace – kdo rozhodl, kdy došla žádost, průběh certifikace atd.	3	4	3	3

Tabulka 12 - Primární aktiva II.

ID	Název	Kategorie	Garant aktiva
PA1	Služba certifikace senzorů	Služba	Jan Novák, Tereza Černá
PA2	Seznam certifikovaných senzorů	Informace	Renata Malá
PA3	Rozhodnutí	Informace	Jan Novák, Tereza Černá
PA4	Žádosti, technická dokumentace	Informace	Jan Novák, Tereza Černá
PA5	Informace o průběhu certifikace	Informace	Jan Novák, Tereza Černá

Jelikož předmětem výběrového řízení je nákup páskových knihoven pro certifikační IS, jsou páskové knihovny jediným aktivem, které se bude v rámci HR VZ hodnotit. Poptávaný předmět výběrového řízení je určen pro zajištění provozu informačního systému poskytujícího certifikační službu. Předmět výběrového řízení bude dodavatelem instalován a provozován ve vlastním datovém sálu Ministerstva, přičemž dodavatel bude poskytovat servisní podporu.

Hodnocení podpůrného aktiva vychází z vlastní metodiky Ministerstva pro HR VZ a provádí se s garantem VZ.

Tabulka 13 - Podpůrná aktiva I.

ID	Podpůrné aktivum	Dostupnost	Ztráta	Důvěrnost	Integrita
POD01	Páskové knihovny	3	3	4	4

Tabulka 14 - Podpůrná aktiva II.

ID	Podpůrné aktivum	Kategorie	Garant VZ
POD01	Páskové knihovny	HW	Tomáš Fiala

Ohodnocení podpůrných aktiv probíhá individuálně s určeným garantem. Garant rozhodl, že v souladu s interní metodikou Ministerstva ohodnotí atributy důvěrnost a integrita hodnotou 4 (kritická) a atributy dostupnost a ztráta hodnotou 3 (vysoká). Tyto hodnoty budou dále při výpočtu rizik použity jako hodnota dopadu. Jedná se o vliv narušení jednoho z atributů bezpečnosti na primární aktivum.

3.5.2 Identifikace zranitelností a hrozeb

Po identifikaci a ohodnocení aktiv se zpravidla přistoupí k identifikaci zranitelností. Seznam zranitelností může vycházet z interně definovaného katalogu zranitelností nebo z přílohy č. 3 VKB. Nad rámec těchto zranitelností je možné zohlednit i specifické zranitelnosti, které jsou relevantní pro danou VZ.

Obdobný postup je aplikován i u hrozeb, tj. seznam může vycházet z interně definovaného katalogu nebo VKB, příp. v odůvodněných případech se mohou identifikovat i hrozby v rámci varování NÚKIB. Nad rámec těchto hrozeb je opět možné zohlednit i specifické hrozby, které jsou relevantní pro danou VZ.

Modelový příklad:

Ministerstvo na základě interního katalogu identifikovalo pro hodnocení rizik následující zranitelnosti:

Tabulka 15 - Identifikované zranitelnosti

ID	Popis zranitelnosti
Z1	Nedostatečné bezpečnostní povědomí lidských zdrojů
Z2	Nedostatečná údržba aktiv
Z3	Nedostatečná míra nezávislé kontroly

Stejným způsobem byly identifikovány i hrozby:

Tabulka 16 - Identifikované hrozby

ID	Popis hrozby	Bezpečnostní atribut
H1	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	CIA

H2	Poškození nebo selhání technického nebo programového vybavení	CA
H3	Nedodržení smluvního závazku ze strany dodavatele	CIA
H4	Pochybení ze strany zaměstnanců a administrátorů	CIA

Při posouzení VZ byla ze strany MKB identifikována skutečnost, že v rámci VZ se může přihlásit dodavatel, který dodává technické prostředky, které jsou předmětem varování ze dne 17. prosince 2018. Následně byly identifikovány níže uvedené dodatečné hrozby dle Metodiky k varování NÚKIB ze dne 17. prosince 2018:

Tabulka 17 - Identifikované hrozby z varování

ID	Popis hrozby	Bezpečnostní atribut
HV1	Přístup k veškerým datům	CIA
HV2	Kontrola nad obsahem přenášených dat	C
HV3	Možnost odepření služby	IA

Obdobně se, v rámci identifikace hrozeb, může postupovat i v případě ostatních varování, která jsou pro danou VZ relevantní. Může se jednat např. o varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací nebo varování spočívající v instalaci a používání aplikace TikTok.

Pro úplnost je níže znázorněna matice hrozeb a zranitelností definovaná dle interní metodiky Ministerstva. Křížek znamená, že daná zranitelnost je relevantní pro danou hrozbu. Matice bude následně využita při výpočtu hodnot rizik.

Tabulka 18 - Matice hrozeb a zranitelností

-	Z1	Z2	Z3
H1	**X**	**x**	**x**
H2		**x**	
H3	**X**		**x**
H4	**X**	**x**	**x**
HV1		**x**	**x**
HV2		**x**	**x**
HV3		**x**	**x**

Výše identifikované seznamy tak představují všechny hrozby a zranitelnosti, které budou do HR VZ vstupovat.

3.5.3 Ohodnocení hrozeb a zranitelností

Po identifikaci hrozeb a zranitelností je přistoupeno k jejich ohodnocení na základě interně definované metodiky, viz kapitola 3.3. Při hodnocení hrozeb a zranitelností se vychází ze standardních postupů hodnocení rizik, např. dle Průvodce AR. Hodnocení hrozeb a zranitelností je posuzováno s ohledem na bezpečnostní opatření, která již má organizace nasazena a která mohou hodnotu hrozby snížit, a současně také s ohledem na ustanovení budoucích smluv, která hodnotu pravděpodobnosti hrozeb a zranitelností rovněž snižují.

Výjimku tvoří hrozby uvedené NÚKIB ve vydaných varováních. U hrozeb identifikovaných z varování NÚKIB je nutné vyplnit dvě hodnoty – pro *rizikové technologie* a pro *ostatní*

technologie, které nejsou předmětem varování. Hodnoty pro rizikové technologie jsou předmětem varování NÚKIB a HR VZ je tak automaticky přebírá. Hodnoty pro ostatní technologie jsou vyplněny ve spolupráci např. s garantem VZ či jinou odpovědnou osobou (např. zaměstnancem odpovědným za smluvní vztah).

Modelový příklad:

Pro podpůrné aktivum – předmět VZ byly ve spolupráci s garantem VZ identifikované zranitelnosti ohodnoceny v souladu s interní metodikou HR VZ, a to následujícím způsobem.

Tabulka 19 - Hodnocení zranitelností

ID	Popis zranitelnosti	Z-OST
Z1	Nedostatečné bezpečnostní povědomí lidských zdrojů	3
Z2	Nedostatečná údržba aktiv	3
Z3	Nedostatečná míra nezávislé kontroly	4

Obdobným způsobem proběhlo i ohodnocení hrozeb ve vztahu k podpůrnému aktivu – předmět VZ. Hrozby H1-H6 byly ohodnoceny pouze v kontextu *ostatních technologií* (H-OST), tj. technologií, které nejsou předmětem žádného varování NÚKIB. Hrozby HV1-HV3 byly ohodnoceny jak v kontextu ostatních technologií, tak *rizikových technologií* (H-RIZ), tj. technologií, které jsou předmětem některého z varování NÚKIB (v tomto případě varování ze dne 17. prosince 2018). U těchto rizikových technologií bylo přihlédnuto k varování NÚKIB a všechny hrozby tak byly ohodnoceny hodnotou 4 (kritická).

Tabulka 20 - Hodnocení hrozeb

ID	Popis hrozby	H-OST	H-RIZ
H1	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	2	-
H2	Poškození nebo selhání technického nebo programového vybavení	3	-
H3	Nedodržení smluvního závazku ze strany dodavatele	3	-
H4	Pochybení ze strany zaměstnanců a administrátorů	2	-
HV1	Přístup k veškerým datům	2	4
HV2	Kontrola nad obsahem přenášených dat	2	4
HV3	Možnost odepření služby	2	4

3.5.4 Výpočet rizik

Po předchozích krocích se přistoupí k vyhodnocení identifikovaných rizik. Toto vyhodnocení je založeno na kalkulaci kombinací hrozby, zranitelnosti a dopadu na aktivum a je většinou prováděno automaticky pomocí např. tabulkového procesoru (MS Excel) nebo specifického nástroje pro hodnocení rizik. Propočet probíhá vždy dle interně definované metodiky HR VZ. Vzorec výpočtu by měl odpovídat všem požadavkům VKB, viz kapitola 2.5.

Jako dopad se bere hodnota podpůrného aktiva (předmět VZ).

U hrozeb je nutné brát v potaz bezpečnostní atributy, které hrozba ohrožuje. Ne každá hrozba ohrožuje všechny atributy, což je při výpočtu nutné zohlednit. Pokud hrozba ohrožuje např. pouze dostupnost, tak je nutné dopad kvantifikovat pouze skrze atribut dostupnosti u aktiva. Pokud hrozba ohrožuje více bezpečnostních atributů, tak se vždy bere nejvyšší identifikovaná hodnota dopadu (= hodnoty aktiva).

U hrozeb je nutné rovněž zohledňovat varování NÚKIB a doporučené hrozby. Vzhledem k tomu, že v rámci hrozeb identifikovaných dle doporučení NÚKIB dochází ke dvojímu hodnocení (např. rizikové technologie a ty ostatní), pak i při hodnocení rizik je výsledné riziko vypočteno dvakrát.

Modelový příklad:

Ministerstvo má pro výpočet rizik v metodice HR VZ definován vzorec:

riziko = dopad (hodnota příslušného aktiva) x hrozba x zranitelnost

Na základě všech dříve identifikovaných hodnot, tak došlo k výpočtu rizik, viz tabulka níže.

Tabulka 21 - Hodnocení rizik

ID	R-OST	R-RIZ
H1Z1	24	-
H1Z3	32	-
H2Z2	36	-
H3Z3	48	-
H4Z1	24	-
H4Z2	24	-
HV1Z2	24	48
HV1Z3	32	64
HV2Z2	18	36
HV2Z3	24	48
HV3Z2	24	48
HV3Z3	32	64

3.5.5 Zvládání rizik

Po identifikaci všech rizik je potřeba přistoupit k jejich zvládání. Způsoby zvládání rizik by měly být zpravidla definované v interní metodice, spolu např. s hranicí akceptovatelných rizik. Obecné způsoby zvládání (akceptace, redukce, přenesení a vyhnutí se) jsou blíže popsány v kapitole 3.3.

Modelový příklad:

Ministerstvo má ve své interní metodice definovány následující způsoby vypořádání rizik – akceptace, sledování, redukce, eliminace, vyhnutí, přenes a sdílení. Hranici pro akceptovatelná rizika má nastavenou na hodnotu rizika 31 (více kapitola 3.3). Na základě této informace přistoupí MKB k filtraci rizik, která jsou akceptovatelná. Všechna nízká rizika jsou automaticky

akceptována, u středních závisí na rozhodnutí MKB (příp. obecně role, která HR VZ zpracovává). U akceptovatelných rizik je nutné zmínit, že hodnota akceptovatelnosti je pouze vodítko a nikoliv hodnota, kterou musí MKB slepě následovat. Jak u nízkých, tak středních (akceptovatelných) rizik lze přistoupit k jiným způsobům vypořádání.

Dle tabulky 22 MKB rozhodl o akceptaci následujících rizik:

Tabulka 22 - Vypořádání rizik – akceptace

ID	Způsob vypořádání
H1Z1	Akceptace
H4Z1	Akceptace
H4Z2	Akceptace
HV1Z2	Akceptace
HV2Z2	Akceptace
HVZ3	Akceptace
HV3Z2	Akceptace

Všechna ostatní rizika již akceptovatelná nejsou a MKB tak bude muset přistoupit k dalším způsobům vypořádání. Při pohledu na tabulku rizik č. 21 je patrné, že rizikové technologie dle varování představují v rámci této VZ velký problém. Většina rizik vázaná k těmto technologiím jsou na nejvyšší úrovni, tj. úrovni kritické. Po uvážení možných bezpečnostních opatření MKB rozhodl, že jejich potenciální implementace by byla velice finančně náročná a po jejich implementaci by byla vyžadována neustálá kontrola, na kterou Ministerstvo nemá kapacity. Z toho důvodu je pro MKB jednou z možností přistoupení k aplikaci způsobu vypořádání – eliminaci. V tomto konkrétním příkladu to znamená, že MKB navrhne dodavatele, kteří nabízí technologické a programové prostředky, které jsou předmětem varování, z VZ vyloučit a jejich nabídky neakceptovat. Všechny tyto úvahy ve vztahu ke zvládání rizik je nutné řádně zdokumentovat.

Jedná se pouze o modelovou situaci. V tomto případě sice bylo přistoupeno k eliminaci (doporučení vyloučit dodavatele), nicméně to neznamená, že tuto cestu lze univerzálně aplikovat na všechny případy v rámci varování NÚKIB. Jednotlivé případy je nutné individuálně posuzovat a náležitě odůvodnit.

Tabulka 23 - Vypořádání rizik – eliminace

ID	Způsob vypořádání
HV1Z2 – rizikové technologie	Eliminace
HV1Z3 – rizikové technologie	Eliminace
HV2Z2 – rizikové technologie	Eliminace
HV2Z3 – rizikové technologie	Eliminace

HV3Z2 – rizikové technologie	Eliminace
HV3Z3 – rizikové technologie	Eliminace

V rámci rizik, která zbývají, navrhne MKB redukci, tj. implementaci bezpečnostního opatření, které sníží hodnotu rizika. U všech rizik MKB po implementaci bezpečnostních opatření předpokládá, že dojde ke snížení jejich hodnot na akceptovatelnou úroveň.

Tabulka 24 - Vypořádání rizik – redukce

ID	Způsob vypořádání	Zbytkové riziko
H1Z3	Redukce	**16**
H2Z2	Redukce	**24**
H3Z3	Redukce	**24**
HV1Z3 – ostatní technologie	Redukce	**16**
HV3Z3 – ostatní technologie	Redukce	**16**

Řazením podle priorit (prioritizací) může organizace snadněji určit, která bezpečnostní opatření je potřeba implementovat přednostně (tj. která mají nejvyšší prioritu), což souvisí také s tím, že některá aktiva vyžadují vyšší stupeň ochrany. Bezpečnostní opatření nižší priority při pozdějším nasazení definovaného opatření nenese tak velké riziko pro bezpečnost samotného aktiva. MKB v rámci vypořádání rovněž připraví i tabulku s konkrétními bezpečnostními opatřeními a riziky, která se na opatření váží, včetně priorit jednotlivých opatření. To může garantovi VZ pomoci při rozhodování, která opatření řešit přednostně.

Tabulka 25 - Vypořádání rizik – prioritizace opatření

ID	Rizika	Priorita
NO1	H2Z2, H3Z3	**1**
NO2	H1Z3	**3**
NO4	HV1Z3, HV3Z3	**2**

V rámci navržených bezpečnostních opatření je nutné zmínit, že mají pouze doporučující charakter. Vyhodnocení možnosti uplatnění výše uvedených opatření, nákladů na jejich případnou realizaci a efektivity v podobě snížení dopadů při uplatnění zvažovaných rizik musí zvážit zpravidla OVZ, zaměstnanec odpovědný za smluvní vztah, anebo garant VZ.

3.6 Výstupy HR VZ a dopady do dokumentace VZ

Samotným zpracováním hodnocení rizik na konkrétní předmět VZ činnosti nekončí. Hodnocení rizik v předem dohodnuté formě je potřeba předat odpovídajícímu útvaru nebo oddělení, které zajistí, že výstupy navržené v hodnocení jsou náležitým způsobem vypořádány tak, aby došlo k formálnímu naplnění celého procesu. Vypořádáním výstupů hodnocení rizik je v této souvislosti myšlena implementace závěrů hodnocení do zadávací dokumentace VZ, příp. do smluv s dodavateli. Výstupy z HR VZ mohou mít podobu doporučených bezpečnostních opatření, které

musí dodavatel, v rámci přihlášení do VZ, splnit. V opačném případě může následovat vyloučení dodavatele z VZ. K tomuto dochází zejména v souvislosti s varováními NÚKIB, kdy organizace nedokáže implementací bezpečnostních opatření zajistit dostatečnou úroveň bezpečnosti a výsledná rizika tak stále zůstávají vysoká.

Výstupní dokumentaci HR VZ není vhodné zveřejňovat a neměla by být dostupná k nahlédnutí dodavatelům. Je nutné si uvědomit, že se jedná o citlivý dokument v rámci dané organizace, který slouží k naplnění interních procesů. V ojedinělých případech lze tuto dokumentaci však poskytnout relevantním odpovídajícím autoritám jako NÚKIB nebo ÚOHS.

Je rovněž nutné si uvědomit, že zpracováním HR VZ a následným zapracováním do dokumentace VZ nekončí celý proces řízení dodavatelů. Řízení dodavatelů probíhá kontinuálně, a to i v rámci jedné konkrétní VZ. Naplňování bezpečnostních opatření dle HR VZ je nutné průběžně řídit v podobě kontrol dodržování smlouvy a zpracovávání aktualizací hodnocení rizik. Více o této problematice je rozvedeno v kapitole 3.7.

Modelový příklad:

Na Ministerstvu je při hodnocení rizik v procesu zaměřeném na VZ současně také rozveden způsob vypořádání identifikovaných rizik. Stanovisko je na Ministerstvu součástí analýzy, avšak může mít formu samostatného dokumentu. Zvládání rizik pak odráží, zda je potřeba přistoupit k dalším krokům (při vysokém nebo kritickém riziku), anebo postačují již aktuální nasazená opatření (při nízkém nebo středním riziku). Nicméně samotné hodnocení rizikovosti je na odpovědném MKB, který se danými hodnotami může řídit, ale i přesto může navrhovat určitá opatření. Na garantovi/osobě zodpovědné za smluvní vztah je poté zvážit, zda se rozhodne navrhnutá opatření aplikovat dle doporučení MKB (tedy zda v celém rozsahu, a nakolik je to pro podnik ekonomicky únosné).

MKB při hodnocení rizik u jednotlivých kombinací navrhnul některá opatření, na jejichž základě se Ministerstvo rozhodlo k následujícím krokům v podobě vypořádání (ošetření) rizik:

- Akceptací rizik, a to u kombinace rizik H4Z1, H4Z2, HV1Z2, HVZ3 a HV3Z2. Tato uvedená rizika jsou v intervalu hodnot, ve kterém není potřeba nasazovat žádná další opatření oproti stávajícím, tedy již nasazeným. Tato rizika nebudou dále postoupena na OVZ. MKB je však bude dále, v rámci kontinuálního řízení rizik, sledovat a v případě nutnosti, při přezkoumání, potenciálně rozhodne o navýšení hodnoty, resp. zvolí jiný způsob vypořádání.
- Redukcí rizik, a to u kombinace rizik H1Z3, H2Z2, H3Z3, HV1Z3 a HV3Z3. Při redukci klesnou hodnoty na přijatelnou úroveň prostřednictvím zavedení bezpečnostních opatření (doporučuje se u všech rizik s vysokou pravděpodobností hrozby). Zbytkové riziko, které zůstane po aplikování opatření, by již mělo být doporučeno k akceptaci. Tato rizika MKB postoupí na OVZ, které v součinnosti s garantem VZ zajistí implementaci doporučených bezpečnostních opatření do zadávací dokumentace VZ, resp. potenciální smlouvy s dodavatelem.
- Eliminací rizik, a to u kombinace rizik HV1Z2, HV1Z3, HV2Z2, HV2Z3, HV3Z2 a HV3Z3. Zejména bývá u rizik s kritickou úrovní, a také pokud není možné využít žádný z dalších uvedených přístupů pro zvládání rizik (akceptace, přenos na jinou stranu, redukce). V provedeném hodnocení rizik se všechna rizika doporučená k eliminaci váží na rizikové technologie dle varování NÚKIB. MKB zvážil potenciální opatření, která by mohla mitigovat identifikovaná rizika, nicméně žádné ze zvažovaných opatření není aplikovatelné. Z tohoto důvodu je žádoucí eliminace rizik, což v této rovině znamená

doporučení vyloučit z VZ jakéhokoliv dodavatele, který nabídne technologické a programové prostředky dle varování NÚKIB. Toto stanovisko MKB postoupí OVZ, které ve spolupráci s právním oddělením dodavatele vyloučí.

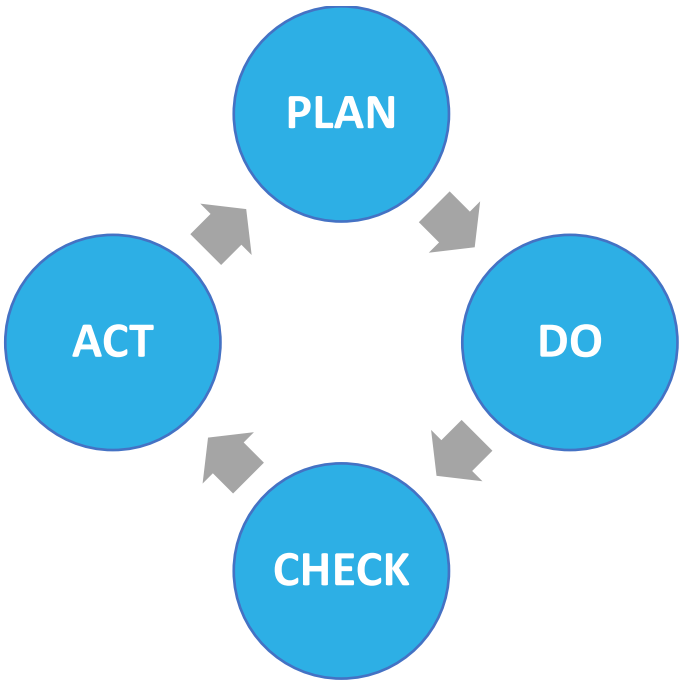
3.7 PDCA cyklus

PDCA cyklus neboli Demingův model, je iterativní metodou postupného zlepšování kvality výrobků, služeb, aplikací či dat. Metoda je založena na neustálém opakování čtyř základních činností – PLAN (plánuj), DO (dělej), CHECK (kontroluj) a ACT (jednej).

- **PLAN** – identifikace procesů (naplánování zamýšleného zlepšení (záměr)
- **DO** – popis a dokumentace procesů (realizace plánu)
- **CHECK** – řízení procesů na základě dokumentace (ověření výsledku realizace oproti původnímu záměru)
- **ACT** – následná optimalizace procesů (úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe)

Nedílnou součástí PDCA cyklu je dokumentace všech etap cyklu. Jednotlivé procesy je třeba identifikovat, popsat a zdokumentovat, na základě dokumentace řídit a poté optimalizovat jejich průběh.

Obrázek 4 - PDCA cyklus



Modelový příklad:

3.7.1 PLAN

Prvním krokem je plánování. To spočívá v identifikování problému (nutného k vyřešení) nebo příležitosti (vhodné ke zlepšení) na Ministerstvu a ve stanovení si cílů, jak jich dosáhnout. Důležité je v tomto případě přesné zhodnocení situace a pochopení podstaty toho, co je potřeba zlepšit nebo napravit. Stanovují se zde možná řešení situace a následně je vybrána ta, která jsou nejvhodnější k realizaci (ať již z důvodu ekonomického, technického, lidských zdrojů, ad.).

Příklad 1 (obecný):

Ministerstvo na základě interního jednání dospělo k názoru (příležitosti ke zlepšení), že je potřeba přistoupit k zavedení nového modulu a navrhlo úpravy vnitřního prostředí svého systému pro certifikaci senzorů. V rámci tohoto kroku odpovědné osoby pověřené zpracováním vytváří koncept, který zkoumá možné dopady (přínosy, rizika) do systému, a vliv této změny jak na Ministerstvo samotné, tak pro občany žádající o certifikaci. Za tímto účelem je zpracován akční plán, který rozvádí jednotlivé cíle, jež si Ministerstvo klade a chce je v rámci této změny splnit (tj. očekávané výsledky). Aby se na Ministerstvu podařilo naplnit vše požadované, je potřeba si stanovit kritéria a zjistit odpovědi na některé otázky. Mezi takové otázky může patřit například to, jaký bude pracovní postup od instalace modulu, přes testování až po zavedení do provozu, kdo bude modul spravovat, kdo zajišťovat podporu, jaké další zdroje jsou potřeba (finanční, lidské), zda bude nový modul účinný (např. zda dojde ke zlepšení úrovně produktivity lidí s novým modulem a úrovně výkonu Ministerstva při poskytování služeb) a efektivní (dojde k dosažení požadovaných cílů, resp. výstupů, stanovených v tomto kroku) nebo kolik času zabere samotná realizace.

Příklad 2 (§ 8 VKB):

V rámci auditu KB bylo zjištěno, že Ministerstvo neplní požadavky § 8 VKB – nemá stanovena pravidla pro dodavatele, nevede evidenci významných dodavatelů, neřídí rizika s nimi spojená a pravidelně nepřezkoumává smlouvy aj. Na základě této skutečnosti bylo rozhodnuto, že MKB připraví interní dokumentaci s veškerými postupy tak, aby došlo k naplnění všech bodů § 8 VKB. MKB rovněž připraví interní proces kontroly nově vydaných varování NÚKIB.

3.7.2 DO

Druhým krokem označeným jako „dělej“ se Ministerstvo snaží převést první krok do praxe. To zahrnuje implementaci navrhnutých řešení a sběr dat, ideálně v menším měřítku (testování na menším okruhu), aby bylo umožněno snadnější vyhodnocení funkčnosti i řešení případných zaznamenaných problémů.

Příklad 1 (obecný):

Jakmile si Ministerstvo stanovilo koncept a cíle, začínají práce na realizaci řešení. Ty mohou zahrnovat různé schůzky a konzultace. Oproti předchozímu kroku se však bude jednat již o schůzky nad konkrétní tvorbou procesu nebo služby (předchozí krok lze vnímat jako schůzky směřující k tvorbě analýzy proveditelnosti či konceptu Ministerstvem požadovaného řešení). V tomto kroku se již zaměřujeme na samotnou tvorbu postupů nebo funkcionalit modulu v systému či na jeho nákup a instalaci, a na aplikaci požadovaného řešení. Ministerstvo například přistoupí k zadání a vysoutěžení VZ, najímá další pracovníky schopné zrealizovat požadované cíle (instalaci, správu a údržbu modulu v systému). Za tímto účelem připravuje také školicí program/workshop pro zaměstnance na seznámení se s novým pracovním modulem a s tím souvisejícími novými možnostmi systému. Nakupuje licenci, uzavírá smluvní dohodu, testuje funkcionality modulu a jeho chování v prostředí systému a identifikuje pracovní role, které budou uvedené provádět, a metody, kterými se budou pracovníci řídit. Zároveň zjišťuje a zajišťuje vhodné úložiště dat pro vyhodnocení účinnosti zavedeného modulu.

Příklad 2 (§ 8 VKB):

Proces řízení dodavatelů byl v plném rozsahu dle § 8 VKB v rámci Ministerstva implementován. Jsou definována pravidla, Ministerstvo vede evidenci významných dodavatelů, má nastaven proces posuzování VZ a řízení rizik dodavatelů a pravidelně přezkoumává smlouvy. MKB

pravidelně u relevantních VZ zpracovává hodnocení rizik, bere přitom ohled na vydaná varování NÚKIB a navrhuje opatření do smluv.

3.7.3 CHECK

Ve třetím kroku jsou vyhodnocována obdržená, nashromážděná data a výsledné hodnoty porovnávány s plánovanými výsledky, rovněž se navrhuje další postup. Pakliže nedosahuje Ministerstvo plánovaných výsledků (navrhnuté řešení nezafungovalo), vrací se ke kroku č. 1 – PLAN. Pokud Ministerstvo vyhodnotí, že dosáhlo cíle jen do určité míry, zváží vylepšení stávajícího řešení a pokusí se o jeho další aplikaci. Pokud Ministerstvo dosáhlo vytyčených požadavků, pokračuje k dalšímu kroku. Současně prověřuje veškeré neočekávané vedlejší efekty spojené se zavedeným řešením.

Příklad 1 (obecný):

Ministerstvo kontroluje nově zavedené postupy související s modulem systému, jeho fungování, uživatelskou přívětivost, zda systém vše řádně zaznamenává a poskytuje očekávané informace a data, a to v očekávané kvantitě i kvalitě za určité stanovené období.

Příklad 2 (§ 8 VKB):

Na základě zpracovaného HR VZ byla ve smlouvě s dodavatelem XY navržena bezpečnostní opatření. Tato opatření byla přenesena do smlouvy s dodavatelem a Ministerstvo nyní chce provést kontrolu toho, zda dodavatel opatření plní. U dodavatele tak provede audit s cílem ověřit implementaci daných opatření.

3.7.4 ACT

V posledním čtvrtém kroku Ministerstvo kompletně zavádí navrhnuté řešení, které se stává jeho novým základním prvkem. Ministerstvo poté udržuje zavedené řešení a aplikuje v čase potřebné změny. Zatímco druhý krok představuje spíše implementaci řešení, čtvrtý krok představuje již jeho integraci a následné upravování. V případě nevyhovujícího stavu i opuštění tohoto řešení a v dalším cyklu Ministerstvo navrhne řešení nové.

Příklad 1 (obecný):

Ministerstvo na základě stanovených metrik identifikuje oblasti pro další možné zlepšení funkcionalit modulu sytému nebo při poskytování svých služeb. Takovým dalším krokem může být rozhodnutí o další investici do nových technologií, které pomohou zaměstnancům pracujícím s modulem nebo operátorům HotLine/ServiceDesk s rychlejším získáním přístupu k požadovaným informacím. Dalším krokem zde může být implementace nového kontrolního systému zajišťujícího sledování poruch modulu nebo telefonní linky a včasné oznámení nastalého problému příslušnému pracovišti.

Příklad 2 (§ 8 VKB):

V rámci auditu byly zjištěny nedostatky v implementaci opatření na straně dodavatele. Zároveň byly odhaleny nové skutečnosti, které vyžadují implementaci dodatečných opatření. S dodavatelem proběhne aktualizace smlouvy. MKB zároveň zpracuje nové hodnocení rizik, které bude zohledňovat skutečnosti nalezené v rámci auditu.

3.7.5 Nový cyklus PDCA

Jelikož se chce Ministerstvo stále zlepšovat, pokračuje dalším PDCA cyklem v plánování, dělání, kontrole a jednání za účelem zlepšení již aplikovaného modulu nebo poskytované služby a opět probíhá další kolo tohoto cyklu. Podstatou tohoto cyklu je vytvoření určitého standardu, který je

v dalších cyklech vylepšován, doplňován, pozměňován, a to vždy za účelem jeho přizpůsobení se aktuální situaci, pokroku či potřebě.

4 Další modelové příklady HR VZ

V této kapitole jsou blíže popsány další příklady hodnocení rizik, které se však svým postupem mírně liší od příkladu prostupujícího kapitolou 3. Jak už bylo však řečeno výše, uvedené postupy jsou spíše doporučujícího charakteru a nelze je rozhodně brát jako dogma, dle kterého je nutné se řídit.

Hodnocení rizik v případě, kdy žádné z varování není relevantní

V rámci hodnocení rizik se v tomto případě postupuje tak, že v procesu nejsou identifikovány dodatečné hrozby dle doporučení NÚKIB v kontextu jednotlivých varování. Povinná osoba vybírá pouze z relevantních zranitelností a hrozeb dle např. Přílohy č. 3 VKB. Reálně to znamená to, že každé riziko bude mít pouze jednu hodnotu, která bude platná pro všechny dodavatele, a nikoliv dvě, jako tomu bylo v případě identifikace dodatečných hrozeb dle varování.

Hodnocení rizik v případě nutnosti zohlednit varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací

V případě tohoto varování doporučuje NÚKIB zohlednit hrozbu *„nedodržení smluvního závazku ze strany dodavatele“*, která je typovou hrozbou č. 10 z Přílohy č. 3 VKB. Dle NÚKIB *„Osoby povinné dle ZKB musí hrozbu zohlednit v rámci své analýzy rizik, tedy zvýšit hodnotu typové hrozby **„nedodržení smluvního závazku ze strany dodavatele“** vůči dodavatelům, u kterých identifikují významný vztah k Ruské federaci, na hodnotu určenou varováním a příslušně přizpůsobit následné procesy řízení bezpečnosti informací“.*

Samotná povinnost zohlednění tedy vyplývá hlavně pro celkové hodnocení rizik dle § 5 a nikoliv pro proces HR VZ. Toto logicky vyplývá z časové posloupnosti, kdy se jednotlivé úkony hodnocení rizik, resp. HR VZ provádějí. Hodnocení rizik se provádí nad konkrétním podobou IS, tzn. zpracovatel dokáže objektivně identifikovat jednotlivá aktiva, která do systému vstupují, v tomto případě dodavatele, které mají vazby na Ruskou federaci, zatímco u HR VZ nemusí dopředu vědět, kdo bude dodávku zajišťovat.

V případě HR VZ se však hodnotí potenciální budoucí stav a zpracovatel tak jednoduše není schopný předem identifikovat, zda se do VZ takový dodavatel přihlásí nebo ne. Možným řešením je obsáhnutí tohoto varování v každém HR VZ. Každé zpracované HR VZ by tak automaticky muselo obsahovat hrozbu *„nedodržení smluvního závazku ze strany dodavatele“* s hodnotou Vysoká. Tento postup je analogický s hlavním modelovým příkladem a hrozbami z varování ze dne 17. prosince 2018.

Optimálnějším řešením je zapracování požadavku na dodavatele do zadávací dokumentace rovnou, bez nutnosti je zohledňovat v každém HR VZ. Výsledné riziko, resp. navržené bezpečnostní opatření (= požadavek na dodavatele) je totiž stále stejné. Tento požadavek může mít např. podobu čestného prohlášení dodavatele, kterým stvrdí, že nemá žádné vztahy s Ruskou federací, které by představovaly hrozbu dle tohoto varování.

Varování je pro tento postup podkladem s právní závazností. Zohlednění požadavků vyplývajících z varování v míře nezbytné nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěže.

Hodnocení rizik v případě nutnosti zohlednit varování TikTok

V souvislosti s aplikací TikTok a její instalací na mobilních zařízeních vyšlo varování, které upozorňuje na hrozbu spojenou s možností cílených kybernetických útoků na konkrétní osoby,

využití dat k vydírání cílených osob a narušení bezpečnosti České republiky. Smyslem tohoto varování je předejít negativním dopadům spojených s instalací a používáním aplikace TikTok na zařízeních přistupujících k informačním systémům základní služby, významným informačním systémům, informačním a komunikačním systémům kritické informační infrastruktury. Hrozba je hodnocena na úrovni Vysoká, tzn. že je pravděpodobná až velmi pravděpodobná. Každá dotčená organizace by toto měla při hodnocení rizik ve vztahu k uvedenému varování zohlednit.

Zohledněním v tomto smyslu bude zvýšení hodnoty příslušné identifikované hrozby u předmětného aktiva na odpovídající stupeň (tj. na hodnotu 3).

Povinné osoby provozující výše uvedené systémy mají také povinnost reagovat přijetím přiměřených **bezpečnostních opatření**. Navrhovaným bezpečnostním opatřením pak může být v prostředí organizace přistoupení k zákazu instalace aplikace na firemních zařízeních, případně přistoupit k oddělení pracovního a soukromého prostředí. U soukromých zařízení přistupujících do podnikových aplikací platí obdobné. Zákaz může být v takovém případě vynucován podnikovou bezpečnostní politikou, podmíněn pracovněprávním postihem nebo být přímo v zařízení automaticky zakázán (či zablokován). Doporučujícím opatřením pak může být například nepoužívat aplikaci TikTok ani na soukromých zařízeních. Důležité je zejména to, v jakém prostředí se nalézá osoba, která by tuto aplikaci využívala, a s jakými informacemi, daty nebo systémy přichází do styku při své pracovní činnosti.

Příklad:

Na základě výše uvedeného varování přistoupila organizace k následujícím krokům:

- Zohlednila varování ve svém hodnocení rizik, kdy navýšila hodnotu hrozby "*zneužití nebo neoprávněná modifikace údajů*“ na hodnotu Vysoká (3) u podpůrného aktiva „Mobilní telefon“.
- Zohlednila varování přijetím bezpečnostního opatření blokace aplikace TikTok na všech podnikových zařízeních s vydáním doporučení obdobného postupu i pro zařízení soukromá.
- Zadala požadavek, aby dodavatelé (v relevantních) nabídkách předložili čestné prohlášení, ze kterého bude jednoznačně vyplývat splnění podmínek stanovených ve varování.

5 Podpůrné materiály

V této kapitole jsou uvedeny podpůrné materiály a odkazy, které mohou povinným osobám a organizacím pomoci nejen při HR VZ, ale i v dalších oblastech KB.

Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti, včetně všech příloh a vzorových materiálů, je dostupný na webových stránkách NÚKIB, sekci „Vyhláška o kybernetické bezpečnosti":

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Problematika řízení dodavatelů a zadávání VZ v oblasti KB je více přiblížena v podpůrných materiálech:

- Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost,
- Požadavky na smlouvy s dodavateli,
- Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení a
- Metodika řízení dodavatelů.

Dostupných na webových stránkách NÚKIB:

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Podpůrný materiál Provozovatel informačního nebo komunikačního systému se zaměřuje na shrnutí nejdůležitějších bodů týkajících se praktického použití institutu provozovatele systému podle ZKB. Materiál se zaměřuje na popis definičních prvků provozovatele systému, jeho informování a následné povinnosti. Podpůrný materiál je dostupný na webových stránkách NÚKIB:

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Úřední deska obsahuje výčet vydaných opatření, včetně dalších materiálů přibližujících tuto problematiku, která je dostupná na webových stránkách NÚKIB:

https://www.nukib.cz/cs/uredni-deska/

Dalším odkazem, který může být nápomocen, je Infoservis, kde jsou vydávány hrozby a zranitelnosti z oblasti KB, který je dostupný na webových stránkách NÚKIB:

https://www.nukib.cz/cs/infoservis/hrozby/

V případě dalších dotazů k dané problematice se můžete obrátit na regulace@nukib.cz.

6 Q & A

Q1: Je možné na základě hodnocení rizik vyloučit účastníka výběrového řízení?

A1: Ano. Pokud hodnocení rizik splňuje požadavky VKB a výsledkem je, že nelze přijmout jiná bezpečnostní opatření než účastníka vyloučit.

Q2: Musí se HR VZ dle VKB provádět u všech dodavatelů v rámci všech VZ?

A2: Ne. Hodnocení rizik je obecně požadováno jen v souvislosti s významnými dodavateli. Ostatní dodavatelé jsou řízeni podle § 8 odst. 1 písm. e) VKB.

Q3: Jak poznám, kdo je významný dodavatel a kdo je obyčejný?

A3: Definici významného dodavatele a jeho charakteristiku lze nalézt v kapitole 2.

Q4: Co když není ustanoven Garant aktiva?

A4: Každé identifikované aktivum by mělo mít garanta, který byl jmenován v souladu s VKB. Pokud u daného aktiva jmenován není, měla by organizace garanta dodatečně určit a doplnit.

Q5: Musí se v rámci HR VZ zohlednit všechna varování NÚKIB?

A5: Ne. V rámci HR VZ se zohledňují pouze varování relevantní k dané VZ. Určení relevantnosti spolu např. s rozhodnutím o významném dodavateli je součástí posouzení VZ.

Q6: Jak poznám, že povaha zakázky vyžaduje přijmout bezpečnostní opatření?

A6: Odpověď lze nalézt v kapitole 2.1 dokumentu. Záleží na výstupu hodnocení rizik, které je u konkrétní zakázky prováděno. To, která opatření se nakonec rozhodne organizace zavést, záleží také na dalších okolnostech, jako jsou finanční zdroje, stanovený risk apetite a aktuální stav bezpečnostních opatření každé organizace.

Q7: Je možné použít i jiný způsob HR VZ než uvedený v tomto podpůrném materiálu?

A7: Ano, uvedený způsob je pouze ilustrační a jeden z možných řešení. Konkrétní řešení je nutné upravit individuálně dle potřeb organizace.

Q8: Jak fungují varování vydaná NÚKIB? Musí si sám zadavatel VZ zjistit, zda je pro dodavatele vydáno varování nebo NÚKIB vybrané organizace obesílá sám?

A8: Odpověď lze nalézt v kapitole 2.4. NÚKIB vydává varování pro konkrétní případy. Organizace musí tato varování sledovat a posléze, pokud se to organizace týká, na ně implementovat vhodné bezpečnostní opatření.

Q9: Na koho se obrátit, když si nejsem jistý, zda je dodavatel vhodný/bezpečný? Je nějaký rádce?

A9: Organizace si sama musí vyhodnotit vhodnost/bezpečnost dodavatele skrze konkrétní stanovené podmínky. Vhodným doplňkem může být Metodika řízení dodavatelů vydaná NÚKIB společně s tímto podpůrným materiálem nebo dokument Požadavky na smlouvy s dodavateli ze dne 22. prosince 2022, viz kapitola 5.

Q10: V jakých případech může dojít k přenesení povinnosti kontroly dodavatelů na třetí stranu?

A10: Toto je vhodné v případech, kdy organizace nemá zdroje či prostředky pro vypořádání se s rizikem, anebo není ochotna se s rizikem vypořádat vlastní cestou. Přenesením rizika se organizace snaží vyhnout tomu, že by riziko stále přetrvávalo, a zároveň upřednostní, aby toto riziko pro ni mitigoval jiný dodavatel.

Q11: Kdo je odpovědný za celý proces hodnocení VZ?

A11: Na celém procesu HR VZ spolupracuje několik osob a dle modelové RACI matice je odpovědný za celý proces MKB. Jedná se jen o modelový příklad a v každé organizaci může být za tento proces odpovědná jiná osoba dle specifických potřeb a personálních možností dané organizace.

Q12: Je možno využít stávající metodiky pro identifikaci a hodnocení aktiv a rizik pro vytvoření metodiky pro HR VZ, nebo musí být vytvořena nová odlišná metodika?

A12: Je možno využít stávající metodiky. Není potřeba vytvářet nové a je možno již vytvořené stupnice využít pro metodiku HR VZ a specifické potřeby organizace. Tento krok ušetří čas a zajistí, že bude metodika HR VZ kompatibilní s hlavní metodikou pro identifikaci a hodnocení aktiv a rizik.

Q13: Jsou stanoveny lhůty pro provedení HR VZ? Pokud ano, kde?

A13: Lhůty pro provedení celého procesu HR VZ (posouzení dokumentace s výstupem, analýza) nejsou přímo stanoveny. V rámci dobré praxe může být stanoveno např. pět dní na posouzení dokumentace spojené s rozhodnutím o dalším postupu a dalších pět dní na provedení analýzy, pokud k ní bude přistoupeno. Organizace si toto stanovuje samostatně. Lhůta by měla být taková, aby byla časově únosná a zároveň aby reflektovala potřeby organizace.

Q14: Co dělat v případě, když NÚKIB vydá varování pro našeho dodavatele?

A14: V takovém případě je nutné provést nové hodnocení rizik, popř. aktualizovat již provedené, a zohlednit v něm příslušné varování a přijmout adekvátní bezpečnostní opatření. Dále je potřeba zjistit, kolik zakázek je s tímto dodavatelem sjednáno, a přijmout příslušné bezpečnostní opatření.

Q15: Jak provést prokazatelné informování dodavatele o tom, že je významný dodavatel?

A15: Takový dodavatel musí být písemně vyrozuměn o této skutečnostisvé roli a v rámci smluvního vztahu musí být ošetřeny na základě toho splňovat relevantní požadavky vyplývající z Přílohy č. 7 VKB (viz kapitola 2.3). Prokazatelné informování musí obsahovat náležitosti dle § 8 odst. 3 VKB.

7 Seznam obrázků a tabulek

7.1 Obrázky

7.2 Tabulky

8 P1 – Modelová RACI matice

↓ Činnosti / Pracovní role →		Specialista/Referent VZ	Garant VZ	Právník	MKB	ARCHKB	MKBJR	Zaměstnanec odpovědný za smluvní vztah
Příprava	Zaslání dokumentace VZ na posouzení	**A**	**I**					**I**
Posouzení	Analýza dokumentace, posouzení VZ				**A**	**C**	**R**	
	Evidence posouzení VZ				**A**		**R**	
	Zpracování a zaslání výstupní dokumentace	**I**	**I**	**I**	**A**		**R**	**I**
HR VZ	Zpracování HR VZ		**C**		**A**		**R**	
	Návrh bezpečnostních opatření				**A**	**C**	**R**	
	Zpracování a zaslání výstupní dokumentace	**I**	**I**	**I**	**A**		**R**	**I**
Dokončení	Zapracování výstupů hodnocení rizik do zadávací dokumentace		**C**	**A**	**I**	**I**	**I**	**C**

Legenda k RACI matici:

Zkratka	Popis
R	Responsible (ti, kteří práci/úkol vykonávají)
A	Accountable (ti, kteří zodpovídají za celkové splnění úkolu)
C	Consulted (ti, kteří by se k danému mohli vyjádřit a být nápomocni s jeho řešením)
I	Informed (ti, kteří mají být informováni)

9 P2 – Modelová evidence HR VZ

V každé organizaci je vhodné vést k příslušným zakázkám i jejich evidenci. Tento typ evidence by měl být řádně uchováván např. v podnikovém dokumentačním systému (spisové službě), také někdy označovaném zkratkou DMS (Document Management System). Tyto systémy se obvykle v podniku zavádějí pro pořízení, tvorbu, ukládání, sdílení a oběh dokumentů, až po jejich archivaci a skartaci. Organizace může vést evidenci také v jiné odpovídající službě, která bude poskytovat dostatečné zabezpečení. Je čistě na každé organizaci, pro jakou evidenci se rozhodne. Níže uvedená tabulka je pouze vzorová. Smyslem této evidence je vytvořit záznamový arch, ze kterého bude patrné, jaké zakázky byly posuzovány, kdy byly posuzovány, zda se u zakázky vyskytuje významný dodavatel a jestli byla provedena analýza rizik. Vhodné je arch doplnit také o identifikační číslo zakázky. Další informace lze brát jako doplňkové a je vhodné je doplnit dle potřeb organizace.

Zaměstnanec odpovědný za smluvní vztah	Měsíc	Rok	Název VZ	Identifikátor VZ	Organizační jednotka	Významný dodavatel	Provedení AR
Martin Novotný	01	2024	Nákup licencí	MCS/SPZN/2023-01-OLI	Oddělní LINUX	**ANO**	**ANO**
Jan Novák	01	2024	Přesun technologií do prostředí MS cloud	MCS/SPZN/2023-01-OSMST	Oddělení správy MS technologií	**NE**	**NE**
Tereza Černá	03	2024	Nákup diskových polí	MCS/SPZN/2023-03-OSKT	Oddělení správy komunikačních technologií	**ANO**	**ANO**
Tomáš Fiala	04	2024	HW a SW podpora produktů SAP	MCS/SPZN/2023-04-OEKO	Ekonomické oddělení	**NE**	**NE**
Renata Malá	05	2024	Instalace EPS, EZS a PZTS v objektu	MCS/SPZN/2023-05-OOST	Oddělení ostrahy	**NE**	**NE**

Legenda k Modelové evidenci HR VZ:

Zkratka	Popis
Zaměstnanec odpovědný za smluvní vztah	Jedná se o osobu, která je zodpovědná za uzavření smluvní rámcové dohody s dodavatelem.
Měsíc/Rok	Měsíc a rok, ve kterém se posouzení VZ provedlo.
Identifikátor VZ	Interní podnikové označení veřejné zakázky.
Organizační jednotka	Jedná se o úsek/odbor nebo oddělení, pro které je VZ určena, a bude v přímé komunikaci s dodavatelem.
Významný dodavatel	Informace, zda bylo na základě posouzení vyhodnoceno, že se pro podnik jedná o významného dodavatele, jak jej specifikuje VKB.
Provedení AR	Informace, zda bylo na základě posouzení přistoupeno k potřebě provedení analýzy rizik.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
4. září 2023	1.0	NÚKIB, SCPSS	Vytvoření dokumentu

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP: RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP: AMBER**	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
Oranžová **TLP: AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
Zelená **TLP: GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP: CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.