Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Návrh bezpečnostního hodnocení dodavatele

Bakalářská práce

Autor: Mgr. Lenka Michalcová
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové březen 2020

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne 21.3.2020 Lenka Michalcová

Poděkování:
Děkuji vedoucímu bakalářské práce Mgr. Josefovi Horálek, Ph.D. za metodické vedení práce, jakož i rady při jejím zpracování. Dále děkuji své rodině a partnerovi za podporu v průběhu studia a po dobu přípravy této práce.

Anotace

Předkládaná bakalářská práce se zabývá bezpečnostním hodnocením dodavatele v kontextu platné legislativy v oblasti kybernetické bezpečnosti. Cílem práce je navržení metodiky hodnocení dodavatele a stanovení okruhu a významu bezpečnostních opatření, jejichž zavedení potenciálním dodatelem zajistí zákonem požadovanou úroveň zabezpečení informačního a komunikačního systému.

Autorka nejprve předkládá teoretickou analýzu relevantního legislativního a normativního rámce doprovozenou vysvětlením základních konceptů v oblasti řízení rizik. Jelikož bakalářská práce usiluje o navržení metodiky vyhovující požadavků právní úpravy v České republice, zaměřuje se tato část především na české právní předpisy z oblasti soukromého i veřejného práva. Legislativní přehled je doplněn komparací a analýzou normativního rámce, zejména norem ISO/IEC řady 2700x, jež jsou v této oblasti mezinárodně akceptovaným standardem.

Následně je v bakalářské práci předkládán popis hodnocení dodavatele a určení okruhu bezpečnostních opatření, jejichž implementaci je třeba od konkrétního dodavatele vyžadovat. Autorka podobně vysvětluje, jak jednotlivé kroky procesu, jakož i jejich význam. Na závěr bakalářské práce je pak předkládán konkrétní příklad využití v této práci navržené metodiky hodnocení dodavatele a určení bezpečnostních opatření.

Klíčová slova: dodavatel, bezpečnostní opatření, kritická infrastruktura

Annotation

The presented bachelor thesis addresses supplier security evaluation in the context of the current legislation in the field of cyber security. The goal of the thesis is to propose a methodology for supplier evaluation and determination of the scope and importance of security measures through implementation of which the security level of the information and communication system required by law shall be secured.

First, the author presents theoretical analysis of the relevant legislative and normative framework accompanied by an explanation of the core principles of the risk management field. As the thesis strives to propose a methodology compliant with the Czech legal regulation, this part is primarily concerned with the Czech law, from both, private and public, area. The legislative overview is completed by a comparison and analysis of the normative framework, especially ISO/IEC standards, series 2700x, which is considered an internationally accepted industry standard.

Subsequently, a description of the supplier evaluation and determination of the scope of the security measure, which are to be required from a particular supplier, is presented in the thesis. The author explains in detail, both the individual steps of the process and their meaning. In conclusion of the bachelor thesis is presented an example of application of the methodology proposed in the thesis to evaluate a supplier and to determine security measures.

Key words: supplier, security measures, critical infrastructure

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

„*Většina (ne-li všechny) organizace po celém světě, bez ohledu na jejich velikost či obor činnosti, mají vztahy s dodateli různých druhů, jež jim dodávají zboží nebo služby.*“ [1, s. v] K vytvoření a/nebo udržování dodavatelského vztahu organizace zpravidla přistupuje v případě, že (a) soustředí své interní zdroje na stěžejní činnosti a zapojením dodavatele cílí na snížení nákladů, (b) pro dosažení určitého cíle potřebuje krátkodobě získat určité či vysoce specializované kompetence, jimiž daná organizace standardně nedisponuje, (c) má potřebu čerpat službu, jež je běžně či okamžitě dostupná (př. elektrická energie nebo telekomunikační služby), (d) má zájem rozšířit svou působnost do nových geografických oblastí, (e) v zájmu zvýšení efektivity naplňování cílů organizace rozhodne o nabytí nového či nahrazení stávajícího vybavení či služeb [1, s. 4]. Motivace individuální organizace může být samozřejmě založena na libovolné kombinaci výše uvedených cílů. Stejně tak může organizace k naplnění konkrétního cíle využít více než jednoho dodavatele a naopak, jeden strategický dodavatel může organizaci asistovat v dosažení více než jednoho cíle.

Zapojením dodavatele ale odběratelská organizace ztrácí přímou kontrolu nad výrobním procesem či procesem poskytování služby a je tedy nucena důvěřovat kontrole vykonávané jí vybraným dodavatelem. Dodavatel dále může mít přímý či nepřímý přístup k informacím a informačním a komunikačním systémům odběratelské organizace. Zapojení dodavatele tedy nevyhnutelně představuje riziko, které organizace musí vyhodnotit a řídit. Toto riziko potenciálně ohrožuje nejen schopnost odběratelské organizace vykonávat svou provozní činnost, ale také dostát svým zákonným povinnostem v oblasti ochrany informací. Z tohoto důvodu je proces výběru dodavatele v řadě případů omezen zákonnými pravidly, jež je třeba v průběhu procesu respektovat.

Zároveň nelze opomenout skutečnost, že v praxi dodavatelské organizace často využívají další dodavatele (z pohledu konečné odběratelské organizace subdodavatele). Skupina subdodavatelů podílejících se na plnění dodavatele, jenž je v přímém smluvním vztahu s konečnou odběratelskou organizací, vytváří tzv.

dodavatelský řetězec. Riziko popsané v předchozím odstavci prostupuje celý dodavatelský řetězec a pochopitelně narůstá s rostoucí komplexitou dodavatelského řetězce.

Oblast kritické informační infastruktury zahrnuje služby (př. zásobování elektřinou, tepelnými energiemi, provoz vodního hospodářství, dopravní sítě či fungování státního aparátu), které jsou stěžejní pro řádné fungování společnosti a ekonomiky. Z toho důvodu je na její ochranu kladen zvýšený důraz, mj. formou právní regulace. Riziko, jež pro kritickou informační infrastrukturu může představovat dodavatelský řetězec, bylo široce medializováno po vydání *„Varování NÚKIB před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation“* [43]. Vydání tohoto varování bylo motivováno *“právním a politickým prostředím Čínské lidové republiky (‘ČLR’)”* [43, s.1], jejímž zákonům tyto společnosti podléhají a které jim ukládají povinnost součinnosti *„při naplňování zájmů ČLR, včetně podílu na zpravodajských aktivitách aj.“* [43, s.1] Z tohoto důvodu NÚKIB vyhodnotil, že používání technických nebo programových prostředků dodávaných těmito společnostmi může představovat bezpečnostní riziko pro Českou republiku a její zájmy.

V kontextu této bakalářské práce je bezpečnostní hodnocení dodavatele pojímáno jako proces, v jehož rámci je stanovena významnost dodavatele a je určen rozsah bezpečnostních opatření, jejichž implementace na straně dodavatele je nezbytná k zajištění bezpečnosti informačních a komunikačních systémů provozovaných povinnými osobami. Nejedná se tedy o statické hodnocení dodavatele, jež by kvalifikovalo jeho obecnou bezpečnostní způsobilosti poskytovat povinné osobě jakékoli služby. Ačkoli by statické hodnocení bylo jistě zajímavou sondou do bezpečnostní připravenosti dodavatelského řetězce, autorka této bakalářské práce věří, že metodika určení rozsahu bezpečnostních opatření ve vztahu ke konkrétní dodávce má vyšší praktický přínos.

Při hodnocení rizika zapojení konkrétního dodavatele odběratelské organizace zpravidla zkoumají zavedení určitých procesů a implementaci konkrétních opatření

dodavatelem. Cílem hodnocení je ověřit úroveň zabezpečení a kvalitu kontroly vykonávané potenciálním dodavatelem nad jím spravovanými aktivy využívanými při poskytování plnění odběratelské organizaci.

V praxi jsou k tomuto účelu obvykle využívány rozsáhlé dotazníky analyzující rozličné aspekty zabezpečení jednotlivých aktiv. Aniž je však před přípravou těchto dotazníků či při jejich vyhodnocení provedena analýza konkrétních hrozeb vznikajících zapojením daného dodavatele s daným předmětem činnosti, hrozí zkreslení výsledného hodnocení. V důsledku toho, dodavatel, který postrádá podstatná bezpečnostní opatření v oblastech, která jsou z hlediska jeho předmětu plnění pro odběratelskou organizaci klíčová, ale zavedl nadstandardní bezpečnostní opatření v jiných, může být vyhodnocen jako důvěryhodný (v bezpečnostním smyslu).

Zároveň je vhodné zmínit, že řada formulářů určených k hodnocení dodavatelů v praxi využívaných často čítá desítky, ne-li stovky kolonek, na jejichž vyplnění i vyhodnocení obvykle participují zodpovědné osoby napříč organizační strukturou odběratelské i dodavatelské organizace. Jedná se tedy o administrativně náročný proces, jehož důsledné provedení vyžaduje kombinaci technických a v omezeném rozsahu též právních znalostí.

Bakalářská práce je členěna na tři základní části. První část, teoreticky zaměřená část, je označena „legislativní a normativní rámec“. V této části je vymezena relevantní právní i normativní úprava vztahující se k předmětu bakalářské práce a jsou vysvětleny jejich vzájemné vazby, je vymezen okruh povinných osob dle ZKB, a též je předložen výklad stěžejních pojmů v oblasti řízení rizika. V druhé části je předkládán teoretický popis procesu hodnocení dodavatele a stanovení bezpečnostních opatření. Ve třetí části je pak použití navržené metodiky demonstrováno na konkrétním příkladu.

2 Cíl práce

Jak je nastíněno v úvodu bakalářské práce, řízení rizika souvisejícího se zapojením dodavatele je komplexní disciplína. Cílem této bakalářské práce je navržení metodiky hodnocení dodatelů z hlediska naplnění požadavků ZKB a VKB. Cílem předkládané metodiky je hodnocení významnosti dodavatele a stanovení okruhu a významu bezpečnostních opatření, jejichž zavedení potenciálním dodatelem zajistí zákonem požadovanou úroveň zabezpečení informačního a komunikačního systému.

Navržená metodika klade důraz na propojení mezi konkrétní hrozbou a relevantním opatřením. Po provedení hodnocení dle navržené metodiky by tedy povinná osoba měla být schopna informovaně rozhodnout, zda v oblastech, jež jsou z hlediska plnění dodavatele pro odběratelskou organizaci klíčové, poskytuje dodavatel dostatečné garance bezpečnosti informací.

Bakalářská práce se tedy omezuje na kvalitativní hodnocení dodatele z hlediska jím zajišťované úrovně bezpečnosti informací. Metodika je navržena se zřetelem na regulatorní požadavky ZKB a VKB, přesto ji však mohou jako vodítko využít i subjekty, jež se nekvalifikují jako povinné orgány a osoby ve smyslu §3 ZKB. Jelikož ale proces hodnocení dodavatelů lze považovat za nadstavbový proces, je předpokladem aplikace metodiky těmito subjekty existenci dalších standardních procesů v odběratelské organizaci, zejm. systému řízení bezpečnosti informací a řízení aktiv.

Hodnocení schopnosti dodavatele z hlediska jeho schopnosti splnit závazek či kvality jeho plnění je v metodice zohledněno pouze v rozsahu, v jakém porušení povinnosti dodavatele plnit řádně a včas je schopno narušit bezpečnost informací.

S ohledem na rozsah bakalářské práce, v bakalářské práci nejsou řešeny speciální povinnosti ukládané poskytovateli digitální služby dle prováděcího nařízení Komise (EU) [11].

Metodika zcela zanedbává (a) obchodní aspekty výběru dodavatele jako jsou cena, platební podmínky, předpokládaný termín dodání, velikost společnosti dodavatele, reference dodavatele a/nebo organizační změny v odběratelské organizaci nezbytné při zapojení dodavatele, (b) právní aspekty jako jsou rozhodné právo dodavatelské smlouvy, pravidla řešení sporů vzniklých na základě či v souvislosti s dodavatelskou smlouvou, záruku za jakost plnění a/nebo rozsah odpovědnosti dodavatele.

Metodika navržená v této bakalářské práci dále nezohledňuje speciální požadavky na zabezpečení utajovaných informací stanovených zákonem č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.

3 Metodika zpracování

3.1 Použité zdroje

Podkladem pro zpracování této bakalářské práce byla analýza relevantních právních předpisů, oborových norem, doprovodné komentářové literatury, odborných knih a domácích i zahraničních zdrojů v oblasti kybernetické bezpečnosti.

Vzhledem k tomu, že metodika hodnocení dodavatelů, která je těžištěm práce, je navržena v souladu se ZKB, je legislativní a normativní rámec předmětu této bakalářské práce vymezen se zřetelem k české právní úpravě. Podstatným zdrojem informací při zpracování bakalářské práce byly zejména metodické materiály publikované NÚKIB.

Zahraniční zdroje byly využity zejména při přípravě samotné metodiky. Nejvýznamnějším zdrojem byly mezinárodní normy ISO vydávané Mezinárodní organizací pro normalizaci.

3.2 *Přehled existujících nástrojů pro hodnocení dodavatelů*

V rámci zpracování bakalářské práce byla provedena rešerše a analýza aktuálně dostupných nástrojů pro hodnocení dodavatelů.

V době zpracování této bakalářské práce není dostupný žádný nástroj, jenž by byl určen pro hodnocení potenciálních dodavatelů povinnými osobami a orgány dle §3 ZKB. V důsledku této situace jsou k hodnocení analogicky používány dostupné nástroje. V rámci rešerše byly identifikovány dva základní, níže popsané, nástroje využitelné k analogické aplikace. Bohužel oba trpí zásadními, níže popsanými, nedostatky, které jejich aplikaci na hodnocení dodavatele podstatně komplikují.

3.2.1 Pomůcka k auditu bezpečnostních opatření podle VKB

Pomůcka k auditu bezpečnostních opatření podle VKB poskytuje přehled povinností, které ZKB ukládá jednotlivým povinným subjektům [3, Úvodní list]. Jednotlivé povinnosti jsou prezentovány formou kontrolního seznamu. Dokument

má povinným subjektům umožnit jednodušší ověření souladu jimi zavedených interních procesů se zákonnými povinnostmi. Bohužel spíše než praktickým vodítkem pro implementaci povinností, je dokument přehledem toho, které zákonné povinnosti dopadají na konkrétní povinný subjekt. Dokument je zároveň primárně určený pro interní sebehodnocení povinných subjektů, nikoli pro hodnocení dodavatelů. Jelikož užití tohoto dokumentu jako východiska pro přípravu interní metodiky hodnocení dodavatelů se nezdá být příliš vhodné, nevychází z něj ani návrh metodiky v této bakalářské práci.

3.2.2 Nástroje pro hodnocení souladu potenciálního dodavatele s ISO standardy

Na trhu je dostupná celá řada jak komerčních, tak open-source, více či méně rozsáhlých nástrojů pro hodnocení souladu dodavatele s mezinárodními standardy ISO. Z hlediska hodnocení zabezpečení informací potenciálním dodavatelem je široce používáno zejm. ISO 27002:2013, jehož českou jazykovou mutací je ČSN ISO/IEC 27002 [4].

Příkladem se v této bakalářské práci uvádí dotazníkový nástroj vytvořený a komerčně nabízený The Santa Fe Group [5]. Výhodou tohoto nástroje je vysoká úroveň personalizace, kdy uživatel může dotazníky pro jednotlivé dodavatele personalizovat výběrem otázek z databáze, jež je v nástroji obsažena. V nástroji jsou implementovány pokročilé makro funkce, umožňující automatické vyhodnocení formuláře dle uživatelem definovaných správných odpovědí. Jednotlivé otázky zároveň odkazují referenci na konkrétní článek ISO/IEC 27002:2013 (a též devět dalších standardů a předpisů), díky čemuž je uživatel schopen získat přehled o zabezpečení v jednotlivých oblastech. Hlavní nevýhoda tohoto nástroje pramení ze skutečnosti, že je vytvořen společností se sídlem ve Spojených státech amerických a není tedy plně přizpůsoben evropské legislativě. Nástroj pochopitelně neobsahuje mapování jednotlivých otázek na ustanovení ZKB, ale též např. v oblasti ochrany soukromí nástroj odkazuje na zákon státu Kalifornie o ochraně soukromí

spotřebitele, nikoli na jednotnou evropskou úpravu[1] [5, informace prezentované ve videu umístěném na stránce]. Adaptace nástroje pro jiný právní systém činí jeho použití povinnými subjekty dle ZKB obtížným, až téměř rizikovým. Neboť však autorka této bakalářské práce považuje nástroj za vysoce kvalitně zpracovaný, jeho koncept ji inspiroval při tvorbě metodiky v této práci předkládané.

3.3 Tvorby metodiky hodnocení dodavatelů

Navržená metodika klade důraz na propojení rizika a vhodného opatření. V této bakalářské práci navržená metodika hodnocení dodavatelů je vystavěna na hypotéze, že kvalifikované posouzení úrovně zabezpečení potenciálním dodavatelem je možné a efektivní pouze pokud se hodnocení soustředí na konkrétní podpůrná aktiva, jež budou dodavatelem využívána při plnění pro odběratelskou společnost a odhlédne od těch aktiv, jež za tímto účelem využívána nejsou. Z tohoto důvodu byla metodika vytvářena ve dvou krocích.

Prvním krokem tvorby metodiky bylo navržení mechanismu hodnocení potenciálního rizika vznikajícího zapojením zvažovaného dodavatele, tj. s ohledem na předmět činnosti dodavatele. V návrhu postupu hodnocení rizika metodika vychází z pravidel hodnocení rizik uvedených v příloze č. 2 VKB. Potenciální hrozby a s nimi související zranitelnosti jsou navrženy na základě jejich demonstrativního výčtu uvedeného v příloze č. 3 VKB s přihlédnutím k příkladům uvedeným v příloze C normy ČSN ISO/IEC 27005:2013 [8]. Klasifikace dopadů je navržena podpůrného materiálu pro hodnocení dopadů vydaného NÚKIB [9].

Začlenění hodnocení rizik do metodiky hodnocení dodavatelů zajišťuje, že odběratelská organizace bude schopna provést informované rozhodnutí o úrovni zabezpečení informací potenciálním dodavatelem v oblastech relevantních pro předmět plnění dodavatele. V případě zapojení významného dodavatele je tento

[1] K této skutečnosti se vyjadřuje i ministerstvo spravedlnosti státu Kalifornie, když v přehledu základních údajů jím vypracovaném k tomuto zákonu uvádí, že *„Zákon na ochranu soukromí spotřebitele a Obecné nařízení o ochraně osobních údajů jsou různé právní rámce mající různé předměty, definice a požadavky.“* [6]

postup též zákonnou povinností odběratelské organizace jako povinné osoby dle §8 odst. 2 VKB.

V druhém kroku byly potenciální hrozby identifikované v prvním kroku propojeny s opatřeními vyžadovanými ZKB ve spojení s VKB v rámci tzv. mapovací tabulky. Mapovací tabulku autorka této práce navrhla na základě ZKB.

Propojení hodnocení rizik s konkrétními opatřeními prostřednictvím mapovací tabulky je považováno za nezbytné pro vymezení okruhu relevantních bezpečnostních opatření. Pouze v případě, že odběratelská organizace má informaci o tom, jaká opatření cílí na konkrétní hrozby, je schopna hodnotit, zda opatření implementovaná potenciálním dodavatelem jsou dostatečná či je zabezpečení v konkrétních oblastech třeba posílit.

3.4 Výzkumné otázky

V rámci bakalářské práce jsou řešeny následující výzkumné otázky:

a) Jaké hrozby jsou zpravidla spojeny se zapojením dodavatele povinnou osobou dle ZKB?
b) Jaký je význam jednotlivých opatření předpokládaných VKB pro předcházení realizaci hrozeb dle písm. a) či snížení jejich dopadu?
c) Je možné zjednodušit proces stanovení rozsahu bezpečnostních opatření, jejichž implementace je od dodavatele vyžadována, aniž by byla kompromitována kvalita tohoto posouzení?

4 Legislativní a normativní rámec

Jak je zmíněno v úvodu této bakalářské práce, v procesu rozhodnutí o zapojení a výběru konkrétního dodavatele je odběratelská organizace často vázána omezujícími zákonnými ustanoveními.

V této části bakalářské práce je předkládán přehled právní úpravy i oborových standardů regulující hodnocení dodavatelů a výklad základních konceptů, jež musí být v tomto procesu respektovány či jsou v praxi využívány.

4.1 Právní rámec povinnosti hodnocení dodavatele

Právní úpravu kladoucí určité kvalitativní nároky na výběr dodavatele lze nalézt v řadě oblastí českého právního řádu. Účel těmito ustanoveními sledovaný je však různý a liší se tedy i jejich relevance z hlediska předmětu této bakalářské práce. Tato část bakalářské práce přibližuje právní úpravu v relevantních právních předpisech.

4.1.1 Občanský zákoník a zákon o obchodních korporacích

OZ, stěžejní předpis soukromého práva [13, s. 39], v §159 zakotvuje povinnost členů voleného[2] orgánu PO jednat s péčí řádného hospodáře. Vzhledem k systematickému zařazení ustanovení v Obecné části OZ, tato povinnost dopadá na všechny druhy soukromoprávních[3] právnických osob. Ve vztahu k obchodním korporacím je pak dále konkretizována v §51 ZOK. Základním elementem péče řádného hospodáře je, spolu s povinností loajality, „*povinnost užívat při výkonu funkce potřebné znalosti a pečlivost*“ [15, s. 8].

Povinnosti péče řádného hospodáře nelze limitovat na povinnost člena voleného orgánu jednat v souladu s právními předpisy, vnitřními předpisy PO a příp. též řádně vydanými usnesením nejvyššího orgánu PO. Povinnost péče řádného hospodáře zahrnuje, z hlediska předmětu této bakalářské práce významnou, povinnost jednat s odbornou péčí. V odborné literatuře nepanuje shoda ohledně

[2] Použitá formulace je však pouze legislativním zkratkou, neboť dle OZ [12, § 152(2)] je “členem voleného orgánu” fyzická osoba, “*která je do funkce volena, jmenována či jinak povolána”.*
[3] Aplikace konceptu péče řádného hospodáře na veřejnoprávní korporace je sporná [15, s.11].

úrovně odbornosti, jíž musí člen voleného orgánu disponovat pro řádný výkon své funkce. Autorka této bakalářské práce se klaní k názoru artikulovaného Dědič a kol. v kontextu zrušeného obchodního zákoníku [16], že odbornost člena voleného orgánu *„nemusí dosahovat úrovně znalostí odborníka daného oboru, avšak musí být odborníkem na řízení korporací, požadavek seznamovat se s novými poznatky v oboru řízení a správy společností a uplatňovat je v činnosti společnosti a při rozhodování se rozhodovat se znalostí věci a v případě, že člen představenstva nemá potřebné odborné znalosti, povinnost zajistit posouzení daného případu osobou, která potřebné odborné znalosti má."* [17, s. 2417]

Zatímco literatura a judikatura vydaná za platnosti zrušeného obchodního zákoníku [16] dovozovala, že člen voleného orgánu je povinen o majetek PO pečovat, jako by se jednalo o jeho vlastní majetek, platný OZ stanoví standard přísnější. Člen voleného orgánu je dle platné právní úpravy při správě majetku PO vázán povinnostmi řádné správy, je *„povinen chránit jej před ztrátou, poškozením či jiným znehodnocením, ale současně i zvažovat a přijmout riziko spojené s podnikatelskou činností, která umožní jeho zhodnocování a rozmnožování majetku společnosti"* [15, s. 12], a to bez ohledu na to, jak by nakládal se svým majetkem [15].

V případě porušení povinnosti člena voleného orgánu vykonávat funkci s péčí řádného hospodáře, byť z nedbalosti, nese tento soukromoprávní odpovědnost k náhradě způsobené škody vůči dané PO. Vzniká též ručitelský závazek tohoto člena voleného orgánu vůči věřitelům PO [12, §159(3)] a může též dojít k naplnění skutkové podstaty trestného činu porušení povinnosti při správě cizího majetku (z nedbalosti) [18, §220 a §221].

Jak bylo již výše uvedeno, povinnost péče řádného hospodáře dopadá pouze na členy volených orgánů soukromoprávních PO. V perspektivě výběru dodavatele je tedy statutární orgán vázán přísnějším standardem než samostatně podnikající fyzická osoba. Tento dvojí standard je dán účelem zákonného ustanovení o povinnosti péče řádného hospodáře, jímž je ochrana majetku dané PO.

Rozhodne-li se samostatně podnikající fyzická osoba pro zapojení dodavatele, není v tomto rozhodnutí ani výběru dodavatele zákonem nikterak omezována. Naproti tomu, člen voleného orgánu PO je povinen při rozhodnutí o zapojení dodavatele i jeho výběru vždy postupovat *„s nezbytnou loajalitou i s potřebnými znalostmi a pečlivostí“* [12, §159 (1)]. V případě, že znalostmi nezbytnými pro rozhodnutí nedisponuje, je povinen si je opatřit. Za znalosti nezbytné k informovanému rozhodnutí o zapojení potenciálního dodavatele lze nepochybně považovat i informaci o úrovni zabezpečení informací tímto dodavatelem. V zájmu naplnění zákonné povinnosti péče řádného hospodáře lze tedy členům volených orgánů doporučit zavedení procesu hodnocení dodavatele, jenž může svou podstatou vycházet z metodiky předkládané v této bakalářské práci.

S ohledem na zaměření toto bakalářské práce na hodnocení dodavatelů v kontextu ZKB, nebude regulace OZ dále rozebírána.

4.1.2 Zákon o kybernetické bezpečnosti

4.1.2.1 Obecně k ZKB

Před přijetím ZKB český právní řád postrádal komplexní úpravu problematiky kybernetické bezpečnosti. Před přijetím ZKB bylo *„zajištění kybernetické bezpečnosti otázkou dobrovolné koordinace dohledových a ochranných činností mezi jednotlivými správci informačních systémů nebo poskytovateli služeb elektronických komunikací, resp. mezi subjekty zajišťujícími sítě elektronických komunikací.“* [19, s. 34] Za tohoto stavu nejen, že nedostatečná proaktivita či neochota správce informačního systému, poskytovatele služeb či subjektu zajišťujícího síť byla způsobilá poskytnout příležitost k rozsáhlému kybernetickému útoku, ale zároveň neexistovaly efektivní nástroje, kterými by bylo možné na něj reagovat [19, s. 34].

Účelem ZKB, jak byl deklarován v důvodové zprávě k němu zpracované, je zabezpečení informační společnosti proti nahodilým i úmyslným bezpečnostním incidentům. Cílem zákona naopak nebyla regulace jejího obsahového fungování. [19, s. 32].

ZKB vstoupil v platnost dne 29. srpna 2014 a dne 1.1.2015 nabyl účinnosti. V souladu se svým cílem deklarovaným v důvodové zprávě ZKB stanovil *„minimální požadavky na standardní zabezpečení kritické informační infrastruktury a významných informačních systémů“* [19, s. 32] a *„zajistil vládnímu dohledovému pracovišti v reálném čase přehled o kybernetické bezpečnostní situaci v kritické infrastruktuře a ve významných informačních systémech.“* [19, s. 32]

Od doby jeho přijetí podobu ZKB ovlivnily dvě významné novelizace. První novelizací účinnou od 1.8.2017 [20] byly mezi povinné osoby dle tohoto zákona zahrnuti provozovatelé informačních systémů a upraveny některé sankce. Druhou novelizací účinnou od 1.3.2017 [21] byla provedena transpozice tzv. Směrnice NIS [22] a zřízen NÚKIB jako *“ústřední správní úřad pro oblast kybernetické bezpečnosti”* [10, §21a].

Oproti OZ, ZKB obsahuje veřejnoprávní úpravu. Právní úpravu v něm obsaženou tedy není možno považovat za speciální ve vztahu k OZ. Povinnosti stanovené OZ a ZKB tedy existují paralelně a uplatňují se navzájem nezávisle.

Na rozdíl od výše popsané úpravy OZ, ZKB ukládá povinnosti pouze orgánům a osobám výslovně vyjmenovaným v §3, a to pouze v rozsahu stanoveném dalšími ustanovení ZKB. Regulace ZKB je tedy vedena principem minimalizace zásahů veřejné moci do autonomie vůle regulovaných subjektů, kdy zákon ukládá povinnosti pouze těm orgánům veřejné moci a osobám soukromého práva, které mají zásadní význam pro kybernetickou bezpečnost České republiky [19, s. 74].

S ohledem na veřejnoprávní povahu ZKB je třeba respektovat princip legality zakotvený v Ústavě [23, čl. 2(3)] a Listině základních práv a svobod [24, čl. 2(2)], jenž stanoví, že *„státní moc lze uplatňovat jen v případech a v mezích stanovených zákonem a zákonem stanoveným způsobem.“* V souladu s tímto principem je třeba veřejnoprávní předpis vykládat *„zejména za použití jazykového (gramaticko-sémantického) a logického výkladu, tedy zejména podle významu jednotlivých slov, jejich spojení a větné skladby případně za použití argumentace klasické formální logiky (avšak s velmi limitovaným využitím výkladu per analogiam, který se ve*

veřejném právu uplatní jen omezeně)." [25] Z toho mj. plyne, že zatímco subjekty uvedené v §3 ZKB mají povinnost postupovat v souladu s regulací v něm obsaženou, ostatní subjekty, *a contrario*, tuto povinnost nemají nelze ji po nich vyžadovat ani ukládat na základě analogie. [25]

4.1.2.2 Řízení dodavatelů jako bezpečnostní opatření dle ZKB

Subjekty s povinností zavést bezpečnostní opatření stanovená ZKB a VKB

Jak je uvedeno v úvodu této bakalářské práce, řízení dodavatelů je jedním z bezpečnostních opatření dle ZKB [10, §5(2)(e)]. Povinnost zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti spravovaného informačního a komunikačního systému není obecně uložena všem orgánům a osobám uvedeným v §3 ZKB [2, s.245]. Dopadá pouze na:

a) *„správce[4] a provozovatele[5] informačního systému kritické informační infrastruktury[6],*
b) *správce[4] a provozovatele[5] komunikačního systému kritické informační infrastruktury,*
c) *správce[4] a provozovatele[5] významného informačního systému[7],*

---

[4] Správcem systému ZKB rozumí orgán nebo osoba, *„které určují účel zpracování informací a podmínky provozování"* [10, §2(e) a (f)] informačního nebo komunikačního systému. Tato definice se uplatní napříč vymezením povinných osob.

[5] Provozovatelem systému ZKB rozumí *„orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém"* [10, §2(g)]. Navzdory čistě jazykovému výkladu, dle stanoviska NÚKIB vyjádřeného v *„Informace o institutu provozovatele informačního nebo komunikačního systému"*, postačuje, zajišťuje-li provozovatel pouze technické, nebo programové prostředky, eventuálně jejich kombinaci [38, s.4]. Tato definice se uplatní napříč vymezením povinných osob.

[6] Kritickou informační infrastrukturou *"se dle § 2 písm. g) a písm. i) zákona č. 240/2000 Sb., krizového zákona, rozumí prvek nebo systém prvků kritické infrastruktury, v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti dle § 2 písm. b) zákona č. 181/2014 Sb. o kybernetické bezpečnosti* [39]*".* Proces určování prvků kritické infrastruktury probíhá po vzájemném projednání mezi potenciálním povinným subjektem a NÚKIB [39]. Podrobný popis procesu určování prvků kritické informační infrastruktury lze nalézt na webových stránkách NÚKIB [40].

[7] Za významný informační systém ZKB označuje *„informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci"* [10, §2(d)]. Postup určení významných informačních systémů je v detailu popsán na webových stránkách NÚKIB [41].

d) *správce[4] a provozovatele[5] informačního systému základní služby[8], pokud nejsou správcem nebo provozovatelem dle písm. a) nebo b)"*

[10, §4(2)].

S ohledem na bezpečnostní riziko související se zapojením dodavatelů, ZKB stanoví povinnost subjektů vyjmenovaných pod písm. a) až d) výše *„zohlednit požadavky vyplývající z bezpečnostní opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou"* [10, §4(4)].

Požadavky na bezpečnostní garance u dodavatele mohou některým dodavatelům bránit ve spolupráci s odběratelskou organizací. Bez dalšího by tento požadavek odběratelské organizace mohl být chápán jako omezení hospodářské soutěže mezi dodavateli či poskytnutí konkurenční výhody konkrétnímu či skupině potenciálních dodavatelů. V zájmu bezpečnosti informačních a komunikačních systémů však ZKB výslovně stanoví, že v míře nezbytné pro splnění povinností jím stanovených, nelze požadavky vyplývající z bezpečnostní opatření považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži [10, §4(4)].

---

[8] Za základní službu ZKB považuje *„službu, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některých z těchto odvětví a) energetika, b) doprava, c) bankovnictví, d) infrastruktura finančních trhů, e) zdravotnictví, f) vodní hospodářství, g) digitální infrastruktura, h) chemický průmysl"* [10, §2(i)]. Pro to, aby se služba kvalifikovala jako základní služba musí být kromě zákonné definice naplněna též odvětvová a dopadová kritéria stanovená zvláštními právními předpisy. Podrobný popis procesu určení základní služby lze nalézt na webových stránkách NÚKIB [42].

Ve vztahu k základní službě ZKB definuje další povinný subjekt, a to provozovatelem základní služby. Tímto je orgán nebo osoba základní službu poskytující a zároveň určený rozhodnutím NÚKIB [10, §2(k)]. V kontextu bakalářské práce je žádoucí upozornit, že provozovateli základní služby je ukládána informační povinnost směrem ke správci a provozovateli informačního systému základní služby. Není-li však provozovatel základní služby, správcem či provozovatelem informačního systému základní služby, neváže jej povinnost zavést bezpečností opatření k ochraně informačního systému základní služby.

Informačním systémem základní služby ZKB pak rozumí pouze takový systém, na němž je poskytování základní služby závislé [10, §2(j)].

Subjekty, jimž je ukládána povinnost zavést vhodná bezpečnostní opatření

Poskytovateli digitálních služeb je ukládána méně restriktivní povinnost, a to *„zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací, které využívá v souvislosti se zajišťováním své služby“* [10, §4(4)]. V souladu se směrnicí NIS [22, recitál 49], tak ZKB ponechává těmto poskytovatelům větší volnost ve volbě opatření k zajištění kontinuity jejich služeb [2, s.244]. S ohledem na větší volnost při určení bezpečnostních opatření, může být použití metodiky předkládané v této bakalářské práci pro poskytovatele digitálních služeb nad míru limitující. Vzhledem ke specifickému režimu, není určení bezpečnostních opatření ve vztahu k dodavateli poskytovatele digitálních služeb v této bakalářské práci dále rozebíráno.

4.1.2.3 Speciální pravidla pro dodavatele služeb cloud computingu

Speciální požadavky zákon klade též na smlouvy, jejichž předmětem je nabytí služby cloud computingu, uzavírané subjekty s povinností zavést opatření stanovená ZKB a VKB (viz. vymezení výše), popř. provozovatelem základní služby. Tyto speciální požadavky se uplatní pouze v případě jsou-li tyto subjekty orgány veřejné moci. Jimi uzavíraná smlouva musí garantovat:

a) že poskytovatel služby cloud computingu bude dodržovat bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená NÚKIB[9], jakož i
b) dostupnost informací a dat uchovávaných poskytovatelem cloud computingu pro odběratelskou organizaci.

Dále musí smlouva o poskytnutí služby cloud computingu uzavíraná orgány veřejné moci:

a) zavázat poskytovatele služeb k respektování bezpečnostní politiky odběratele služeb, k bezodkladnému informování odběratele o kybernetických bezpečnostních incidentech vzniklých při poskytování služeb a vymezit pravidla zákaznického auditu,

[9] §28(2)(a) ZKB obsahuje zákonné zmocnění k vydání prováděcího předpisu stanovícího rozsah bezpečnostních opatření pro orgány veřejné moci využívající služby cloud computingu. K datu odevzdání této bakalářské práce relevantní vyhláška nebyla vydána.

b) stanovit úrovně poskytovaných služeb a pravidla řízení kontinuity činností souvisejících se službou cloud computingu,
c) určit pravidla schvalování subdodavatelů poskytovatele služeb,
d) vymezit bezpečnostní pravidla pro případ ukončení smluvního vztahu,
e) určit vlastníka uchovávaných dat a pravidla jejich ochrany,
f) obsáhnout dohodu o důvěrnosti smluvního vztahu jako celku, jakož i jeho obsahu, a
g) obsáhnout ujednání o kompenzaci nákladů vynaložených na zavedených bezpečnostních opatření.

[10, §4(5) a (6)].

Zároveň, podobně jako v případě obecné povinnosti zavést a provádět bezpečnostní opatření, je stanoveno, že zohlednění těchto požadavků v míře nezbytné pro splnění povinností dle ZKB, *„nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku v hospodářské soutěži“* [10, §4(7)]. Vyhláška, jíž bude zákonné zmocnění NÚKIB naplněno, je v době zpracování této bakalářské práce v legislativním procesu. Vzhledem k tomu, že v době vzniku této bakalářské práce nejsou povinnosti zavést bezpečnostní opatření pro poskytování služby cloud computingu legislativně ukotveny, nebude tato oblast dále rozebírána.

4.1.3 Vyhláška o kybernetické bezpečnosti

VKB je prováděcím předpisem k ZKB, který byl vydán NÚKIB na základě zákonného zmocnění v ZKB obsaženého [10, §28(2)(a) až (d) a (f)]. Aktuálně platná VKB byla vydána v souvislosti s transpozicí směrnice NIS [22] do českého právního řádu a v plném rozsahu nahradila dřívější právní úpravu.

Z hlediska předmětu této bakalářské práce je stěžejní druhá část vyhlášky, která stanoví obsah a rozsah bezpečnostních opatření, jež jsou povinny zavést osoby určené ZKB (viz. výše). Tato opatření se člení do dvou skupin, a to technická a organizační opatření.

Řízení dodavatelů je řazeno mezi organizační opatření a jeho bližší úpravu nalezneme zejm. v §8 VKB. Při prostudování povinností v tomto paragrafu

stanovených si lze povšimnout, že VKB odlišuje dvě kvalitativně různé skupiny dodavatelů, a to běžné dodavatele a tzv. významné dodavatele (pojmy jsou blíže vymezeny níže).

Na běžné dodavatele se vztahují tři relativně obecné povinnosti. Povinná osoba je povinna stanovit pro tyto dodavatele pravidla zohledňující požadavky systému řízení bezpečnosti informací, s těmito pravidly dodavatele seznámit a vyžadovat jejich plnění. Povinné osobě je dále ukládána povinnost řídit rizika spojená s dodavateli [7, §4(1)(a)(d)(e)]. Pochopitelně, dle pravidla *a minori ad maius*, veškeré povinnosti platné pro běžné dodavatelům, musí být dodržovány i ve vztahu k významným dodavatelům.

Na druhé straně, regulace zapojení a řízení významných dodavatelů je o poznání podrobnější. VKB povinné osobě ukládá, aby:

a) v rámci výběrového řízení a před uzavřením smlouvy provedla hodnocení rizik souvisejících s plněním předmětu výběrového řízení,
b) ve smlouvě s dodavatelem:
    i. zakotvila ujednání o bezpečnosti informací, stanovila způsoby a úrovně realizace bezpečnostních opatření a vymezila rozdělení odpovědnosti za jejich zavedení a kontrolu, jakož i možnost provedení zákaznického auditu;
    ii. zavázala dodavatele k dodržování bezpečnostní politiky odběratelské společnosti, nebo deklarovala schválení bezpečnostní politiky dodavatele;
    iii. adresovala oprávnění k užívání dat, definovala formát jejich předání a pravidla jejich likvidace;
    iv. vyžadovala a deklarovala soulad smluv s právním řádem a stanovila požadavky na autorství programového kódu a poskytnutí softwarových licencí;
    v. stanovila pravidla zapojení subdodavatelů garantující, že vybraní subdodavatelé neodporují požadavkům povinné osoby na dodavatele

a zaváží subdodavatele k dodržování ujednání mezi dodavatelem a povinnou osobou;

vi. stanovila pravidla řízení změn, řízení kontinuity činností závisejících či ovlivněných dodavatelem a podmínky ukončení spolupráce;

vii. zavázala dodavatele bezodkladně informovat povinnou osobu o kybernetických bezpečnostních incidentech, procesu řízení rizik dodavatelem a identifikovaných zbytkových rizicích, jakož i o změně kontroly dodavatele jako celku či významných aktiv využívaných dodavatelem při poskytování plnění;

viii. vyhradila si právo odstoupit od smlouvy pro případ významné změny kontroly nad dodavatelem či změny kontroly nad stěžejními aktivy využívanými dodavatelem pro plnění smlouvy; a

ix. stanovila sankce pro případ porušení smluvních povinností dodavatelem.

[7, §8(2) a příloha 7]

c) prováděla pravidelné hodnocení rizik a kontrolu bezpečnostních opatření, jakož i plnění smlouvy významným dodavatelem z hlediska systému řízení bezpečnosti informací, a to buď svépomocí či za pomoci třetí strany (typicky specializované auditní společnosti), a zajistila řešení zjištěných nedostatků,

d) vedla evidenci významných dodavatelů a prokazatelně písemně je o vedení v této evidenci informovala, a to v minimálním rozsahu stanoveném VKB [7, §8(1)(2)].

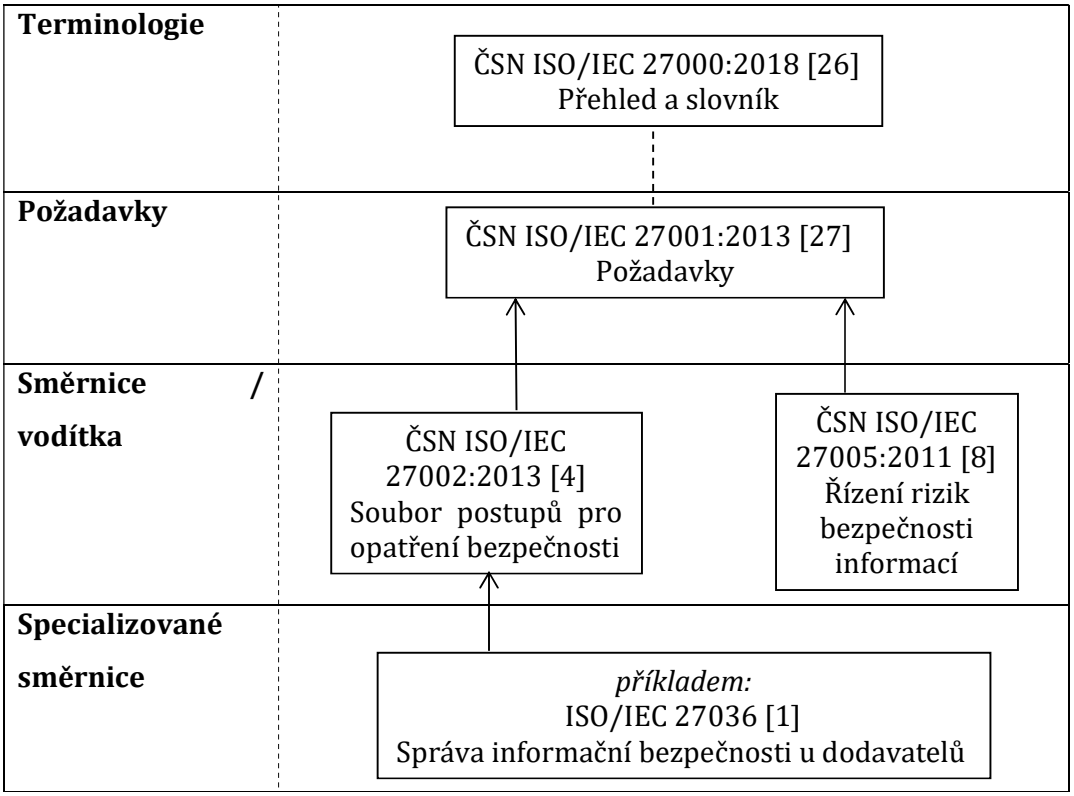
Úprava řízení dodavatelů však není jediným ustanovením VKB, které ovlivňuje nastavení práv a povinností v rámci dodavatelského vztahu. Dodavatelé musí být zohledněni i v rámci řízení aktiv [7, §4], kdy dle VKB jsou dodavatelé považováni za podpůrné aktivum. Povinná osoba musí zajistit poučení dodavatelů v rámci implementace bezpečnosti lidských zdrojů [7, §9]. A v neposlední řadě je povinná osoba povinna zajistit, že mj. i dodavatelé budou oznamovat neobvyklé chování systému či podezření na zranitelnosti v rámci systému zvládání kybernetických bezpečnostní událostí a incidentů [7, §14].

VKB je, stejně jako ZKB, předpisem veřejného práva. Ustanovení v nich obsažená jsou tedy kogentní, tzn. není možné se od nich odchýlit soukromoprávní dohodou učiněnou mezi povinnou osobou a dodavatelem. Dle názoru autorky by tak např. smluvní ujednání dodavatelské smlouvy, které významnému dodavateli uloží pouze obecnou povinnost zavést vhodná technická opatření k zabezpečení relevantních aktiv, bylo v rozporu s veřejnoprávní regulací, neboť nedosahuje kvality požadované VKB [7, §8(2)(b)]. Za tento postup povinné osobě hrozí pokuta až 5 min. Kč [10, §25(7)(a) ve spojení s §25(12)(a)], a to bez ohledu na skutečnost, zda k narušení bezpečnosti informací dojde či nikoli. Zároveň povinná osoba nebude schopna požadovat náhradu vzniklé újmy (tj. zaplacenou částku pokutu) od dodavatele.

Na druhou stranu, je nepochybně možná úprava nad rámec ustanovení ZKB a VKB, např. o rozdělení nákladů na implementaci bezpečnostních opatření vyžadovaných odběratelskou společností. Stejně tak, odběratelská organizace může (narozdíl od státu, srovnej výklad k principu legality obsažený v předchozí kapitole) požadovat v rámci soukromoprávního smluvního vztahu s dodavatelem zabezpečení informací nad rámec zákonných povinností.

4.2 Technické normy ISO

„ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace.“[4, s.6] V oblasti informační bezpečnosti je za oborový standard považována řada ISO/IEC 2700x také označovaná jako Systém řízení bezpečnosti informací.
Základní systematiku ISO/IEC norem adresujících předmět této bakalářské práce vyjadřuje následující schéma:



Tabulka 1 - Systematika ISO/IEC norem

Zdroj: na základě [26, obrázek na s. 19]

Z hlediska zpracování této bakalářské práce jsou významné především normy ČSN ISO/ IEC 27001:2013[27] a ČSN ISO/ IEC 27002:2013[4], jimiž se silně inspirovala i regulace obsažená v ZKB[19, s.55].

ČSN ISO/ IEC 27001:2013[27] je obecnější z obou norem a stanoví *„požadavky na ustanovení, implementování, udržování a neustálé zlepšování řízení bezpečnosti informací“* [27, s.6], jakožto rámcového procesu směřujícího k zajištění dostupnosti, důvěrnosti a integrity informací prostřednictvím informovaného řízení související rizik.

ČSN ISO/ IEC 27002:2013[4] pak můžeme označit za prováděcí normu k ČSN ISO/ IEC 27001:2013[27], neboť obsahuje soubor doporučení či pokynů pro implementaci opatření v rámci procesu řízení bezpečnosti informací. [27, s. 7]

Obě výše uvedené, i další normy z řady ISO/IEC 2700x, mají doporučující charakter a jejich aplikace není omezena na organizace konkrétního typu. Pravidla v nich obsažená mohou zavést a provádět jak organizace soukromého, tak veřejného sektoru, komerční i neziskové, a to bez ohledu na jejich velikost. Z organizačních důvodů ale procesy v nich popsané zavádějí primárně střední až velké organizace. Nespornou výhodou těchto standardů je jejich celosvětové uznání.

Mezinárodní normy ISO/IEC jsou pro české prostředí překládány a vydávány Úřadem pro technickou normalizaci, metrologii a stavební zkušebnictví jako ČTN. Neboť relevantní ČTN jsou pouze překladem mezinárodních standardů, pracuje s nimi tato bakalářská práce jako s jedním normativním celkem.

Status ČTN je určen zákonem, který stanoví, že *„ČTN není obecně závazná"* [28, §4]. I z tohoto pravidla však existují výjimky, kdy zákon na ČTN výslovně odkáže a závaznost jí tak přizná. V oblasti kybernetické bezpečnosti však takovýto odkaz v platné právní úpravě nenalezeme. Pro úplnost je však vhodné zmínit, že úprava obsažená v dnes již zrušené vyhlášce o kybernetické bezpečnosti [29], k ISO/ IEC 27001:2013, resp. ČSN ISO/ IEC 27001:2013[27] referovala jako jednomu ze způsobů prokázání certifikace. Vyhláška stanovila, že byl-li informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém povinného orgánu nebo osoby zcela zahrnut do rozsahu systému řízení rizik certifikovaného podle ISO 27001:2013, resp. ČSN ISO/ IEC 27001:2013 akreditovaným certifikačním orgánem a zároveň vede-li povinný subjekt ve vyhlášce vyjmenované dokumenty, platí, že splňuje požadavky podle zákona a dané vyhlášky. [29, §29] Tato regulace však do platné VKB převzata nebyla.

Je-li účelem regulace ZKB a VKB nikoli pouze formální, ale materiální zajištění bezpečnosti kritické infrastruktury, pak tento odklon zákonodárce od prokázání certifikace skrze certifikaci dle technických norem, je nutno považovat za správný. *„Podstatný rozdíl totiž je a vždycky byl v pojetí technických opatření, což má své logické opodstatnění – ISO 27001 je univerzální a to, jakým způsobem ji organizace*

implementují, je na nich samotných a jen při certifikačním auditu se dvoustupňově zjišťuje, jak byla příslušná doporučení aplikována.“ [30]

Na druhé straně, ačkoli ISO normy nejsou v českém právním prostředí právně závazné a ISO certifikací není možno prokázat soulad s požadavky ZKB a VKB, jsou stále důležitým podpůrným zdrojem při stanovení konkrétním opatření k naplnění zákonných požadavků a z téhož důvodu byly též intenzivně využívány při přípravě metodiky předkládané v této bakalářské práci.

4.3 Typy dodavatelů a s nimi spojená rizika pro bezpečnost informací

4.3.1 Z hlediska povahy předmětu plnění

Základním, široce používaným, kritériem rozlišení dodavatelů je povaha jimi poskytovaného plnění odběratelské společnosti. Tím může být zboží nebo služba. V kontextu dodavatelů povinných subjektů dle ZKB lze jako příklad uvést dodání hardware nebo vývoj personalizovaného software.

Ačkoli z hlediska právního, se budou tyto vztahy řídit různými smluvními typy[10], potenciální zranitelnosti, které je třeba v těchto případech adresovat, jsou shodné a lze je rozdělit do tří základních skupin.

Prvním z nich je přístup dodavatele k určitým informacím odběratelské organizace za účelem dodání a/nebo vytvoření zboží a/nebo poskytnutí služby a zpracování těchto informací na zařízení dodavatele osobami, ať již zaměstnanci či dalšími dodavateli, pod kontrolou dodavatele.

Druhou oblastí je pak poskytování služeb a/nebo provádění díla v prostorách odběratelské společnosti a přístup zaměstnanců či spolupracovníků k technickému či programovému vybavení odběratelské společnosti.

---

[10] Nejčastěji se pak jedná o smlouvu kupní, smlouvu o dílo, smlouvu licenční či jejich kombinaci nebo smlouvu nepojmenovanou.

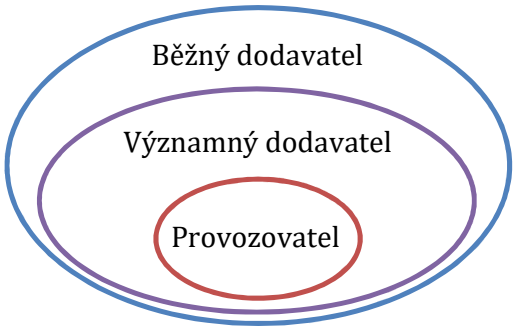
Třetí oblastí je pak nedostatečná kvalita dodaného zboží či poskytnuté služby, a to jak faktická (tj. zda zboží či služba trpí vadami), tak právní (tj. zda neporušuje práva třetích stran).

I při odhlédnutí od regulatorních požadavků, má odběratelská organizace z těchto důvodů legitimní zájem nejen na kvalitativní kontrole dodaného zboží, ale též výrobního či vývojového procesu.

Kvalifikované hodnocení rizika souvisejícího se zapojením či spoluprací s konkrétním dodavatelem je však možno provést pouze při posouzení sjednaného předmětu plnění, jakož i způsobu jeho poskytnutí.

4.3.2 Z perspektivy ZKB a VKB

Z pohledu ZKB a VKB jsou rozlišovány tři typy dodavatelů. Vztah mezi nimi demonstruje následující diagram:



Obrázek 1 - Typy dodavatelů
Zdroj: vlastní zpracování

4.3.2.1 Provozovatel

Na provozovatele lze nahlížet dvojí optikou. Jednak je dodavatelem správce, zároveň je však sám povinnou osobou, jíž ZKB přímo ukládá povinnosti.

Za provozovatele systému ZKB považuje *„orgán nebo osobu zajišťující funkčnost technických a programových prostředků tvořících informačního nebo komunikační systém“* [10, §2(g)]. Navzdory čistě jazykovému výkladu, dle stanoviska NÚKIB vyjádřeného v *„Informace o institutu provozovatele informačního nebo*

komunikačního systému", postačuje, zajišťuje-li provozovatel pouze technické, nebo programové prostředky, eventuálně jejich kombinaci [38, s.4].

Na druhé straně, k získání statusu provozovatele nepostačuje, aby dodavatel poskytl povinné osobě *„jednorázové dodávky technických a programových prostředků, bez dalších navazujících činností (typicky se jedná o servis a support aj.)"* [2, s. 165]. Status provozovatele rovněž nemohou nabýt dodavatelé provozovatele, neboť pověření k provozování informačního či komunikačního systému kritické infrastruktury nebo významného informačního systému může udělit pouze správce [10, §6a, téže 2, s. 165].

Zapojení provozovatele je tedy *„ve své podstatě outsourcing činností, služeb či systémů, které správce výše uvedených systémů nezajišťuje (nespravuje), nebo nemusí zajišťovat."* [2, s. 297] Outsourcing je však možný pouze pokud ho nezakazuje zvláštní zákon.

Pověří-li správce dodavatele provozováním informačního či komunikačního systému kritické infrastruktury nebo významného informačního systému, z části na něj přenáší odpovědnost za soulad těchto systémů se zákonem [38, s. 5]. V zájmu kontinuity provozu těchto systémů, ZKB výslovně upravuje povinnost provozovatele předat správci na vyžádání data, údaje a informace získané či zpracovávané v souvislosti s provozováním systému [10, §6a].

ZKB nezakládá žádná výslovná omezení pro výběr subjektu provozovatele. Z dikce VKB však lze dovodit, že provozovatel je vždy též významným dodavatelem [7, §8(4)], a při jeho výběru je tedy třeba respektovat pravidla stanovená pro výběr významného dodavatele.

4.3.2.2 Významný dodavatel

Významným dodavatelem je provozovatel (dle definice výše) *„a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému."* [7, §2(n)] Pro výběr a řízení významných dodavatelů platí pravidla popsaná v kapitole 4.1.3 této bakalářské

práce. Z hlediska výše zmíněné kvalifikace provozovatele jako povinné osoby dle ZKB je významná zejm. povinnost správce (tj. odběratelské společnosti) informovat své významné dodavatele o jejich evidenci. Na splnění této informační povinnosti správce je vázána povinnost provozovatele oznámit své kontaktní údaje NÚKIB [7, §8(4)].

4.3.2.3 Běžný dodavatel

Poslední skupinou dodavatelů jsou běžní dodavatelé, kteří se nekvalifikují jako významní dodavatelé ani jako provozovatelé. Ve vztahu k těmto platí relativní volnost a uplatní se pouze omezené povinnosti blíže popsané v kapitole 4.1.3 této bakalářské práce.

4.4 Bezpečnostní opatření

Dle ZKB se bezpečnostním opatřením rozumí *„soubor úkonů, jejich cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru“* [10, §4(1)].

Dle důvodové zprávy k ZKB slouží bezpečnostní opatření především ke zvýšení odolnosti kritické infrastruktury proti kybernetickým útokům, tj. mají primárně preventivní účel [19, s. 74]. V ZKB a prováděcí VKB nalezneme ale i řadu opatření reaktivního charakteru, jejichž cílem je efektivní zvládnutí kybernetických bezpečnostních událostí a incidentů [19, s. 74].

Bezpečností opatření, která jsou povinné subjekty povinny zavést ZKB člení do dvou skupin, a to opatření technická opatření a organizační opatření [10, §5].

„Organizačními opatřeními jsou a) systém řízení bezpečnosti informací, b) řízení rizik, c) bezpečnostní politika, d) organizační bezpečnost, e) stanovení bezpečnostních požadavků pro dodavatele, f) řízení aktiv, g) bezpečnost lidských zdrojů, h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému, i) řízení přístupu osob ke kritické informační infrastruktuře nebo významnému informačnímu systému, j) akvizice, vývoj a údržba kritické informační infrastruktury a významných infomačních systémů, k) zvládání

kybernetických bezpečnostní událostí a kybernetických bezpečnostních incidentů l) řízení kontinuity činností a m) kontrola a audit kybernetické informační infrastruktury a významných informačních systémů.“ [10, §5(1)]

Mezi technická opatření se řadí *„a) fyzická bezpečnost, b) nástroj pro ochranu integrity komunikačních sítí, c) nástroj pro ověřování identity uživatelů, d) nástroj pro řízení přístupových oprávnění, e) nástroj pro ochranu před škodlivým kódem, f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů, g) nástroj pro detekci kybernetických bezpečnostních událostí, h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, i) aplikační bezpečnost, j) kryptografické prostředky, k) nástroj pro zajišťování úrovně dostupnosti informací a l) bezpečnost průmyslových a řídících systémů.“* [10, §5(2)]

Ve větším detailu je pak obsah a rozsah jednotlivých bezpečnostních opatření popsán v druhé části VKB. K povinnosti zavést bezpečnostní opatření viz. kapitola 4.1.2 této bakalářské práce. Tyto subjekty jsou současně povinny vést o bezpečnostních opatřeních bezpečnostní dokumentaci, jejíž obsah závazně stanoví příloha č. 5 VKB.

Jak v ZKB, tak následně ve VKB, jsou jednotlivá bezpečnostní opatření navržena v souladu s principem technologické neutrality. Tzn. že *„bezpečnostní opatření, k jejichž dodržování zavazuje ZKB vybrané subjekty, jsou definována tak, aby mohlo být jejich splnění řešeno za užití různých technologií a postupů.“* [2, s. 134] Je tedy na uvážení a rozhodnutí povinných osob, jaký konkrétní způsob zabezpečení svých informačních struktur zvolí, a to včetně volby dodavatele bezpečnostního řešení [2, s. 135]

Z hlediska požadavků na zavedení bezpečnostních opatření dodavatelem je významné ustanovení VKB, jež stanoví, že *“povinná osoba v rámci uzavíraných smluvních vztahů stanoví způsoby a úrovně realizace bezpečnostních opatření”* [7, §8(2)(b)]. V této souvislosti je vhodné odkázat na normu ČSN ISO/IEC 27002:2013, jež konstatuje, že *“výběr opatření je závislý na organizačních rozhodnutí na základě*

kritérií přijetí rizika, možnosti ošetření rizika a obecného přístupu k řízení rizik platících pro organizaci" [4, s. 8]. Pro úplnost je však třeba podotknout, že zde citované ustanovení VKB dopadá pouze na významné dodavatele. Ve vztahu k běžným dodavatelům je povinná osoba zákonem vázána pouze stanovit pravidla, nikoli k určení bezpečnostních opatření. Jak však bylo již zmíněno výše, zákon povinné osobě nebrání, aby v rámci soukromoprávního vztahu s dodavatelem stanovila nároky na dodavatele přísnější, než požaduje zákon.

4.5 Řízení rizika

V této kapitole je předkládán výklad základních pojmů z oblasti řízení rizika, a to v rozsahu, v jakém s nimi pracuje proces hodnocení dodavatele nastíněný v této bakalářské práci.

4.5.1 Aktivum

4.5.1.1 Dle ČSN ISO/IEC 2700x

V kontextu norem ČSN ISO/IEC 2700x se aktivem rozumí *„cokoli, co má pro organizaci hodnotu a vyžaduje ochranu"* [8, s. 19]. Norma ČSN ISO/IEC 27005 též předkládá kategorizaci aktiv na aktiva primární a podpůrná a příklady aktiv, které je možné do daných kategorií zařadit [8, příloha B].

Za primární aktiva označuje takové obchodní činnosti a procesy, jejichž ztráta, omezení či změna by měla dopad na plnění poslání organizace, znemožnila plnění smluvních, regulatorních či zákonných požadavků a/nebo obsahují chráněné technologie. Za primární aktiva jsou dále považovány informace, a to jsou-li nezbytné pro plnění poslání či činnost organizace, osobní údaje chráněné zvláštními zákony, strategické informace a velmi nákladné informace. [8, 19]

Jako příklady podpůrných aktiv pak norma uvádí hardware, software, sítě, pracovníky, lokalitu a organizaci. [8, 19]

Kategorizace aktiv navržená ČSN ISO/IEC 2700x klade důraz na hodnocení aktiva v kontextu organizace jako celku, nikoli konkrétního systému.

4.5.1.2 Dle VKB

Ačkoli ZKB i VKB hojně používají obecný pojem „aktiva“, jeho zákonnou definici v nich nenalezneme. VKB definuje pouze podřízené pojmy, a to primární a podpůrné aktivum.

Primárním aktivem se dle VKB rozumí *„informace nebo služba, kterou zpracovává nebo poskytuje informační systém“* [7, §2(g)].

Podpůrným aktivem se dle VKB rozumí *„technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému“* [7, §2(f)].

Lze si povšimnout, že ve srovnání s terminologií používanou normativní řadou ČSN ISO/IEC 2700x je kategorizace VKB úžeji spjata s provozem informačního a komunikačního systému. S ohledem na zaměření toto bakalářské práce, proces hodnocení dodavatelů navržený v této bakalářské práci vychází z členění aktiv obsaženého ve VKB.

4.5.2 Hrozba

4.5.2.1 Dle ČSN ISO/IEC 2700x

ISO/IEC 27000 hrozbou rozumí potenciální příčinu nechtěného incidentu, který může způsobit škodu systému či organizaci [26, s. 10]. Tuto definici dále rozvíjí ČSN ISO/IEC 27005 a uvádí, že *„hrozby mohou být přírodního i lidského původu a mohou být náhodné nebo úmyslné. Hrozba může vyvstat zevnitř i zvenčí organizace.“* [8, s. 19]

4.5.2.2 Dle VKB

Podobnou definici hrozby, jakou obsahuje ISO/IEC 27005 nalezneme i v české právní úpravě, která hrozbu chápe jako *“potenciální příčinu kybernetické bezpečností události nebo kybernetického bezpečnostního incident, která může způsobit škodu.”* [7, §2(e)]

Při výkladu výše uvedené definice je třeba zohlednit také pojmy „kybernetický bezpečnostní incident“ a „kybernetická bezpečnostní událost“. Kybernetickou

bezpečnostní událostí se rozumí *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací“* [10, §5(1)]. Kybernetickým bezpečnostním incidentem *„je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečností události“* [10, §5(2)]. Z hlediska posouzení schopnosti hrozby vést ke vzniku škody je třeba vhodné poznamenat, že v kontextu OZ je škoda definována jako *„újma na jmění“* [12, §2894], která zahrnuje náhradu skutečné škody a ušlého zisku [12, §2952]. S ohledem na pojetí prezentované NÚKIB v jím vydaných metodikách k hodnocení rizika (viz. doporučené aspekty hodnocení dopadu dle [9]) však tento výklad není udržitelný a při posuzování možné „škody“ dle VKB je třeba hodnotit veškerou potenciální újmu, vč. nemajetkové, a to v nejširším možném rozsahu.

Z kontextu výše uvedených zákonných definic je patrné, že relevantní hrozbou v kontextu zákonné úpravy kybernetické bezpečnosti je pouze potenciální příčina narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací, a to pouze za předkladu, že je způsobilá vést ke vzniku újmy, ať již organizaci či třetím subjektům.

Detailnější pojednání o konceptu hrozby přesahuje téma této bakalářské práce a nebude tedy dále rozvíjeno. Podrobnější informace lze nalézt např. v publikaci Cybersecurity [2, s.73 a násl.]

4.5.3 Zranitelnost

ISO/IEC 27000 i VKB definují zranitelnost shodně jako *„slabé místo aktiva nebo bezpečnostních opatření, která může být zneužito jednou nebo vícero hrozbami.“* [26, s. 11; 7, §2(p)]

Podobně v případě hrozby může být příčinou zranitelnosti celá řada faktorů jako technická závada, jednání člověka nebo zásah vyšší moci [2, s. 72]. Příklady možných zranitelností najdeme ve VKB [7, příloha 3] i ČSN ISO/IEC 27005 [8, příloha D].

4.5.4 Riziko

Stejně jako v případě zranitelnosti, i definice rizika je shodná pro ISO/IEC 27000 a VKB. *„Rizikem je možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu.“* [7, §2(h); 26, s. 8] Riziko tedy vyjadřuje pravděpodobnost, s jakou může nastat určitá nežádoucí událost [2, s.68]. V řadě norem ISO/IEC 2700x je hodnocení rizika věnována norma ISO/IEC 27005 [8]. V rámci zákonné regulace je úprava hodnocení rizika o poznání strožejší a je limitována na přílohu č. 2 VKB [7].

V rámci hodnocení rizika je standardně zvažována závažnost hrozby, příp. zranitelnosti a dopadu. Výsledkem hodnocení rizika je jeho klasifikace. Pro klasifikaci rizik je standardně používána stupnice 1 až 4, což odpovídá i metodice nastíněné VKB, které riziko doporučuje hodnotit jako nízké, střední, vysoké až kritické [7, příloha č. 2].

V návaznosti na hodnocení rizika je třeba zvolit vhodnou metodu ošetření daného rizika. ČSN ISO/IEC 27005 uvádí čtyři možné způsoby ošetření rizika, a to jeho redukci, podstoupení, vyhnutí se nebo sdílení rizik [8, s. 24]. Naproti tomu VKB pracuje pouze se dvěma způsoby ošetření rizika, a to jeho akceptace a redukce. Za akceptovatelné bez dalšího označuje nízké riziko. Střední riziko je akceptovatelné pouze v případě, že opatření k jeho redukci byly vysoce náročná. Je-li riziko vysoké či kritické, musí být redukováno, v případě kritického rizika neprodleně. [7, příloha 2].

Platná právní úpravy kybernetické bezpečnosti kritické infrastruktury tedy nepřipouští prosté přenesení rizika na dodavatele. Tímto je podpořen závěr učiněný v části 4.1.3, že k naplnění požadavků zákonné úpravy, nepostačuje, je-li dodavateli smlouvou uložena obecná povinnost zavést vhodná technická opatření k zabezpečení relevantních aktiv.

4.5.5 Důvěrnost, integrita, dostupnost v. Parkerian Hexad

Dle ZKB se bezpečností informací rozumí *„zajištění důvěrnosti, integrity a dostupnosti informací a dat“* [10, §2(c)]. Stejně jako řada norem ISO/IEC 2700x je ZKB založen na klasické triádě CIA (confidentiality, integrity, availability) [srovnej

26, čl. 4.2.3]. Bližší definici jednotlivých pojmů však v platné legislativě nenalezneme, je však možné opřít se o vymezení těchto pojmů v ISO/IEC 27000 [26].

4.5.5.1 Důvěrnost informací a dat

Koncept důvěrnosti informací je relativně široce známý. ISO/IEC 27000 uvádí, že důvěrností se rozumí, že informace *„není zpřístupněna nebo sdělena neoprávněným jedincům, osobám nebo procesům“* [26, s. 2].

Jako příklad kybernetického bezpečnostního incidentu spočívajícího v porušení důvěrnosti informací lze uvést ukradení a prodej interní databáze klientských údajů zaměstnancem telekomunikačního operátora T-Mobile k němuž došlo v roce 2016. Tímto útokem bylo zasaženo přibližně 1,5 milionů klientů společnosti [31].

4.5.5.2 Integrita informací a dat

Integritou dat se rozumí jejich přesnost a úplnost [26, s. 5]. Zatímco útoky cílící na důvěrnost a dostupnost dat jsou poměrně časté, útoky na integritu dat jsou relativně nové. Jedná se o sofistikovanější útoky, které jsou zpravidla dobře naplánované a provedené. Jejich cílem je utajené pozměnění dat nebo transakce.

Jako příklad útoku na integritu je možno uvést útok známý pod názvem Carabanak, kterým byly v roce 2018 napadeny východoevropské banky. Útok byl realizován prostřednictvím škodlivého malware, jenž selektivně pozměnil relativně malý počet konkrétních transakcí. Pozměněním několika transakcí organizovaná skupina ukradla mezi 300 miliony a 1 bilionem dolarů [32].

4.5.5.3 Dostupnost informací a dat

Dostupnost informací a dat je chápána jako možnost oprávněné osoby k těmto datům na vyžádání přistoupit a použít je [26, s. 2].

Útoky na dostupnost dat jsou poměrně časté. Jejich cílem je buď odepření dostupnosti (typicky DDoS útok) nebo slouží jako nástroj pro vydírání správce informací či dat (tzv. ransomware útok).

Jako příklad útoku narušujícího dostupnost informací lze uvést hackerský útok, který odstavil z provozu veškeré přístroje a počítače v nemocnici v Benešově v listopadu minulého roku (2019) [33].

4.5.5.4 Parkerian Hexad

V odborné literatuře se setkáváme s názory, že CIA triáda není dostatečná. Argumentace je dvojí. Jednak CIA triáda je primárně zaměřena na technologie, jimiž jsou informace chráněny, a sekundárně je v některých případech problematické určit, který z jejích elementů byl konkrétním incidentem narušen (viz. např. [36]). Z toho důvodu je argumentováno pro používání tzv. Parkerianovy Hexády, která koncept CIA triády rozšiřuje o atributy kontroly (possession), užitečnosti (utility) a pravosti (autenticity) [35].

Kontrola

Aspekt kontroly v Parkerianovy Hexádě postihuje situaci, kdy důvěrná data jsou držena a ovládána neoprávněnou osobou, aniž tato má úmysl prolomit jejich důvěrnost [36].

Typickým příkladem může být krádež hardwarového vybavení za účelem jeho zpeněžení, nikoli přístupu k datům. Jsou-li data na zařízení uložená zálohována, nedojde k narušení dostupnosti. Jsou-li data též šifrována, je pravděpodobné, že nedojde ani k porušení důvěrnosti.

Je zřejmé, že tento aspekt je úzce spjat se základním konceptem důvěrnosti. Aniž dojde k narušení kontroly, nemůže dojít k narušení důvěrnosti. Narušení kontroly však bez dalšího neznamená narušení důvěrnosti.

Užitečnost (utility)

Název tohoto konceptu vysvětluje i jeho podstatu. Tento atribut odkazuje ke skutečnosti, že ačkoli jsou určité informaci či data dostupná, nemusí být pro útočníka užitečná. Koncept užitečnosti se tedy soustředí na obsah informace, čímž překonává základní aspekt dostupnosti informace či data. [36]

Ke ztrátě užitečnosti přitom může dojít nejen v důsledku jednání (př. šifrováním dat), ale též v důsledku životního cyklu informace (tj. informace již není validní, a tudíž nevyžaduje ochrany).

Pravost (autenticity)

Aspekt pravosti *„poskytuje záruku, že zpráva, transakce, nebo jiná výměna informací pochází od zdroje, z nějž udává“* [36, s. 14]. Pravost tedy, narozdíl od integrity vyžaduje prokázání identity, nikoli pouze správnosti a úplnosti. V praxi tedy vyžaduje, aby s informací byl spojen digitální certifikát identifikující jejího původce, nebo byla předávána skrze šifrované spojení mezi klientem a serverem [36].

Koncept pravosti je někdy terminologicky označován též jako princip neodmítnutelnosti, nepopiratelnosti či non-repudiation, a pod tímto názvem se se s ním můžeme setkat i v dalších InfoSec dokumentech [35].

S ohledem na to, že Parkerianova Hexáda jde nad rámec požadavků ZKB, není v metodice hodnocení dodavatelů zahrnuta.

5 Teoretický popis procesu hodnocení dodavatele

5.1 Prerekvizity hodnocení dodavatele

5.1.1 Zavedení systému řízení bezpečnosti informací

Za první prerekvizitu hodnocení dodavatele lze označit zavedení systému řízení bezpečnosti informací povinnou osobou. Tj. v organizaci povinné osoby musí být definovaný zejm. rozsah a cíle systému řízení bezpečnosti informací. Pro stanovený rozsah systému řízení bezpečnosti informací pak musí být provedeno hodnocení bezpečnostních potřeb, hodnocení rizik a stanovena přiměřená bezpečností opatření [7, §3(a) až (c)]. Pouze je-li tato prerekvizita naplněna, lze rozhodnout, zda služby potenciálního dodavatele spadají do rozsahu systému řízení bezpečnosti informací, či nikoli.

Mohlo by se zdát, že optimální cestou zajištění souladu povinné osoby se zákonnými požadavky je požadovat naplnění bezpečnostních požadavků po všech dodatelích, bez ohledu na předmět jejich činnosti. Ponecháme-li stranou značnou administrativní a ekonomickou neefektivitu takového přístupu, je nezbytné upozornit, že takové jednání povinné osoby by mohlo být hodnoceno jako nezákonné omezení hospodářské soutěže či neodůvodněná překážka v hospodářské soutěži. Výjimka stanovená ZKB, že zohlednění požadavků vyplývajících z bezpečnostních opatření není nezákonným omezením hospodářské soutěže nebo neodůvodněnou překážkou v hospodářské soutěži, se totiž uplatní pouze v rozsahu nezbytném pro splnění povinností dle ZKB.

5.1.2 Řízení aktiv

Další nezbytnou podmínkou určení rozsahu povinnosti dodavatele implementovat bezpečnostní opatření je existence katalogu primárních a podpůrných aktiv povinné osoby, jakož i metodiky jejich řízení.

S ohledem na to, že předkládaná metodika je navržena primárně dle platné legislativy v oblasti kybernetické bezpečnosti, je vhodné, aby v souladu s ní byla provedena též klasifikace aktiv povinné osoby. Nebude-li tomu tak, bude nezbytné

metodiku upravit tak, aby umožňovala hodnocení všech kategorií aktiv evidovaných povinnou osobou.

Metodika předpokládá existenci katalogu aktiv v následující struktuře:

- **Primární aktiva:** informace nebo služba, kterou poskytuje nebo zpracovává informační a komunikační systém.
- **Podpůrná aktiva:**
    - technická aktiva, tj. hardwarové a softwarové vybavení využívané k provozu, rozvoji, správě nebo zajištění bezpečnosti informačního a komunikačního systému.
    - personální aktiva, tj. zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.

Metodika je tedy založena na předpokladu, že předmětem plnění dodavatele je produkt či služba využívaná primárním aktivem. Metodika dále předpokládá, že důležitost toto primární aktiva je rámci organizace povinné osoby ohodnocena.
Předmětem metodiky není hodnocení aktiv ani jejich vzájemných vazeb.

5.1.3 Určení odpovědnosti

Následně je třeba určit okruh rolí zapojených do nastavení vztahů s a požadavků na dodavatele a určit rozsah jejich oprávnění a odpovědnosti. Níže je identifikován minimální okruh rolí, jež se na tomto procesu podílí. Kompetence všech níže zvažovaných rolí jsou stanoveny VKB [7, §7 a příloha 6].

5.1.3.1 Garant dodavatele

Dle VKB je garant aktiva *„bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva“* [7, §7(3)]. Z hlediska VKB je dodavatel podpůrným aktivem. Jako takovému mu proto musí být přiřazen garant. Obdobně jako v případě jiných aktiv, je garant dodavatele odpovědný za zajištění rozvoje, využití a bezpečnosti dodavatele jako aktiva.

Garant aktiva tedy nese ultimátní odpovědnost za nastavení parametrů spolupráce s dodavatelem, včetně stanovení a kontrolu zavedení řádných bezpečnostních opatření. Z praktického hlediska bude garantem dodavatele osoba oprávněná k podpisu smlouvy s daným dodavatelem.

5.1.3.2 Garanti dotčených primárních aktiv

S ohledem na to, že jeden dodavatel jako jedno podpůrné aktivu může být využíván vícero primárními aktivy, je třeba, aby tito byli při zapojení dodavatele konzultováni. Tento požadavek plyne z faktu, že požadavky kladené na dodavatele (vč. bezpečnostních) jsou přímo závislé na požadavcích kladených na primární aktiva. Opačně pak platí, že primární aktiva jsou pouze natolik zabezpečená, nakolik jsou zabezpečená podpůrná aktiva zapojená do jejich provozu, rozvoje či správy.

5.1.3.3 Manažer kybernetické bezpečnosti

Další rolí, jež musí být konzultována v rámci zapojení dodavatele do systému řízení bezpečnosti informací je manažer kybernetické bezpečnosti. Manažer kybernetické bezpečnosti nese dle VKB odpovědnost za systém řízení bezpečnosti informací, a to ve vztahu k vrcholovému vedení povinné osoby. Kromě toho se manažer kybernetické bezpečnosti podílí na procesu řízení rizik a vyhodnocuje vhodnost a účinnost bezpečnostních opatření [7, příloha 6]. S ohledem na klíčovou roli manažera kybernetické bezpečnosti v systému řízení informací není možné v tomto systému provádět změny bez vědomí a koncepční změny bez souhlasu této role.

5.1.3.4 Matice RACI

Standardní metodou zobrazení odpovědnosti v rámci určitého úkolu je tzv. matice RACI. RACI je akronymem počátečních písmen čtyř úrovní odpovědnosti, které tato metoda rozlišuje, konkrétně:

- R (Responsible) – osoba odpovědná za vykonání daného úkolu;
- A (Accountable) – osoba nesoucí celkovou odpovědnost za správné provedení úkolu;
- C (Consulted) – osoba, jejíž stanovisko je vyžadováno;

- I (Informed) – osoba, která je informována o průběhu a výsledku plnění úkolu.

Rozdělení odpovědnosti v procesu, hodnocení a zapojení výběru dodavatele lze tedy zobrazit následující RACI maticí:

ROLE	**RACI**			
	R	**A**	**C**	**I**
Garant dodavatele	ANO	ANO	-	-
Garanti dotčených primárních aktiv	-	-	ANO	ANO
Manažer kybernetické bezpečnosti	-	-	-	ANO

Tabulka 2 - RACI matice odpovědnosti v procesu řízení dodavatelů
Zdroj: vlastní zpracování

5.2 Klasifikace dodavatele

Bylo-li rozhodnuto, že dodávka potenciálního dodavatele náleží do rozsahu systému řízení bezpečnosti informací, je třeba rozhodnout, zda se bude dodavatel, z hlediska předmětu své činnosti klasifikován jako běžný nebo významný, nebo zda bude vystupovat v roli provozovatele. Tato kategorizace dodavatele je podstatná z nejen hlediska následného postupu stanovení bezpečnostních pravidel pro dodavatele, ale též proto, že v této fázi musí být provedeno rozhodnutí, zda předmět plnění dodavatele jen kvalifikuje jako provozovatele systému. Pouze správce má dostatek informací a nese odpovědnost za identifikaci provozovatele a splnění notifikační povinnosti stanovené ZKB [10, §4a(1) a (3)] a VKB [7, §8(4)] [38, s.5].

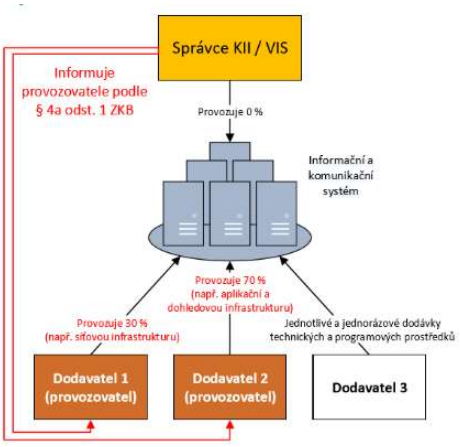
5.2.1 Provozovatel

Ke splnění zákonných požadavků nepostačuje, kvalifikuje-li správce dodavatele jako provozovatele. Je třeba, aby jej provozem systému prokazatelně pověřil.

Pro případ, že má být provoz systému v plném rozsahu svěřen dodavateli, tj. správce nebude zajišťovat funkčnost technických a programových prostředků tvořících informační a komunikační systém [10, §2(g)], ukládá ZKB povinné osobě povinnost informovat dodavatele, že se stal povinnou osobou dle tohoto zákona [10, §4a(1) a (3)].

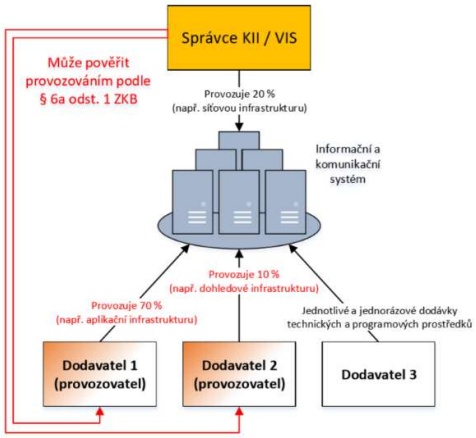
V případě, že se správce na provozu systému v částečném rozsahu podílí, informační povinnost mu ZKB neukládá. Nicméně i v tomto případě je tento postup doporučován [38, s. 5].

Výše popsaný princip ilustrují následující obrázky:



Obrázek 3 - Schéma identifikace provozovatele podle § 4a odst. 1 ZKB

Zdroj: [38, s. 13]



Obrázek 2 - Schéma identifikace provozovatele podle § 6a odst. 1 ZKB

Zdroj: [38, s. 13]

Provozovatel je povinen implementovat bezpečnostní opatření v rozsahu stanoveném VKB a za splnění této povinnosti nese přímou veřejnoprávní odpovědnost.

S ohledem na to, že provozovatel je zároveň významným dodavatelem, bude povinná osoba dále postupovat dle pravidel stanovených pro významné dodavatele s přihlédnutím ke skutečnosti, že systém řízení bezpečnosti informací musí být, ve vztahu k předmětu plnění, dodavatelem implementován v celém rozsahu.

5.2.2 Významný dodavatel

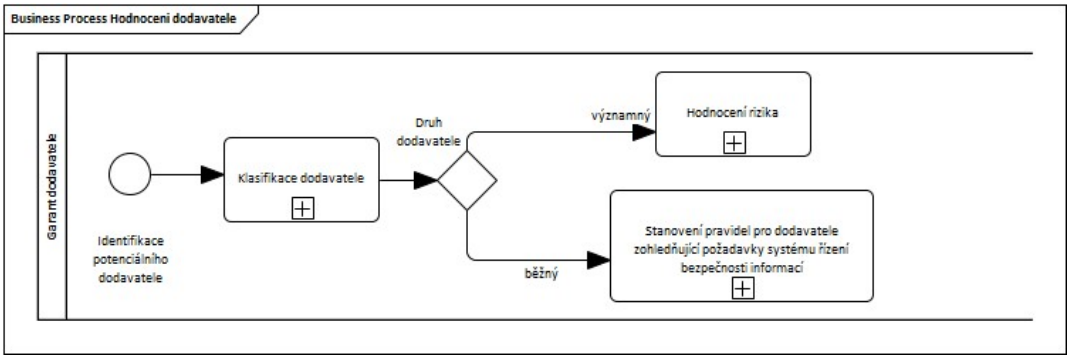
Má-li v konkrétním případě dojít k zapojení významného dodavatele, je povinná osoba povinna v rámci výběrového řízení a před uzavření smlouvy provést hodnocení rizik souvisejících s předmětem výběrového řízení [7, §8(2)(a)]. V rámci

tohoto hodnocení je vázána postupovat přiměřeně[11] dle přílohy č. 2 VKB [7, §8(2)(a)].

5.2.3 Běžný dodavatel

Má-li dojít k zapojení běžného dodavatele, je povinná osoba „pouze“ povinna stanovit pravidla pro dodavatele zohledňující požadavky systému řízení bezpečnosti informací. Neboť součástí systému řízení bezpečnost informací je též řízení rizik, lze uzavřít, že i v tomto případě bude třeba provést hodnocení rizik spojených se zapojením dodavatele, byť je možno postupovat méně formálně.

Zde popsaný proces je možno vyjádřit prostřednictvím následujícího diagramu:



Obrázek 4 - Business Process Hodnocení dodavatele

Zdroj: vlastní zpracování.

5.3 Hodnocení rizika

K hodnocení rizika je využita tabulka předkládaná v rámci této metodiky, viz. příloha č. 2 této bakalářské práce. Proces hodnocení rizika za použití navržené metodiky probíhá v 7 krocích. Jednotlivé kroky jsou v detailu popsány v této kapitole bakalářské práce.

[11] Povinnost použít právní úpravu přiměřeně znamená, že se použijí pouze určité, relevantní části odkazované právní úpravy. [37, s.2]

5.3.1 Krok první - Identifikace podpůrného aktiva

Nejprve garant aktiva specifikuje podpůrné aktivum (tj. službu dodavatele), které bude předmětem posouzení rizika. Tento údaje je do tabulky zanášen na prvním místě zejm. za účelem zvýšení přehlednosti jejího vyplňování.

5.3.2 Krok druhý – Identifikace a hodnocení primárního aktiva

Následným krokem hodnocení rizika je určení primárního aktiva, jež bude služby dodavatele, jakožto podpůrného aktiva, využívat. V souladu s dikcí platné legislativy je třeba, aby takovýmto primárním aktivem byla *„informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém.“* [7, §2(g)]

Samozřejmě je možné, že služby dodavatele bude využívat nakolik primárních aktiv. Tuto skutečnost předpokládá i navržená metodika, která umožňuje zadání neomezeného počtu primárních aktiv. Označení primárního aktiva je do tabulky hodnocení rizika zadáváno pouze pro zvýšené přehlednosti, na rozdíl od hodnocení primárního aktiva, metodika s označením primárního aktiva dále nepracuje.

V následujícím kroku vyžaduje metodika vložení hodnocení důležitosti primárního aktiva z hlediska zájmu na jeho zabezpečení. V souladu s VKB může být důležitost aktiva hodnocena jako nízká (1), střední (2), vysoká (3) nebo kritická (4). Určení hodnocení důležitosti primárního aktiva musí být provedeno předtím, než je zahájeno hodnocení požadavků na potenciálního dodavatele a jeho výpočet tedy není součástí navržené metodiky. Hodnocení primárního aktiva však neprovádí garant dodavatele, nýbrž toto hodnocení pouze přebírá, z již vytvořeného systému řízení aktiv existujícího u povinné osoby. Hodnocení primárního aktiva totiž není prováděno pouze pro účely zapojení dodavatele, ale naopak je zachováváno jednotné v rámci celého systému řízení bezpečnosti informací povinnou osobou.

Hodnocením primárního aktiva je korigováno vypočtené riziko hrozící sekundárnímu aktivu. Je-li zadáno vícero primárních aktiv, resp. vícero hodnocení, je vypočtené riziko omezeno nevyšším ze zadaných hodnocení primárních aktiv.

Dílčí část použitého vzorce je následující:

=(MIN(MAX(*sloupec_hodnocení_primárních_aktiv*); *výpočet_vázaný na_podpůrné_aktivum*))

Díky této korekci metodika předchází určení požadavku extrémního zabezpečení sekundárního aktiva, jež je využíváno primárním aktivem, pro nějž byl vyhodnocen nižší stupeň důležitosti.

5.3.3 Krok třetí – Hodnocení podpůrného aktiva

V dalším kroku je pak třeba provést hodnocení důležitosti podpůrného aktiva z hlediska zájmu na ochraně jeho důvěrnosti, dostupnosti a integrity, v každém jednotlivém případě na stupnici nízká až kritická.

V případě, že je předmět plnění dodavatele, představuje jednotný celek, je možné provést hodnocení dodávky jako celku. Skládá-li se plnění dodavatele z vícero plnění různého druhu a významu, může být účelné provést hodnocení pro tato plnění odděleně. Alternativně se, pochopitelně, nabízí možnost provedení jediného hodnocení s nastavením opatření dle plnění nejvýznamnějšího. Volba konkrétního postupu je již na uvážení a preferenci povinné osoby.

Hodnocení důvěrnosti, dostupnosti a integrity je prováděno dle níže uvedených pravidel:

5.3.3.1 Hodnocení důvěrnosti

Pro hodnocení důvěrnosti je používána následující kategorizace:

Stupeň	Definice	Vložit do tabulky
Nízká	Aktivum je veřejně přístupné nebo určeno ke zveřejnění. Narušení důvěrnosti neohrožuje zájmy povinné osoby a nebude mít negativní dopad.	1
Střední	Aktivum není veřejně přístupné a tvoří know-how povinné osoby. Jeho ochrana není vyžadována žádným právním předpisem ani smluvním ujednáním.	2
Vysoká	Aktivum není veřejně přístupné a tvoří know-how povinné osoby. Jeho ochrana je vyžadována právním předpisem nebo smluvním ujednáním (př. obchodní tajemství, osobní údaje).	3
Kritická	Aktivum není veřejně přístupné a vyžaduje nadstandardní míru ochrany nad rámec předchozí kategorie (př. strategické obchodní tajemství, zvláštní kategorie osobních údajů).	4

Tabulka 3 - Hodnocení důvěrnosti
Zdroj: [7, příloha 1]

5.3.3.2 Hodnocení dostupnosti

Pro hodnocení dostupnosti je používána následující kategorizace:

Stupeň	Definice	Vložit do tabulky
Nízká	Narušení dostupnosti není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do1 týdne).	1
Střední	Narušení dostupnosti by nemělo překročit dobu 1 pracovního dne. Dlouhodobější výpadek může ohrozit oprávněné zájmy povinné osoby.	2
Vysoká	Narušení dostupnosti by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	3
Kritická	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k závažnému ohrožení oprávněných zájmů povinné osoby.	4

Tabulka 4 - Hodnocení dostupnosti
Zdroj: [7, příloha 1]

5.3.3.3 Hodnocení integrity

Pro hodnocení integrity je používána následující kategorizace:

Stupeň	Definice	Vložit do tabulky
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje zájmy povinné osoby.	1
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	2
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	3
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	4

Tabulka 5 - Hodnocení integrity
Zdroj: [7, příloha 1]

5.3.3.4 Výpočet důležitosti podpůrného aktiva

Ze zadaného hodnocení důvěrnosti, dostupnosti a integrity je aritmetickým průměrem vypočtena důležitost podpůrného aktiva. Relevantní část výpočetního vzorce je následující[12]:

$$Důležitost\ podp.akt. = (Důvěrnost + Dostupnost + Integrita) \div 3$$

[12] Ve vzorci není použita Excel funkce PRŮMĚR, protože nejsou-li hodnoty vyplněny, zobrazuje chybovou hlášku #DĚLENÍ_NULOU!.

Touto hodnotou je následně korigována dále vypočtená úroveň rizika hrozícího poskytování plnění dodavatele. Výše uvedený vzorec je tedy rozšířen do následující podoby:

=(MIN(MAX(*sloupec_hodnocení_primárních_aktiv*); MIN(*důležitost_podp.akt.; vypočtené_riziko_hrozby*))

Tento krok je začleněn pro případ, že plnění dodavatele má z hlediska využití primárního aktiva pouze omezený význam a jeho hodnocení se tedy liší od hodnocení samotného primárního aktiva, s nímž je spojeno.

5.3.4 Krok čtvrtý – Výběr relevantních hrozeb

Dále povinná osoba pokračuje s výběrem relevantních hrozeb. Je třeba, aby v tomto kroku povinná osoba identifikovala ty hrozby, jež ohrožují plnění dodavatele anebo jsou způsobilé nepříznivě zasáhnout povinnou osobu. Výběr hrozeb je tedy prováděn primárně z perspektivy dodavatele se zřetelem k ochraně zájmů povinné osoby. Zájmy povinné osoby je třeba mít na zřeteli zejména proto, aby nedošlo k nadměrné eliminaci hrozeb.

Hrozby jsou pro zvýšení přehlednosti rozděleny dle svého primární cíle, a to na hrozby primárně zaměřené na:

- technická aktiva, tj. hardwarové a softwarové vybavení, média a dokumenty, a
- personální aktiva, tj. zaměstnance a dodavatele povinné dodavatele.

Metodika je navržena tak, aby povinné osobě dávala možnost výběr zúžit pouze na relevantní hrozby. Díky tomu je možno snáze vymezit rozsah povinností dodavatele směřující k efektivnímu zajištění bezpečnosti informačního a komunikačního systému. Tento postup nejenže snižuje administrativní zátěž procesu řízení dodavatele, ale je nejvýhodnější též z ekonomické perspektivy, neboť stanovení rozsáhlých povinností v souvislosti s poskytnutím plnění často vede k navýšení ceny dodavatelem.

5.3.4.1 Hrozby – technická aktiva

Ve vztahu k technickým aktivům metodika navrhuje hodnocení následujících hrozeb:

1	porucha zařízení nebo chybné fungování aplikačního programového vybavení
2	nedbalostní nebo úmyslné poškození, chyba použití
3	ztráta, odcizení médií nebo dokumentů
4	zneužití vnitřních prostředků (použití pro osobní účely, použití k jinému než legálnímu účelu), zneužití oprávnění
5	zneužití identity, falšování zpráv
6	zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)
7	zneužití vyměnitelných technických nosičů dat a mobilních zařízení
8	poškození dat použitím aplikačních programů na špatná data z hlediska času
9	provedení neoprávněných činností
10	zneužití oprávnění ze strany uživatelů a administrátorů
11	vzdálená špionáž
12	odposlech
13	cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik
14	instalace zákeřného kódu
15	neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění
16	dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb
17	přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie
18	porušení bezpečnostní politiky
19	chybná identifikace technických aktiv

Tabulka 6 - Identifikované hrozby, technická aktiva
Zdroj: vlastní zpracování

5.3.4.2 Hrozby – personální aktiva

Ve vztahu k personálním aktivům metodika umožňuje hodnocení následujících hrozeb:

1	nedodržení smluvního závazku ze strany subdodavatele
2	pochybení ze strany zaměstnanců (včetně trestné činnosti)
3	nedostatečná odborná úroveň nebo bezpečnostní kvalifikace
4	přechod klíčového personálního aktiva ke konkurenci
5	vyzrazení informací
6	nedostatečné předání agendy nebo ztráta know-how při odchodu zaměstnance ze společnosti
7	chybná identifikace personálních aktiv

Tabulka 7 - Identifikované hrozby, personální aktiva
Zdroj: vlastní zpracování

Pro obě skupiny aktiv je uvedena též hrozba spočívající ve špatné identifikaci chráněných aktiv. Touto hrozbou je zohledněna skutečnost, že pokud určité aktivum není zahrnuto do rozsahu, pro který je riziko hodnoceno, zůstává potenciálně nechráněno a vystaveno zneužití existujících zranitelností.

Neboť předkládaná metodika představuje pouze obecný proces, je vhodné, aby jej povinná osoba před zahájením používání validovala a eventuálně rozšířila o další jí identifikované hrozby nebo naopak, v zájmu zjednodušení, eliminovala hrozby, jež jako validní nehodnotí.

V souvislosti s rozdělením odpovědnosti mezi povinnou osobu a dodavatele, je vhodné, aby identifikaci a kvalifikaci relevantních hrozeb byla provedla nejen povinnou osobou, ale též dodavatelem. Toto doporučení je založeno na skutečnosti, že dodavatel, jakožto osoba vykonávající primární kontrolu nad službami jím poskytovanými, má, či by měl mít, ucelený přehledem o hrozbách, jež jím poskytované plnění potenciálně ohrožují. Za tímto účelem je možné dodavateli poskytnout část metodiky hodnocení rizika, a to v rozsahu identifikace a hodnocení hrozby. Je-li hodnocení prováděno pro části plnění dodavatele samostatně, pak by tento postup měl být analogicky uplatněn i pro sebe hodnocení dodavatele.

Po provedení sebe hodnocení dodavatele, povinná osoba provede komparaci výsledků sebe hodnocení dodavatele a výstupů hodnocení povinnou osobou. V případě, že se výsledky liší, požádá dodavatele o vysvětlení důvodů, proč byly identifikovány další hrozby či naopak některé hrozby byly kvalifikovány jako nerelevantní. S ohledem na validitu vysvětlení pak povinná osoba vytvoří výsledný seznam hrozeb, jež předloží dodavateli. S ohledem na skutečnost, že primární odpovědnost za zajištění systému bezpečnosti informací nese povinná osoba, se autorka této práce domnívá, že je třeba, aby povinná osoba provedla též konečné rozhodnutí o okruhu hrozeb, jež budou ve vztahu ke konkrétnímu dodavateli řízeny. Smluvně lze doporučit, aby se součástí smlouvy uzavřené mezi povinnou osobou a dodavatelem stal nejen seznam opatření, jež je dodavatel povinen zavést, ale též seznam identifikovaných hrozeb. Tento seznam by mělo doprovázet prohlášení dodavatele, že jej považuje za ucelený a není si vědom existence hrozeb v tomto

seznamu neuvedených. Zároveň by dodavatel měl být smluvně vázán průběžně provádět identifikaci hrozeb ve vztahu k jeho plnění pro povinnou osobu a povinnost povinnou osobu bezodkladně informovat, je-li identifikována hrozba neobsažená v seznamu smluvními stranami potvrzeném v době podpisu smlouvy. V případě, že dodavatel informuje povinnou osobu o nové, dosud nehodnocené hrozbě, je třeba, aby povinná osoba tuto hrozbu analyzovala a shledá-li jí validní, upravila okruh bezpečnostních opatření tak, aby tato hrozba byla efektivně adresována.

5.3.5 Krok pátý – Hodnocení závažnosti hrozby

V následném kroku je hodnocena závažnost hrozby pro plnění dodavatele. Kategorizace hrozeb je, v souladu s VKB, prováděna na stupnici od 1 do 4. Jednotlivým kategoriím je přiřazen následující význam:

Stupeň	Definice	Vložit do tabulky
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.	1
Střední	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.	2
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.	3
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.	4

Tabulka 8 - Hodnocení závažnosti hrozby
Zdroj: [7, příloha 2]

Při provádění hodnocení je třeba klást důraz na předmět plnění dodavatele pro povinnou osobu. V rámci hodnocení tedy není posuzována obecná pravděpodobnost realizace hrozby ve sféře dodavatele. Je posuzována pravděpodobnost takové realizace hrozby, jež bude mít za následek ohrožení plnění dodavatele poskytované povinné osobě či zájmů povinné osoby.

Proces hodnocení hrozby vede garant dodavatele. S ohledem na výše nastíněnou perspektivu hodnocení je třeba, aby v jejím procesu byli konzultováni garanti jednotlivých primárních aktiv, jimiž budou služby dodavatele využívány.

Hodnocení hrozby je následně zahrnuto do výpočtu rizika následujícím způsobem:

=(MIN(MAX(*sloupec_hodnocení_primárních_aktiv*); MIN(*důležitost_podp.akt.;*
(hodnocení hrozby + dopad / 2))

5.3.6 Krok šestý – Hodnocení dopadu realizace hrozby

Posledním krokem výpočtu rizika je určení pravděpodobných dopadů realizace hrozby, a to opět z perspektivy povinné osoby. Za tímto účelem metodika zapracovává metodiku doporučenou NÚKIB [9, příloha 1]. Dle této metodiky je hodnocení dopadů prováděno v 10 kategoiích, a to a) bezpečnost a zdraví osob, b) ochrana osobních údajů, c) zákonné a smluvní povinnosti, d) trestně-právní řízení, e) veřejný pořádek, f) mezinárodní vztahy, g) řízení organizace, h) ztráta důvěryhodnosti, i) finanční ztráty a j) zajišťování nezbytných služeb. Pro jednotlivé kategorie pak metodika sestavená NÚKIB stanoví následující vodítka pro určení úrovně závažnosti dopadu na stupnici 1 až 4:

5.3.6.1 Bezpečnost a zdraví osob

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Žádné vodítko.	1
Střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	2
Vysoká	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	3
Kritická	Může vést k přímému ohrožení či ztrátě života skupiny osob.	4

Tabulka 9 - Hodnocení dopadu: bezpečnost a zdraví osob
Zdroj: [9, příloha 1].

5.3.6.2 Ochrana osobních údajů

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Může způsobit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	1
Střední	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2% celkového ročního obratu - viz. čl. 83/4 GDPR).	2
Vysoká	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 20 mil. EUR nebo 4% celkového ročního obratu - viz. čl. 83/5 GDPR).	3
Kritická	Žádné vodítko.	4

Tabulka 10 - Hodnocení dopadu, ochrana osobních údajů
Zdroj: [9, příloha 1].

5.3.6.3 Zákonné a smluvní povinnosti

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Může zapříčinit porušení interních předpisů a postupů, nikoli však k porušení zákonných a smluvních povinností.	1
Střední	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo náhradě škody.	2
Vysoká	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	3
Kritická	Žádné vodítko.	4

Tabulka 11 - Hodnocení dopadu: zákonné a smluvní povinnosti
Zdroj: [9, příloha 1].

5.3.6.4 Trestně-právní řízení

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Žádné vodítko.	1
Střední	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	2
Vysoká	Může vést k narušení vyšetřování trestné činnosti nebo soudnímu řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	3
Kritická	Může vést k závažnému dlouhodobému narušení schopnosti vyšetřovat trestnou činnosti, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	4

Tabulka 12 - Hodnocení dopadu: trestně-právní řízení
Zdroj: [9, příloha 1].

5.3.6.5 Veřejný pořádek

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Žádné vodítko.	1
Střední	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	2
Vysoká	Může zapříčinit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	3
Kritická	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit pořádek s celostátními dopady.	4

Tabulka 13 - Hodnocení dopadu: veřejný pořádek
Zdroj: [9, příloha 1].

5.3.6.6 Mezinárodní vztahy

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Žádné vodítko.	1
Střední	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v 1 státě.	2
Vysoká	Může vytvářet negativní obraz ČR ve světě.	3
Kritická	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	4

Tabulka 14 - Hodnocení dopadu: mezinárodní vztahy
Zdroj: [9, příloha 1].

5.3.6.7 Řízení a provoz organizace

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Může narušit řádné řízení nebo fungování části nebo celé organizace.	1
Střední	Může omezit provádění důležitých činností organizace.	2
Vysoká	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	3

Kritická	Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti.	4

Tabulka 15 - Hodnocení dopadu: řízení a provoz organizace
Zdroj: [9, příloha 1].

5.3.6.8 Ztráta důvěryhodnosti

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Může negativně ovlivnit vztahy s jinými částmi organizace nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhého trvání.	1
Střední	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	2
Vysoká	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	3
Kritická	Může závažně a dlouhodobě ovlivni vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	4

Tabulka 16 - Hodnocení dopadu: ztráta důvěryhodnosti
Zdroj: [9, příloha 1].

5.3.6.9 Finanční ztráty

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	1
Střední	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05% a 2% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	2
Vysoká	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2% a nižším či rovným 10% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	3
Kritická	Může přímo či nepřímo vést ke ztrátám přesahujícím 10% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	4

Tabulka 17 - Hodnocení dopadu: finanční ztráty
Zdroj: [9, příloha 1].

5.3.6.10 Zajišťování nezbytných služeb

Stupeň závažnosti	Vodítko	Hodnota v tabulce
Nízká	Žádné vodítko.	1
Střední	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.	2
Vysoká	Může způsobit závažné omezení, narušení či nedostupnost nezbytných služeb pro více než 25.000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivá odvětví, viz. vyhláška č. 437/2017 Sb.)	3
Kritická	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiný závažný zásah do každodenního života postihující více než 125.000 osob.	4

Tabulka 18 - Hodnocení dopadu: zajišťování nezbytných služeb
Zdroj: [9, příloha 1].

V rámci hodnocení dopadu nejprve vyloučíme ty kategorie, v nichž dopad není předpokládán, příp. jejichž dopad nemá dosah do sféry povinné osoby. Následně je třeba pro každou z kategorií identifikovat nejhorší možné scénář, jež může nastat v případě porušení důvěrnosti, dostupnosti nebo integrity bezpečnosti informací zpracovávaných dodavatelem za účelem poskytnutí služby využívané primárním aktivem konkrétní hrozbou. *"V případě, že je pro konkrétní případ hodnocení bezpečnosti dat poplatných více oblastí dopadů (např. je relevantní 'Bezpečnost a zdraví osob' a 'Ochrana osobních údajů'), použije se pro výsledné stanovení závažnosti dopadu nejvyšší dosažená hodnota v rámci hodnocených oblastí dopadů"* [9, s. 4].

Výše uvedený vzorec pro výpočet rizika je tedy dále rozšířen do náledující podoby:

=(MIN(MAX(*sloupec_hodnocení_primárních_aktiv*); MIN(*důležitost_podp.akt.; (hodnocení hrozby + MAX(dopad) / 2*))

Obdobně jako v případě identifikace potecniálních hrozeb, je vhodným postupem provádění hodnocení dopadu sérií řízených rozhovorů s garanty primárných aktiv, které by měla služby dodavatele využívat. Tyto rozhovory by měly být vedeny garantem dodavatele. Z těchto rozhovorů by následně měly být identifikovány krizové scénáře napříč dotčenými primárními aktivy.

5.3.7 Krok sedmý - Vypočtené riziko

Riziko vypočtené shora uvedeným způsobem je následně zaokrouhleno na celá čísla. Konečná podoba vzorce pro výpočet rizika je tedy následující:

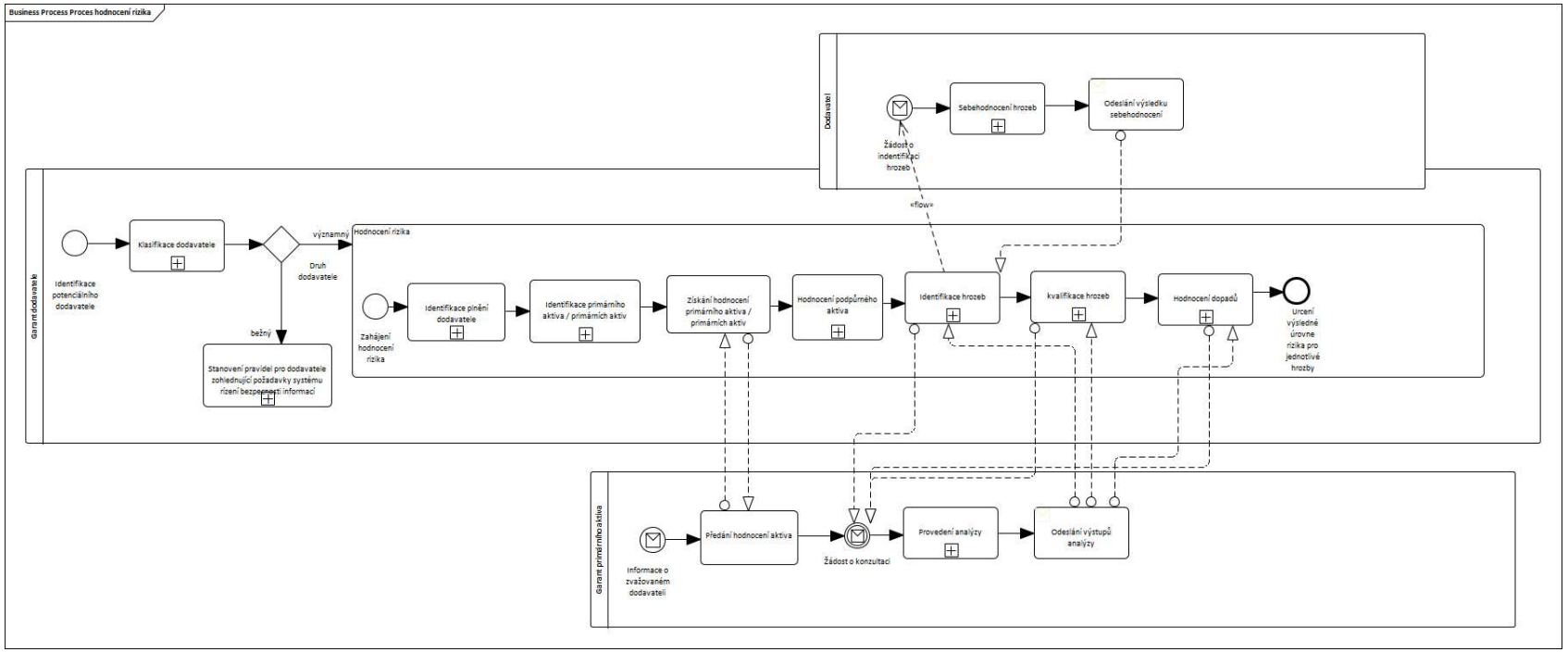
=ZAOKROUHLIT(MIN(MAX(*sloupec_hodnocení_primárních_aktiv*);
MIN(*důležitost_podp.akt.; (hodnocení hrozby + MAX(dopad) / 2*));0)

Výsledkem hodnocení rizika je tedy celé číslo v intervalu <1,4> vyjadřující úroveň závažnosti rizika, jež ohrožuje služby dodavatele využívané konkrétním primárním aktivem. Riziko je určeno zvlášť pro každou hrozbu. Jednotlivé úrovně jsou, v souladu s VKB, definovány následovně:

Stupeň významnosti	Definice	Hodnota v tabulce
Nízké	Riziko je považováno za akceptovatelné.	1
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti je riziko akceptovatelné.	2
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	3
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	4

Tabulka 19 - Hodnocení rizika
Zdroj: [7, příloha 2].

Výše popsaný proces je možno znázornit prostřednictvím následujícího diagramu:



Obrázek 5 - Business Process Hodnocení rizika
Zdroj: vlastní zpracování.

5.4 Určení vhodných bezpečnostních opatření

5.4.1 Proporcionalita bezpečnostních opatření

Pro každou z potenciálních hrozeb je následně třeba určit vhodná opatření, která buď realizaci hrozby předcházejí nebo snižují významnost jejího dopadu a tím snižují celkové riziko s hrozbou spojené. Tento postup odpovídá požadavku VKB [7, §8(2)], dle kterého povinná osoba *"v rámci uzavíraných smluvních vztahů stanoví způsoby a úrovně realizace bezpečnostních opatření"*. Tento postup je závazným způsobem předepsán pro smlouvy uzavírané s významnými dodavateli (tedy vč. smluv uzavíraných s provozovateli), ale jeho dodržování je touto prací vysoce doporučováno i ve vztahu k běžným dodavatelům.

Se znalostí rizika, jež konkrétní hrozba představuje, může povinná osoba stanovit bezpečnostní opatření proporcionálně k úrovni rizika. Povinná osoba tak není, v obavě z porušení povinností stanovených platnou legislativou, nucena vyžadovat nejvyšší stupeň zebezpeční pro ta podpůrná aktiva, či jejich části, s nimiž je spojeno riziko nízké úrovně. Zároveň metodika také poskytuje legitimní zdůvodnění kladených požadavků na dodavatele, ať již v úrovni obchodní či v úrovni obrany proti námitkám neoprávněného omezení hospodářské soutěže.

5.4.2 Určení významnosti bezpečnostních opatření

Významnost jednotlivých bezpečnostních opatření byla určena prostřednictvím analýzy zranitelností, které mohou vést k realizaci konkrétní hrozby či zvyšovat závažnost jejího dopadu. Potenciální zranitelnosti byly navrženy na základě demonstrativního seznamu uvedeného ve VKB [7, příloha 3] a i ČSN ISO/IEC 27005 [8, příloha D].

Příkladem[13] lze uvést např. hrozbu označenou jako „*Porucha zařízení nebo chybné fungování aplikačního programového vybavení*“, ve vztahu k níž, byly identifikovány následující zranitelnosti:

- zastaralost a nedostatečná údržba technického aktiva;
- nesprávná konfigurace technického aktiva;
- nejasné nebo neúplné zadání pro vývojáře, neodladěný nebo nový program;
- žádné nebo nedostatečné testování programů;
- použití nevhodného nebo nekompatibilního technického aktiva (př. aktiva obsahujícího známé chyby);

K těmto zranitelnostem byla následně přiřazena opatření upravená VKB, jež jsou relevantní z hlediska prevence hrozby či snížení jejího dopadu. Pro účely této analýzy byla opatření klasifikována z hlediska jejich působení a důležitosti do následujících úrovní:

Preventivní opatření - podpůrné, omezená aplikovatelnost
Preventivní opatření - méně významné
Preventivní opatření - stěžejní
Reaktivní opatření - stěžejní
Reaktivní opatření - méně významné nebo omezená aplikovatelnost

Tabulka 20 - Klasifikace opatření
Zdroj: vlastní zpracování.

Pro hrozbu „*Porucha zařízení nebo chybné fungování aplikačního programového vybavení*“, které je v této kapitole uváděna jako příklad[14], byla provedena následující analýza:

[13] Přehled všech zranitelností, jež byly ve vztahu k jednotlivý hrozbám zvažovány, je obsažen v metodice, jež je přílohou č. 2 této práce.
[14] Kompletní přehled všech zranitelností, jež byly pro jednotlivé hrozby analyzovány je obsažen v metodice, jež je přílohou č. 2 této práce.

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H1	zastaralost a nedostatečná údržba technického aktiva	Řízení změn	§11(1)(3)	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity	přezkoumávání dopadu změny, rozhodnutí o penetračním testování, testování zranitelností
porucha zařízení nebo chybné fungování aplikačního programového vybavení		Akvizice, vývoj a údržba	§13(f)	**Akvizice, vývoj a údržba** §13, písm. a), b), c), **Řízení změn** §11	bezpečnostní testování významných změn před uvedením do provozu, zákon požaduje jen u významných změn
		Organizační bezpečnost	§6(1)(c)(k)(g)	**Organizační bezpečnost** §6(3)(b - architekt KB), (c-garant aktiva), **Systém řízení bezpečnosti informací** §3	dostupnost zdrojů, dostatečné pravomoci nebo zdroje k požadované údržbě, dostatečná interní priorita
		Řízení provozu a komunikací	§10(1)(a)(e)(h)(f)	**Řízení aktiv, Řízení rizik, Organizační opatření** (metodiky chování uživatelů, definování komunikací)	řízení tech. zranitelnostní, sledování, plánování a řízení kapacity technického aktiva
		Řízení provozu a komunikací	§10(1)(b)	§15 **Řízení kontinuity činností**	pravidla spouštění, restartu systému, ošetření chybových stavů a mimořádných jevů; postup a zodpovědnosti dle plánu kontinuity činností či interních směrnic
		Zvládání kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	automatizovaný proces detekce kybernetických bezp. událostí a hlášení neobvyklého chování a podezření na zranitelnosti uživateli
		Zajišťování úrovně dostupnosti informací	§27	§15 **Řízení kontinuity činností**, **Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity, **Řízení prozovu a komunikací**	zajištění dostupnosti a redundance technických aktiv nezbytných pro provoz informačního a komunikačního systému, a to s ohledem na hodnocení podp. aktiv
		Průmyslové, řídící a obdobné systémy	§28 (e)(f)	**Řízení aktiv** §4, **Řízení rizik** §5	ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu - omezeno na průmyslové, řídící a obdobné specifické systémy
	nesprávná konfigurace technického aktiva	Řízení provozu a komunikací	§10(1)(a)(j)(g)	**Bezpečnost lidských zdrojů** §9(1)(a)(c)	pravidla a postupy pro instalaci technických aktiv a postupy řízení a schvalování provozních změn
		Bezpečnost lidských zdrojů	§9(1)(c)	opatření dle písm. a) a b)	bezpečnostní školení administrátorů, osob zastávajících bezpečnostní role a dodavatelů
		Akvizice, vývoj a údržba	§13(f)	opatření dle §13, písm. a), b), c)	bezpečnostní testování významných změn před uvedením do provozu, zákon požaduje jen u významných změn
		Řízení změn	§11(1)(3)	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity	přezkoumávání dopadu změny, rozhodnutí o penetračním testování, testování zranitelností
		Zvládní kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobvyklého chování a podezření na zranitelnosti uživateli
	nejasné nebo neúplné zadání pro vývojáře, neodladěný nebo nový program	Akvizice, vývoj a údržba	§13(c)(d)(f)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	stanovení bezpečnostních požadavků a jejich zahrnutí do projektu vývoje a údržby informačního a komunikačního systému
		Řízení změn	§11	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity, **Organizační bezpečnost** §6, odst. 1, písm. c), k), g), §6(3)(b - architekt KB), na to navazuje **Bezpečnost lidských zdrojů** §9(1)(d)	přezkoumávání dopadu změny, rozhodnutí o penetračním testování, testování zranitelností
	žádné nebo nedostatečné testování programů	Aplikační bezpečnost	§25(1)	**Řízení změn** §11(1), **Řízení provozu a komunikací** §10(1)(g), **Řízení aktiv** §4	provádění penetračních testů se zaměřením na důležitá aktiva
		Řízení provozu a komunikací	§10(1)(a)(g)	**Řízení aktiva** §4, **Řízení rizik** §5	postupy řízení a schvalování provozních změn
	použití nevhodného nebo nekompatibilního technického aktiva (př. aktiva obsahujícího známé chyby)	**Řízení změn**	§11(1)	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity, **Organizační bezpečnost** §6, odst. 1, písm. c), k), g), §6(3)(b - architekt KB), na to navazuje **Bezpečnost lidských zdrojů** §9(1)(d)	přezkoumávání dopadu změny, u významných změn též provedení analýzy rizik
		Řízení provozu a komunikací	§10(1)(e)(g)	**Řízení změn** §11(1)	řízení technických zranitelností, schvalování provozních změn
		Průmyslové, řídící a obdobné systémy	§28(a)	**Řízení aktiv** §4, **Řízení rizik** §5	použití technických a programových prostředků určených do specifického prostředí - omezeno na průmyslové, řídící a obdobné specifiké systémy
		Akvizice, vývoj a údržba	§13(d)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	stavenovení požadavků na technické aktivum v projektu akvizice, vývoje a údržby, zákon vyžaduje pouze u významných změn

Tabulka 21 - Příklad identifikace zranitelností pro konkrétní hrozbu
Zdroj: vlastní zpracování.

Na základě této analýzy pak bylo provedeno zobecnění, při kterém byla agregována veškerá opatření identifikovaná pro zranitelnosti přiřazené k dané hrozbě. Ve vztahu k agregovaným opatřením pak byla kvalifikována jejich významnost z hlediska prevence či snížení dopadů hrozby.

Určení významnosti opatření bylo provedeno ve třech krocích[15]:

1. Ohodnocení opatření ve vztahu k jednotlivým zranitelnostem dle následujícího pravidla:

Význam opatření	kvalifikace
Preventivní opatření - podpůrné, omezená aplikovatelnost	**1**
Preventivní opatření - méně významné	**2**
Preventivní opatření - stěžejní	**3**
Reaktivní opatření - stěžejní	**3**
Reaktivní opatření - méně významné nebo omezená aplikovatelnost	**2**

Tabulka 22 - Klasifikace opatření
Zdroj: vlastní zpracování

2. Tyto hodnoty byly následně pro každé opatření sečteny a převedeny na stupnici 1 až 4.
3. V konečném kroku muselo dojít k úpravě významu opatření dle uvážení autorky. Tento krok byl nezbytný, neboť jednotlivé zranitelnosti pokrývají různé množství případů a liší se tedy svou závažností. V rámci této závěrečné korekce byla přidána pátá úroveň důležitosti opatření. Do 5. Úrovně byla zařazena ta opatření, jejich aplikovaltenost je omezena na specifické situace nebo systémy a v obecné rovině tedy není možné jejich význam určit.

15

Ve vztahu k příkladem uváděné hrozbě *Porucha zařízení nebo chybné fungování aplikačního programového vybavení* bylo provedeno následující hodnocení:

Hrozba	Kategorie opatření	Dle mapovací tabulky	Převod na stupnici 1-4	Výsledná hodnota, vč. korekce	Stručný popis
Porucha zařízení nebo chybné fungování aplikačního programového vybavení	Průmyslové, řídící a obdobné systémy	2	1	5	Ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu. Omezeno na průmyslové, řídící a obdobné specifické systémy.
	Akvizice, vývoj a údržba	4	1	5	V souvislosti s plánovanou akvizicí a údržbou řídí významné změny, zahrne bezpečnostní požadavky do projektu, provádí bezpečností testování před jejich zavedením do provozu.
	Řízení provozu a komunikací	14	4	4	Stanoví práva a povinnosti administrátorů a uživatelů, řídí technické zranitelnosti, řídí a schvaluje provozní změny, sleduje a plánuje kapacity lidských a technických zdrojů, zajistí kontakt na osoby systémové a technické podpory.
	Zvládání kybernetických událostí	5	2	3	Automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobvyklého chování a podezření na zranitelnosti uživateli.
	Řízení změn	10	3	3	Přezkoumání možných dopadů změny, určení významných změn, rozhodnutí o provedení testování zranitelností.
	Zajišťování úrovně dostupnosti informací	3	1	2	Zajistí dostupnost a redundanci technických aktiv nezbytných pro provoz informačního a komunikačního systému a to s ohledem na hodnocení podpůrných aktiv.
	Organizační bezpečnost	3	1	2	Zajistí dostupnost zdrojů, dostatečné pravomoci nebo zdroje k požadované údržbě, dostatečnou interní prioritu.
	Bezpečnost lidských zdrojů	3	1	2	Bezpečnostní školení administrátorů, osob zastávajících bezpečnostní role a dodavatelů.
	Aplikační bezpečnost	1	1	1	Penetrační testy před uvedením významné změny do provozu. Omezeno na důležitá aktiva a významné změny.

Tabulka 23 - Klasifikace opatření pro konkrétní hrozbu
Zdroj: vlastní zpracování.

Výše uvedený postup byl proveden pro všechny identifikované hrozby. Výsledkem jsou pak následující tabulky, v nichž jsou ke každé hrozbě přiřazena preventivní či reaktivní opatření, která jsou zároveň ohodnocena z hlediska jejich významnosti.

TECHNICKÁ AKTIVA	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																												
	ORGANIZAČNÍ OPATŘENÍ														TECHNICKÁ OPATŘENÍ														
HROZBA	Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídicí a obdobné systémy
porucha zařízení nebo chybné fungování aplikačního prog. Vybavení				2			2	4	3		5	3											1		2	5
nedbalostní nebo úmyslné poškození, chyba použití							4					2			3			3	3	2	2	2				5
ztráta, odcizení médií nebo dokumentů		2					4	2				3			3	1	4	4	3	3	3	3	1	2		5
zneužití vnitřních prostředků		4		4			4	5		3							3			2	2	2	1			
zneužití identity, falšování zpráv							4			4							4						2			
zničení nebo poškození zařízení v důsledku změn prostředí													3		4											
zneužití vyměnitelných technických nosičů dat		3					4			2									2							
poškození dat použitím aplikačních programů na špatná data z hlediska času																				4		4				
provedení neoprávněných činností, tj. provedení činností k nimž uživatel nemá oprávnění				4			4	4								1	4	3		2		2	2			5
zneužití oprávnění ze strany uživatelů a administrátorů				4			4	4		4								2								
vzdálená špionáž																3	4							2		
odposlech																4								2		
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik		1					4			2						3	3									
instalace zákeřného kódu		1					4	4	5	1	5	2				3			4		2	2				
neoprávněné užití technického aktiva (licenční a smluvní podmínky)				4		4																				
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb						4		4				3	3			2				3		3			3	5
přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie						4		4				2	2			2				2		2				5
porušení bezpečnostní politiky							4					1		1												
chybná identifikace technických aktiv	4																									

Tabulka 24 - Souhrnná klasifikace opatření: technická aktiva
Zdroj: vlastní zpracování

PERSONÁLNÍ AKTIVA	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																												
	ORGANIZAČNÍ OPATŘENÍ														TECHNICKÁ OPATŘENÍ													
HROZBA	Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídicí a obdobné systémy
nedodržení smluvního závazku ze strany dodavatele				3		4	3																					
pochybení ze strany zaměstnanců (včetně trestné činnosti)				4			4																					
nedostatečná odborná úroveň					2		4																					
přechod klíčového personálního aktiva ke konkurenci				4																								
vyzrazení informací (porušení smluvní či zákonné povinnosti mlčenlivosti)				4			4	1																				
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance / dodavatele				4			4																					
chybná identifikace personálních aktiv	4																											

Tabulka 25 - Souhrnná klasifikace opatření: personální aktiva
Zdroj: vlastní zpracování

5.4.3 Určení okruhu bezpečnostních opatření

Jak je vidět z hodnocení výše, jednotlivá bezpečnostních opatření jsou kategorizována na stupnici 1 až 5. Jednotlivým úrovním jsou přiřazeny následující definice a doporučení pro implementaci:

Stupeň významnosti	Definice	Hodnota v tabulce
Nízký	Význam opatření je z hlediska předcházení realizaci hrozby nebo snižování jejích dopadů spíše podružný. V případě, že vyhodnocený stupeň rizika je 1 až 3, opatření není třeba implementovat.	1
Střední	Význam opatření je z hlediska předcházení realizace hrozby nebo snižování jejích dopadů střední. V případě, že vyhodnocený stupeň rizika je 1 nebo 2, opatření není třeba implementovat.	2
Vysoký	Význam opatření je z hlediska předcházení realizace hrozby nebo snižování jejích dopadů vysoký. V případě, že vyhodnocený stupeň rizika je 1, opatření není třeba implementovat.	3
Kritický	Opatření je třeba implementovat vždy, je považováno za minimální zabezpečení.	4
Podmíněný	Opatření je omezeno na specifické systémy či specifické situace, jeho aplikovatelnost je třeba vyhodnotit s přihlédnutím k hodnoceným aktivům a zvažovaným činnostem. Význam opatření nemůže být vyhodnocen v obecné rovině.	5

Tabulka 26 - Hodnocení významu opatření
Zdroj: vlastní zpracování

V návaznosti na provedené hodnocení rizika tedy povinná osoba volí vhodná bezpečnostní opatření k jeho snížení. Primárně přitom vyžaduje, aby dodavatelem byly implementována opatření, jejichž význam je kritický. V případě, že je s danou hrozbou spojeno vysoké až kritické riziko, rozšiřuje okruh opatření též na opatření, jejichž význam je střední či nízký.

Zároveň je nutno upozornit, že nároky jednotlivých opatření mohou být naplněny technickými řešeními různé úrovně složitosti a automatizace. Se zvyšujícím se rizikem by tedy povinná osoba měla klást důraz na to, aby zejm. opatření s kritickou a vysokou úrovní důležitosti byla provedena způsobem odpovídajícím aktuálnímu stavu techniky.

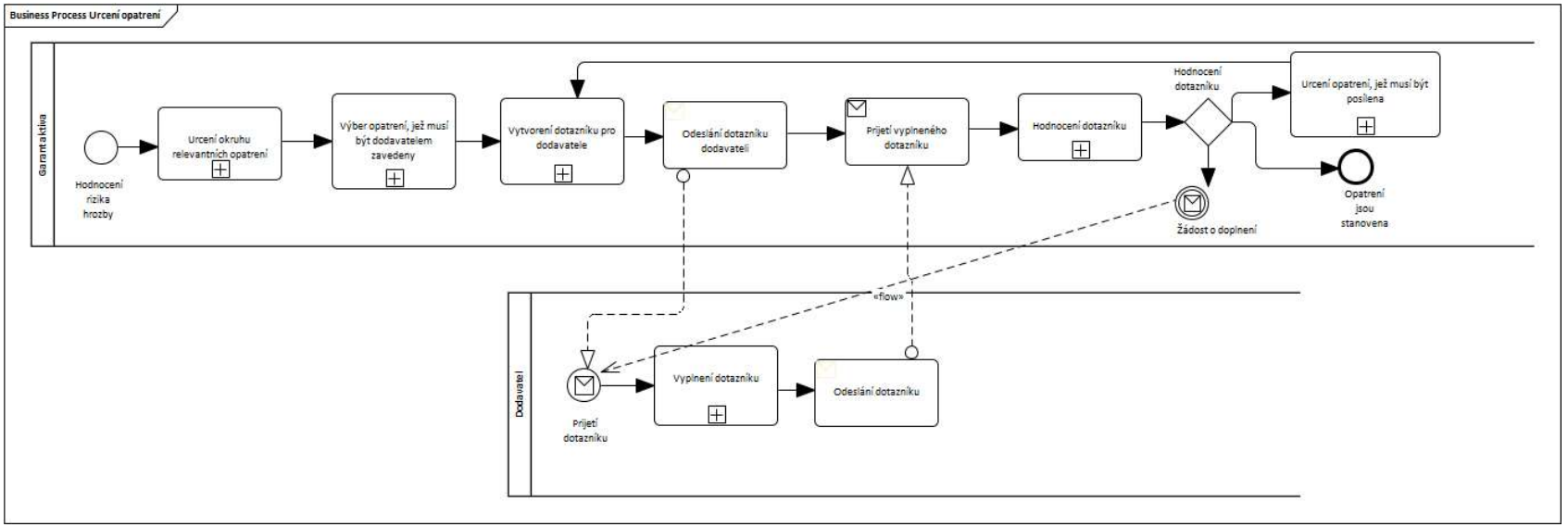
Poté, co byla identifikována relevantní opatření tedy povinná osoba vyzve potenciálního dodavatele, aby doložil, jakým konkrétním způsobem takto opatření

zavedl či se zavazuje zavést před zahájením poskytování služby. K tomuto účelu lze použít jednoduchý dotazník založený na vymezení těchto opatření ve VKB [7].

Po předložení způsobu zavedení bezpečnostních opatření potenciálním dodavatelem povinná osoba provede hodnocení, zda navržený způsob považuje za dostatečný či nikoli. V případě, že dodavatelem poskytnutý popis není dostatečným podkladem pro provedení hodnocení nebo způsob implementace bezpečnostních opatření povinná osoba neshledá dostatečným, vyzve dodavatele k doplnění informací či posílení bezpečnostních opatření. V opačném případě povinná osoba může dodavatele autorizovat jako kvalifikovaného pro účely poskytnutí daného plnění.

Z hlediska smluvního je pak vhodné, aby stanovený rozsah bezpečnostních opatření byl přílohou smlouvy s dodavatelem, včetně způsobu jejich provedení. Smlouvy uzavírané na dobu neurčitou či na dobu přesahující dobu 2 let by pak měly stanovit pravidelné revize způsobu provedení bezpečnostních opatření tak, aby vždy odpovídaly aktuálnímu stavu techniky.

Výše popsaný proces je možno znázornit prostřednictvím následujícího diagramu:



Obrázek 6 - Business Process Určení opatření

Zdroj: vlastní zpracování.

6 Příklad použití navržené metodiky

V této kapitole bakalářské práce je demonstrováno praktické použití navržené metodiky hodnocení dodavatele. Cílem hodnocení je stanovení rozsahu bezpečnostních opatření, jejichž implementace dodavatelem je nezbytná pro zajištění bezpečnosti informačního a komunikačního systému povinné osoby a naplnění požadavků platné legislativy.

Pro účely ilustrativního příkladu předpokládáme, že dodavatel byl kategorizován jako významný.

Proces hodnocení dodavatele a určení bezpečnostních opatření je popisován v jednotlivých krocích, které korespondují s kroky popsanými v předchozí kapitole této bakalářské práce. Kompletní metodika hodnocení je připojena jako příloha č. 3 této práce.

6.1 Hodnocení rizika

6.1.1 Krok první - Identifikace podpůrného aktiva

Předmětem hodnocení jsou služby dodavatele v oblasti zakázkového vývoje software. Příklad předpokládá, že součástí služby není podpora a údržba dodaného software, ani jeho provoz v produkčním prostředí. Ilustrativní případ nepředpokládá přístup dodavatele na produkční prostředí spravované povinnou osobou. Ilustrativní případ dále nepředpokládá předání osobních údajů spravovaných povinnou osobou dodavateli.

6.1.2 Krok druhý – Identifikace a hodnocení primárního aktiva

Byla identifkována dvě primární aktiva, jimiž budou služby dodavatele využívány (pro účely příkladu nejsou blíže specifikována). Důležitost dotčených primárních aktiv byla ohodnocena jako nízká (1) a vysoká (3).

Vypočtené riziko plynoucí ze zapojení dodavatele bude tedy korigováno na úroveň 3 (vysoká).

6.1.3 Krok třetí – Hodnocení podpůrného aktiva

6.1.3.1 Důvěrnost

Důležitost zachování důvěrnosti služeb dodavatele ohodnotil garant dodavatele jako kritickou, tj. úrovní 4. Je přitom zjevně nelogické, aby byl zájem na ochraně podpůrného aktiva vyšší než zájem na ochraně primární aktiva. Předkládaný příklad tedy demonstruje situaci, kdy subjektivní hodnocení garanta dodavatele neodpovídá hodnocení aktiv v kontextu organizace existující u povinné osoby. Subjektivně tedy garant dodavatele hodnotí narušení důvěrnosti (př. obava z vyzrazení aplikační logiky, business zadání) závažněji, než bude jeho skutečný dopad v kontextu organizace.

6.1.3.2 Dostupnost

Důležitost dostupnosti služeb dodavatele ohodnotil garant dodavatele jako nízkou, tj. úrovní 1. Lze předpokládat, že důvodem pro hodnocení důležitosti dostupnosti služby jako nízké, je skutečnost, že její součástí není podpora ani údržba systému v produkčním, tj. živém, prostředí. Úkolem dodavatele tedy nebude řešení incidentů produkčního prostředí.

6.1.3.3 Integrita

Důležitost integrity služeb dodavatele ohodnotil garant dodavatele jako vysokou, tj. úrovní 3. Důvodem pro hodnocení důležitosti integrity služeb jako vysoké, může být obava z korektního zpracovávání dat dodavatelem vytvořeným software.

6.1.3.4 Celkové hodnocení důležitosti podpůrného aktiva

Na základě výše provedeného ohodnocení podpůrného aktiva byla vypočtena jeho důležitost. V souladu s obecným popisem obsaženým v předchozí kapitole, byla důležitost aktiva vypočtena jako aritmetický průměr úrovně dostupnosti, důvěrnosti a integrity. Výsledná důležitost služeb dodavatele je takto ohodnocena jako vysoká, tj. úrovní 3.

Vzhledem k tomu, že celková důležitost služeb dodavatele nepřekračuje důležitost nejvýznamnějšího dotčeného primárního aktiva, nebude význam rizik dále uměle snižován pod tuto hodnotu.

6.1.4 Krok čtvrtý – Výběr relevantních hrozeb

V následujícím kroku byly vyloučeny hrozby, které neohrožují schopnost dodavatele poskytnout sjednané plnění. Je vhodné poznamenat, že vyloučení těchto hrozeb neznamená, že nejsou přítomné v organizaci dodavatele. Předpokladem pro vyloučení hrozby je domněnka, že i v případě realizace hrozby ve sféře dodavatele, nevznikne dopad na plnění poskytované dodavatelem povinné osobě.

Jako nerelevantní bylo označeny následující hrozby:

- zneužití vnitřních prostředků (použití pro osobní účely, použití k jinému než legálnímu účelu), zneužití oprávnění;
- zneužití identity, falšování zpráv;
- poškození dat použitím aplikačních programů na špatná data z hlediska času;
- provedení neoprávněných činností;
- přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie;

Tyto hrozby byly vyloučeny z dalšího hodnocení. To znamená, že bezpečnostní opatření, která budou v následujícím postupu identifikována, proti těmto hrozbám neposkytují ochranu.

6.1.5 Krok pátý – Hodnocení závažnosti hrozby

Hrozby, jež byly nebyly z hodnocení v předchozím kroku eliminovány, byly následně ohodnoceny na stupnici 1 až 4 z hlediska pravděpodobnosti jejich realizace.

V tabulce níže je uvedeno hodnocení jednotlivých hrozeb, včetně stručného zdůvodnění určeného stupně závažnosti hrozby, jakož i příkladu realizace konkrétní hrozby.

Hrozba	**Stupeň**	**Pravděpodobnost, zdůvodnění, příklad realizace hrozby**
porucha zařízení nebo chybné fungování aplikačního programového vybavení	4	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc. Pravděpodobnost byla určena s ohledem na skutečnost, že zakázkový vývoj software je náchylný na výskyt chyb. *Př. kritická vada vyvíjeného software, vada produktu třetí strany integrovaného do dodávaného software*
nedbalostní nebo úmyslné poškození, chyba použití	1	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let. Pravděpodobnost byla určena s ohledem na to, že předmětem posouzení je služba, nikoli produkt. Poškození fyzického zařízení v takovém rozsahu, aby ohrozilo plnění dodavatele není pravděpodobné. *Př. poškození hardwarového vybavení, na němž je prováděn vývoj*

ztráta, odcizení médií nebo dokumentů	2	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let. Pravděpodobnost byla určena s ohledem na zkušenosti hodnotící osoby ohledně četnosti výskytu těchto událostí. *Př. ztráta notebooku, na němž je uloženo zadání*
zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)	1	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let. Jelikož se pracoviště dodavatele nenachází v záplavové oblasti a zařízení využívaná pro poskytování plnění nejsou vysoce citlivá na změnu prostředí, byla hrozba vyhodnocena jako nízká. *Př. požár v provozovně dodavatele*
zneužití vyměnitelných technických nosičů dat a mobilních zařízení	2	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let. Pravděpodobnost byla určena na základě zkušeností hodnotící osoby ohledně frekvence její realizace. *Př. pořízení neoprávněných kopií, získání vyřazeného přenosového média*
zneužití oprávnění ze strany uživatelů a administrátorů	2	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let. Pravděpodobnost byla stanovena na základě zkušeností hodnotící osoby ohledně frekvence její realizace. *Př. smazání nebo pozměnění vyvíjeného software, vytvoření backdoor ve vyvíjeném software*
vzdálená špionáž	1	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let. Hrozba neohrožuje plnění, ale ohrožuje zájmy povinné osoby. Pravděpodobnost byla určena dle úvahy hodnotící osoby ohledně jejího výskytu. *Př. vzdálená špionáž dodavatele za účelem získání informací vztahujících se k povinné osobě*
odposlech	1	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let. Hrozba neohrožuje plnění, ale ohrožuje zájmy povinné osoby. *Př. odposlech dodavatele za účelem získání informací vztahujících se k povinné osobě* Pravděpodobnost byla určena dle úvahy hodnotící osoby ohledně jejího výskytu.
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	2	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let. Pravděpodobnost byla určena dle úvahy hodnotící osoby ohledně jejího výskytu. *Př. ovlivňování nebo nátlak na dodavatele za účelem získání informací vztahujících se k povinné osobě*
instalace zákeřného kódu	3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku. Pravděpodobnost byla stanovena na základě zkušeností hodnotící osoby ohledně frekvence její realizace. *Př. instalace ransomware v síti dodavatele*
neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	4	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc. Vzhledem k tomu, že software je kvalifikován jako autorské dílo, byla pravděpodobnost hrozby stanovena jako kritická. *Př. neoprávněné kopírování částí zdrojového kódu*
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let. Pravděpodobnost hrozby byla stanovena s ohledem na statistický výskyt dlouhodobých výpadků v oblasti, kde je umístěna provozovna dodavatele, v níž bude plnění prováděno. *Př. dlouhodobé výpadky v síti internet nebo výpadky elektřiny*
porušení bezpečnostní politiky	3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku. Pravděpodobnost byla stanovena na základě zkušeností hodnotící osoby ohledně frekvence její realizace. *Př. nedostatečné nastavení bezpečnostní pravidel či jejich komunikace*
chybná identifikace technických aktiv	2	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let. Pravděpodobnost je stanovena s ohledem na frekvenci změny rozsahu aktiv využívaných při plnění dodavatele. *Př. určitá oblast je zcela nechráněna, neboť nebyla vyhodnocena jako podstatná*

nedodržení smluvního závazku ze strany subdodavatele	3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku. Pravděpodobnost je stanovena s ohledem na frekvenci změny rozsahu aktiv využívaných při plnění dodavatele. *Př. nedodání funkcionality ve stanoveném termínu*
pochybení ze strany zaměstnanců (včetně trestné činnosti)	4	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc. S ohledem na to, že zakázkový vývoj software je založen na činnosti zaměstnanců, byla pravděpodobnost hrozby stanovena jako vysoká. *Př. nesprávná konfigurace komponenty*
nedostatečná odborná úroveň nebo bezpečnostní kvalifikace	4	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc. Pravděpodobnost hrozby je stanovena s ohledem na potřebu využití odbornosti na každodenní bázi. *Př. nevhodný návrh architektury dodávaného software*
přechod klíčového personálního aktiva ke konkurenci	3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku. Pravděpodobnost hrozby je stanovena s ohledem na vysokou fluktuaci zaměstnanců v oblasti IT. *Př. odchod Architekta řešení*
vyzrazení informací	4	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc. Pravděpodobnost hrozby je stanovena s ohledem na obecnou tendenci osob sdílet informace. *Př. vyzrazení informací o způsobu zpracování dat vyvíjeným software, o existujících zranitelnostech*
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance ze společnosti	3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku. Pravděpodobnost je stanovena s ohledem na předpokládanou fluktuaci u dodavatele. *Př. nepředání dokumentace či informací o stavu projektu*
chybná identifikace personálních aktiv	2	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let. Pravděpodobnost je stanovena s ohledem na frekvenci změny rozsahu aktiv využívaných při plnění dodavatele. *Př. pro určitou kategorii nejsou stanovena dostatečná procesní pravidla*

Tabulka 27 - Hrozby: Zakázkový vývoj software
Zdroj: vlastní zpracování

6.1.6 Krok šestý – Hodnocení dopadu realizace hrozby

V rámci hodnocení dopadu byly nejprve identifikovány oblasti, jejich zasažení hroznou je vyloučeno, resp. není předpokládáno. Konkrétně se jedná o následující oblasti:

- Bezpečnost a zdraví osob,
- Trestně-právní řízení,
- Veřejný pořádek,
- Mezinárodní vztahy,
- Zajišťování základních služeb,
- Řízení organizace,

Dopad pro tyto oblasti nebyl vyhodnocován a pro účely dalšího vyplňování byly tyto sloupce skryty.

Jak je zmíněno výše, do konečného výpočtu vstupuje vždy nejvyšší identifikovaná úroveň dopadu, a to napříč všemi zvažovanými oblastmi. Vzhledem k tomu, že z hlediska výpočtu, je v oblasti dopadu hledána nejvyšší identifikovaná úroveň dopadu, nikoli hodnota průměrná, neovlivňuje vyloučení, nebo naopak zahrnutí, určitých oblastí výslednou vypočtenou hodnotu rizika.

Je vhodné upozornit, že oblast ochrany osobních údajů nebyla z posuzovaných oblastí vyloučena. A to navzdory tomu, že se nepředpokládá předání osobních údajů pro účely vývoje software ani přístup dodavatele na produkční prostředí. Dopadová oblast ochrany osobních údajů nebyla vyloučena proto, že osobních údaje budou zpracovávány prostřednictvím dodavatelem vytvořeného software.

Ve většině posuzovaných oblastí byla identifikována nízká úroveň dopadu realizace hrozby. Jiná, než nízká úroveň závažnosti dopadu byla vyhodnocena v následujících oblastech:

6.1.6.1 Porucha zařízení nebo chybné fungování aplikačního programového vybavení

Oblast	Úroveň	Důvod
Zákonné a smluvní povinnosti	2	V případě chybného fungování dodaného software, povinná osoba nebude schopna plnit uzavřené smlouvy. V důsledku toho může jejím zákazníkům vzniknout škoda, která může být vynucována v občanskoprávních řízeních.
Ochrana osobních údajů	2	V případě nasazení vadného software hrozí porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2% celkového ročního obratu - viz. čl. 83/4 GDPR).
Ztráta důvěryhodnosti	3	Nasazení vadného software do produkčního prostředí může vést k celostátní negativní publicitě.
Finanční ztráty	3	Potenciální škoda vzniklá užitím vadného software (ztráta budoucích obchodů, ukončení stávajících smluv, náhrada škody), je ohodnocena na přibližně 8% ročního obratu povinné osoby.

Tabulka 28 - Dopad v oblasti porucha zařízení nebo chybné fungování aplikačního programového vybavení
Zdroj: vlastní zpracování

6.1.6.2 Zneužití oprávnění ze strany uživatelů či administrátorů

Oblast	Úroveň	Důvod
Ochrana osobních údajů	2	Vytvořením backdoor v dodávaném software hrozí porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2% celkového ročního obratu - viz. čl. 83/4 GDPR).

Tabulka 29 - Dopad v oblasti zneužití oprávnění ze strany uživatelů či administrátorů
Zdroj: vlastní zpracování

6.1.6.3 Instalace zákeřného kódu

Oblast	Úroveň	Důvod
Zákonné a smluvní povinnosti	2	V případě chybného fungování dodaného software, povinná osoba nebude schopna plnit uzavřené smlouvy. Důsledku toho může jejím zákazníkům vzniknout škoda, která může být vynucována v občanskoprávních řízeních.
Ochrana osobních údajů	2	V případě nasazení vadného software hrozí porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2% celkového ročního obratu - viz. čl. 83/4 GDPR).
Finanční ztráty	3	Potenciální škoda vzniklá užitím vadného software (ztráta budoucích obchodů, ukončení stávajících smluv, náhrada škody), je ohodnocena na přibližně 8% ročního obratu povinné osoby.

Tabulka 30 - Dopad v oblasti instalace zákeřného kódu
Zdroj: vlastní zpracování

Za povšimnutí nepochybně stojí, že dopady jsou podobné jeho v případě hrozby *porucha zařízení* nebo *chybné fungování aplikačního programového vybavení*. Dopad v oblasti ztráta důvěryhodnosti, byl vyhodnocen jako nízký, a to proto, že porušení zabezpečení v důsledku jednání třetí strany je zpravidla veřejností přijímáno snáze než nasazení vadného software povinnou osobou.

6.1.7 Krok sedmý - Vypočtené riziko

Pro každou ze zvažovaných oblastí bylo vypočteno riziko, a to dle následujícího vzorce:

ZAOKROUHLIT(MIN(MAX(3); MIN(3*; (hodnocení hrozby + MAX(dopad) / 2*));0)

Pro jednotlivé hrozby byly vypočteny níže uvedené úrovně rizika:

Hrozba	Riziko
porucha zařízení nebo chybné fungování aplikačního programového vybavení	3
nedbalostní nebo úmyslné poškození, chyba použití	1
ztráta, odcizení médií nebo dokumentů	3
zneužití vnitřních prostředků (použití pro osobní účely, použití k jinému než legálnímu účelu), zneužití oprávnění	0
zneužití identity, falšování zpráv	0
zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)	1
zneužití vyměnitelných technických nosičů dat a mobilních zařízení	3
poškození dat	0
provedení neoprávněných činností	0
zneužití oprávnění ze strany uživatelů[5] a administrátorů	3
vzdálená špionáž	1
odposlech	1
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	2
instalace zákeřného kódu	3

neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	3
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2
přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	0
porušení bezpečnostní politiky	2
chybná identifikace technických aktiv	2
nedodržení smluvního závazku ze strany subdodavatele	2
pochybení ze strany zaměstnanců (včetně trestné činnosti)	3
nedostatečná odborná úroveň nebo bezpečnostní kvalifikace	3
přechod klíčového personálního aktiva ke konkurenci	2
vyzrazení informací	3
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance ze společnosti	3
chybná identifikace personálních aktiv	2

Tabulka 31 - Vypočtené riziko
Zdroj: vlastní zpracování

6.2 Určení bezpečnostních opatření

6.2.1 Určení okruhu proporcionálních bezpečnostních opatření

Na základě komparace souhrnných mapovacích tabulek s výsledkem hodnocení hrozeb byl určen okruh bezpečnostních opatření, jejichž implementace je nezbytná k zajištění bezpečnosti informací při zapojení dodavatele. Zároveň byla, s ohledem na předmět činnosti dodavatele, vyhodnocena významnost tzv. „podmíněných“ bezpečnostních opatření.

Nezbytná bezpečnostní opatření byla určena dle vypočtené úrovně rizika a významu opatření z hlediska prevence realizace hrozby a/nebo mitigace dopadů její realizace:

- Vzhledem k tomu, že s žádnou ze zvažovaných hrozeb není spojeno riziko kritické (4) úrovně, došlo v rámci tohoto procesu např. k vyloučení veškerých opatření, jejichž preventivní či mitigační význam je hodnocen jako nízký (1).
- V případě, že úroveň rizika byla pro konkrétní hrozbu vyhodnocena jako střední (2), byla vyloučena též opatření, jejichž význam je z hlediska prevence hrozby či snížení jejích dopadů střední (2).
- V případě, že úroveň rizika byla pro konkrétní hrozbu vyhodnocena jako nízká (1), byla vyloučena nejen opatření, jejichž význam je z hlediska prevence hrozby či snížení jejích dopadů je nízký (1), střední (2), ale též opatření, jejichž význam je vysoký (3). Pro tyto hrozby tedy zůstaly zachována pouze opatření, jejichž význam je z kritický (4).

Výsledná potřebná struktura bezpečnostních opatření pro technická a personální aktiva je následující:

TECHNICKÁ AKTIVA	Riziko	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																												
		ORGANIZAČNÍ OPATŘENÍ														TECHNICKÁ OPATŘENÍ														
HROZBA		Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídicí a obdobné systémy
porucha zařízení nebo chybné fungování aplikačního prog. Vybavení	3				2			2	4	3		4	3												2		
nedbalostní nebo úmyslné poškození, chyba použití	1							4																				
ztráta, odcizení médií nebo dokumentů	3		2					4	2				3			3		4	4	3	3	3	3		2			
zničení nebo poškození zařízení v důsledku změn prostředí	1															4												
zneužití vyměnitelných technických nosičů dat	3		3					4			2									2								
zneužití oprávnění ze strany uživatelů a administrátorů	3				4			4	4		4								2									
vzdálená špionáž	1																	4										
odposlech	1																4											
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	2							4									3	3										
instalace zákeřného kódu	3							4	4	2		4	2				3			4		2	2					
neoprávněné užití technického aktiva (licenční a smluvní podmínky)	3				4		4																					
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2						4		4				3	3							3		3			3		
porušení bezpečnostní politiky	2							4																				
chybná identifikace technických aktiv	2	4																										

Tabulka 32 - Opatření k implementaci, technická aktiva
Zdroj: vlastní zpracování

PERSONÁLNÍ AKTIVA	Riziko	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																												
		ORGANIZAČNÍ OPATŘENÍ															TECHNICKÁ OPATŘENÍ													
HROZBA		Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvisice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činnosti	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídicí a obdobné systémy
nedodržení smluvního závazku ze strany dodavatele	2				3		4	3																					
pochybení ze strany zaměstnanců (včetně trestné činnosti)	3				4			4																					
nedostatečná odborná úroveň	3					2		4																					
přechod klíčového personálního aktiva ke konkurenci	2				4																								
vyzrazení informací (porušení smluvní či zákonné povinnosti mlčenlivosti)	3				4			4																					
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance / dodavatele	3				4			4																					
chybná identifikace personálních aktiv	2	4																											

Tabulka 33 - Opatření k implementaci, personální aktiva
Zdroj: vlastní zpracování

6.2.2 Návrh opatření k implementaci

Na základě okruhu identifikovaných opatření a části metodiky, v níž je provedeno hodnocení významnosti jednotlivých bezpečnostních opatření, s přihlédnutím ke znění relevantního ustanovení ustanovení VKB, lze snadno sestavit následující seznam konkrétních opatření, jejichž implementaci dodavatelem je třeba vyžadovat.

ORGANIZAČNÍ OPATŘENÍ			
Kategorie opatření	**Potřebná úroveň**	**Hrozba**	**Požadavky na dodavatele**
Systém řízení bezpečnosti informací	4	H19	Pravidelně vyhodnocuje organizační části a aktiva, která jsou využívaná k poskytování plnění odběratelské společnosti.
Organizační bezpečnost	4	H15	Stanovil pravidla pro užití statků chráněných právy duševního vlastnictví.
			Vede evidenci platných licencí, vč. data jejich expirace.
	4	H10	Stanovil pravidla pro určení administrátorů a osob zastávajících bezpečnostní role.
	4	H21	Stanovil pravidla pro výběr zaměstnanců.
			Ověřuje kvalifikaci uchazečů o zaměstnání (př. testování).
			Ověřuje reference předchozích zaměstnavatelů uchazečů o zaměstnání.
			Zaměstnanci mají jasně definovanou pracovní náplň a zodpovědnosti.
	4	H23	V pracovních smlouvách klíčových zaměstnanců a sub-dodavatelů je upravena konkurenční doložka zakazující práci pro subjekt v konkurenčním postavení k dodavateli po určitou dobu po skončení smluvního vztahu s dodavatelem.
	4	H24	Zaměstnanci a dodavatelé jsou vázáni zákonnou nebo smluvní povinností mlčenlivosti.
			Zaměstnanci a dodavatelé byli poučeni o důvěrnosti zpracovávaných informací.
	4	H25	Sub-dodavatelé jsou smluvně vázáni poskytnout podporu dodavateli při ukončení spolupráce.
			Zajišťuje předání práce zaměstnancem při ukončení pracovního poměru.
			Odcházející zaměstnanec je povinen zaškolit zaměstnance, kterému jsou předávány úkoly odcházejícího zaměstnance.
	3	H20	Stanovil pravidla pro výběr dodavatelů.
			Ověřuje reference potenciálního dodavatele.
			Ověřuje kvalifikaci (dostupné zdroje - personální i finanční) potenciálního dodavatele.
	2	H1	Osoby zastávající bezpečnostní role mají dostatečné zdroje (vč. finančních).
			Osoby zastávající bezpečnostní role mají dostatečné pravomoci.
			Dodavatel prosazuje systém řízení bezpečnosti informací a věnuje mu dostatečné zdroje.
Bezpečnostní role	2	H22	Osoby zastávající bezpečnostní role mají předepsanou kvalifikaci.
Řízení dodavatelů	4	H15	Smlouvy se sub-dodavateli zajišťují oprávnění k užívání dat.
			Smlouvy se sub-dodavateli obsahují dostatečné licenční ujednání.

	4	H20	Stanovil pravidla pro sub-dodavatele, která zohledňují požadavky řízení bezpečnosti informací.
			Seznamuje sub-dodavatele s pravidly týkajícími se řízení bezpečnosti informací.
			V případě významných dodavatelů, provádí v průběhu výběrového řízení a před uzavřením smlouvy, hodnocení rizik.
			Zajišťuje, aby se jeho významní dodavatele zavázali dodržovat pravidla bezpečnosti informací ve stejném rozsahu, v jakém je zavázán dodavatel ve vztahu k objednateli.
	4	H16	Stanovil pravidla pro sub-dodavatele (zejm. z hlediska dostupnosti služeb).
			V případě významných dodavatelů smluvně upravuje řízení kontinuity činností souvisejících s dodavateli.
Bezpečnost lidských zdrojů	4	H1	Zajišťuje pravidelná školení zaměstnanců, uživatelů, administrátorů, osob zastávajících bezpečnostních role o jejich povinnostech a bezpečnostní politice.
	4	H2	Zajišťuje pravidelná bezpečnostní školení sub-dodavatelů o jejich povinnostech a bezpečnostní politice.
	4	H3	Provádí pravidelné ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.
	4	H7	Zajišťuje pravidelná odborná školení osob zastávajících bezpečnostní role.
	4	H10	Zajišťuje kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
	4	H13	Zajišťuje, aby v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role byla předána odpovědnost osobě, která bude nadále pozici zastávat.
	4	H14	Určil pravidla a postupy řešení případů porušení stanovených bezpečnostních pravidel.
		H18	
Řízení provozu a komunikací	4	H1	Stanovil práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role.
			Řídí technické zranitelnosti
			Stanovil postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.
			Identifikoval kontaktní osoby pověřené výkonem systémové a technické podpory. Zajistil spojení na tyto osoby.
	2	H3	Vývojové, testovací a provozní prostředí jsou oddělené.
			Provádí pravidelné zálohování dat
			Provádí pravidelnou kontrolu použitelnosti provedených záloh.
			Stanovil pravidla a postupy pro ochranu informací a dat v průběhu celého životného cyklu.
	4	H10	Stanovil práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role.
	4	H14	Stanovil pravidla a postupy pro zajištění bezpečnosti síťových služeb.
			Stanovil pravidla a postupy pro ochranu před škodlivým kódem.
	4	H16	Stanovil postupy pro sledování kybernetických bezpečnostních událostí.
			Přijal opatření pro ochranu přístupu k záznamům o kybernetických bezpečnostních událostech.
			Identifikoval kontaktní osoby pověřené výkonem systémové a technické podpory. Zajistil spojení na tyto osoby.

Řízení změn	3	H1	Při provádění změn v rámci plnění přezkoumává možné dopady změn.
		H14	Určuje významné změny.
			U významných změn dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření ke snížení nepříznivých dopadů změny
			Provádí testování před provedením významné změny.
			V případě významné změny zajišťuje možnost navrácení do původního stavu.
Řízení přístupu	2	H7	Stanovil bezpečnostní opatření pro používání mobilních zařízení a jiných technických zařízení, které nejsou ve správě dodavatele.
	4	H10	Při ukončení smluvního vztahu odebírá přístupové oprávnění.
			Při ukončení změně smluvního vztahu změní přístupové oprávnění.
Akvizice, vývoj a údržba	2	H1	Řídí rizika plnění dle VKB
			Řídí významné změny plnění dle VKB
		H14	Stanovil bezpečnostní požadavky a zahrnul je do projektu vývoje.
			Zajišťuje bezpečnost vývojového a testovacího prostředí a ochranu používaných testovacích dat.
			Provádí bezpečnostní testování významných změn před jejich zavedením do provozu, ev. předáním objednateli.
Zvládání kybernetických bezpečnostních událostí a incidentů	3	H1 H3 H14 H16	Zavedl proces detekce a vyhodnocování bezpečnostních událost a zvládání kybernetických bezpečnostních incidentů
Řízení kontinuity činností	3	H16	Vypracoval, pravidelně aktualizuje a testuje plány kontinuity činností.

Tabulka 34 - Organizační opatření k implementaci
Zdroj: vlastní zpracování

TECHNICKÁ OPATŘENÍ			
Kategorie opatření	**Potřebná úroveň**	**Hrozba**	**Požadavky na dodavatele**
Fyzická bezpečnost	4	H3	Předchází poškození, krádeži nebo zneužití aktiv využívaných pro poskytování plnění nebo přerušení poskytování plnění
	4	H6	Stanovil fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány nebo zpracovávány informace a umístěna technická aktivy využívaná pro poskytování plnění.
Bezpečnost komunikačních sítí	4	H12	Vyčlenil komunikační síť využívanou pro poskytování plnění.
		H14	Zajišťuje řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě
			Zajišťuje důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií pomocí kryptografie.
			Aktivně blokuje nežádoucí komunikaci.
			Při segmentaci sítě a řízení komunikace mezi jejími segmenty využívá nástroj, který zajistí ochranu integrity komunikační sítě.
Správa a ověřování identit	4	H3	Používá autentizační mechanismus založený na více faktorové autentizaci nejméně s 2 různými typy faktorů
		H11	Používá autentizační mechanismus založený na autentizaci pomocí kryptografických klíčů zajišťující obdobnou úroveň jako více faktorová autentizace s 2 různými typy faktorů.

			Identity uživatelů, administrátorů a aplikací, je ověřována pomocí nástroje, který používá k autentizaci identifikátor účtu a heslo, vynucuje 12 znaků u uživatelů a 17 znaků u administrátorů a vymáhá povinnou změnu hesla v intervalu maximálně po 18 měsících.
			Implementace nástroje pro správu a ověření identity uživatelů, administrátorů a aplikací.
Řízení přístupových oprávnění	4	H3	Používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění pro přístup k jednotlivým aktivům využívaným pro poskytování plnění povinné osobě.
	2	H10	Používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění pro čtení, zápis dat a změnu oprávnění.
Ochrana před škodlivým kódem	3	H3	Implementoval nástroj zajišťující nepřetržitou automatickou ochranu před škodlivým kódem.
		H14	Řídí oprávnění ke spouštění kódu.
			Řídí automatické spouštění obsahu výměnných zařízení a datových nosičů.
			Provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.
	2	H7	Monitoruje používání výměnných zařízení a datových nosičů.
Zaznamenávání událostí informačního a komunikačního systému	3	H3 H16	Zaznamenává bezpečnostní a potřebné provozní události aktiv důležitých pro poskytování plnění povinné osobě.
Detekce kybernetických bezpečnostních událostí, Sběr a vyhodnocování kybernetických bezpečnostních událostí	3	H3	V komunikační síti užívané pro poskytování plnění povinné osobě používá nástroj pro detekci kybernetických bezpečnostních událostí.
		H14	Nasadil nástroj pro ověření a kontrolu přenášených dat v rámci komunikační sítě nebo mezi komunikačními sítěmi využívanými pro poskytování plnění.
			Nasadil nástroj pro ověření a kontrolu přenášených dat na perimetru komunikační sítě využívané k poskytování plnění.
			Blokuje nežádoucí komunikaci.
Kryptografické prostředky	2	H3	Používá aktuálně odolné kryptografické algoritmy a kryptografické klíče pro ochranu aktiv užívaných k poskytování plnění.
Zajišťování úrovně dostupnosti informací	2	H1	Zajišťuje redundanci aktiv nezbytných pro poskytování plnění povinné osobě.

Tabulka 35 - Technická opatření k implementaci
Zdroj: vlastní zpracování

7 Shrnutí výsledků

Za použití metodiky navržené v této bakalářské práci byl tedy relativně jednoduchým a intuitivním postupem navržen okruh bezpečnostních opatření, jež poskytují komplexní ochranu služeb dodavatele, a tedy i primárních aktiv tyto služby využívajících.

Okruh bezpečnostních opatření je přímo navázán na definici potenciálních hrozeb. Tímto propojením se snižuje též odbornost nezbytná k úspěšnému dokončení procesu a části tohoto procesu tedy mohou být v rámci organizace povinné osoby delegovány na zaměstnance zastávající nižší pozice, aniž by tím byla kompromitována výsledná kvalita hodnocení.

S ohledem na relativní jednoduchost posuzovaného příkladu (specifikaci služeb dodavatele), je možná výsledný rozsah opatření k implementaci překvapující. Jelikož však byla jednotlivá opatření identifikována v návaznosti na konkrétní hrozby, jejichž okruh je s dodavatelem předjednán, bude povinná osoba schopna své požadavky snadno dodavateli odůvodnit. Na druhou stranu si lze představit, jak náročným úkolem, a to jak z hlediska odbornosti, tak vynaloženého času, je vytvoření tohoto seznamu opatření bez znalosti konkrétních hrozeb.

Na příkladu uvedeném v předchozí kapitole rovněž vidíme, že stěžejní roli v zajištění bezpečnosti informačního systému mohou hrát organizační opatření. Tato, ač ekonomicky nenáročná na implementaci, jsou často standardními nástroji hodnocení dodavatelů opomíjena. Přesto velmi vypovídají mj. o celkové vyzrálosti organizace dodavatele a neměla by tedy být přehlížena.

V neposlední řadě je třeba je třeba si povšimnout, že jednotlivá opatření se vzájemně doplňují a, snad s výhradou hrozby nedostatečné identifikace technických či personálních aktiv, všechny hrozby jsou adresovány několika opatřeními současně. Tímto je pochopitelně dosaženo vyšší úrovně zabezpečení služeb dodavatele, než byla-li by konkrétní hrozba adresována pouze jediným bezpečnostním opatřením.

8 Závěry a doporučení

Tato bakalářská práce si za svůj cíl stanovila navržení metodiky hodnocení významnosti dodavatele a stanovení okruhu a významu bezpečnostních opatření, jejichž zavedení potenciálním dodatelem zajistí zákonem požadovanou úroveň zabezpečení informačního a komunikačního systému. Za tímto účelem byl definován okruh hrozeb, jež mohou při zapojení dodavatele existovat a navržen způsob propojení těchto hrozeb s jednotlivými opatřeními předvídanými VKB. Lze tedy konstatovat, že tento cíl bakalářské práce byl naplněn.

Zároveň si bakalářská práce kladla za úkol ověřit, zda lze proces určení bezpečnostních opatření zjednodušit a zefektivnit, aniž by tím byla kompromitována jeho kvalita. Metodika v této bakalářské práci předložená tento proces rozšířila o hodnocení rizik souvisejících se zapojením dodavatele. Mohlo by tedy být argumentováno, že bakalářská práce se minula svým účelem a proces nezjednodušuje. Přesto se autorka této práce domnívá, že opak je pravdou. Jak bylo demonstrováno v příkladu předloženém v kapitole 5, propojením procesu hodnocení rizik s procesem stanovení okruhu bezpečnostních opatření, došlo ke snížení odborné a potenciálně i časové náročnosti jeho dokončení. Kvalita posouzení přitom byla nepochybně nejen zachována, ba naopak, došlo k jejímu zvýšení. Je tedy argumentováno, že bakalářská práce tento cíl naplnila a předkládá způsob zjednodušení a zefektivnění procesu stanovení bezpečnostních opatření, jejichž implementaci je třeba na dodavateli vyžadovat.

Metodiku předloženou v této bakalářské práci je možno dále rozvíjet. Jedním z možných směrů je další zpřesnění provázání bezpečnostních opatření k jednotlivým hrozbám. Tohoto cíle je možno dosáhnout propojením bezpečnostních opatření též s konkrétními zranitelnostmi identifikovanými pro jednotlivé hrozby. Další cestou může být převedení této metodiky do podoby webové aplikace. V tomto směru bude jistě výzvou navržení uživatelského rozhraní, které uživateli umožní dynamickou úpravu zadaných hodnot.

9 Seznam použité literatury

[1] ISO/IEC 27036-1:2014. *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*. 1. Švýcarsko: Mezinárodní organizace pro standardizaci, 2014.

[2] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

[3] Národní úřad pro kybernetickou a informační bezpečnost. *Pomůcka k auditu bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.: (pracovní verze checklistu)*. In: Národní úřad pro kybernetickou a informační bezpečnost. *Národní centrum kybernetické bezpečnosti: REGULACE A KONTROLA.* PODPŮRNÉ MATERIÁLY [online]. Brno. 2018 [cit. 2019-12-28]. Dostupné z: https://www.govcert.cz/download/kii-vis/NovaVKB/VKB_checklist_2018_v1.xlsx

[4] ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní politiky - Soubor postupů pro opatření bezpečnosti informací*. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[5] THE SANTA FE GROUP. *Standardized Information Gathering (SIG) Questionnaire: The SIG Questionnaire Tools.* In: Standard Information Gathering: Shared Assessment [online]. Santa Fe – Nové Mexiko. [cit. 2019-12-28]. Dostupné z: https://sharedassessments.org/sig/

[6] State of California Department of Justice, Office of the Attorney General. *California Consumer Privacy Act (CCPA): FACT SHEET*. XAVIER BECERRA: Attorney General [online]. California. [cit. 2019-12-28]. Dostupné z: https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

[7] Česká republika. *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. In: Sbírka zákonů České republiky. 2018, částka 43, s. 1122-1168. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82?text=Vyhl%C3%A1%C5%A1ka+o+kybernetick%C3%A9+bezpe%C4%8Dnosti

[8] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[9] Národní úřad pro kybernetickou a informační bezpečnost. *Metodika k vodítkům pro hodnocení dopadů*. In: Národní úřad pro kybernetickou a informační bezpečnost. *Národní centrum kybernetické bezpečnosti: REGULACE A KONTROLA.* PODPŮRNÉ MATERIÁLY [online]. Brno. 2018 [cit. 2019-12-30]. Dostupné z: https://www.govcert.cz/download/kii-vis/Metodika_k_voditkum_pro_hodnoceni_dopadu_NUKIB_v.1.2_s_prilohou.pdf

[10] Česká republika. *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů*. In: Sbírka zákonů České republiky. 2014, částka 75, s. 1926 - 1936. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181?text=kybernetick%C3%A9+bezpe%C4%8Dnosti

[11] Evropská unie. *Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný*. In: Úřední věstník Evropské unie. 2018, L 26, s.48-51. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2018.026.01.0048.01.CES&toc=OJ:L:2018:026:TOC

[12] Česká republika. *Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů*. In: Sbírka zákonů České republiky. 2012, částka 33, s. 1026 - 1365. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89

[13] Ministerstvo spravedlnosti České republiky. *Důvodová zpráva.* In: *Nový občanský zákoník: Texty zákonů* [online]. Česká republika. 2012 [cit. 2019-12-30]. Dostupné z: http://obcanskyzakonik.justice.cz/images/pdf/Duvodova-zprava-NOZ-konsolidovana-verze.pdf

[14] Česká republika. *Zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů*. In: Sbírka zákonů České republiky. 2012, částka 34, s. 1370 - 1482. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-90

[15] NOVOTNÁ KRTOUŠOVÁ, Lucie. *Odpovědnost členů statutárních orgánů právnických osob*. Praha: Wolters Kluwer, 2019. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-039-7.

[16] Česká republika. *Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů*. In: Sbírka zákonů České republiky. 1991, částka 98, s. 2472 - 2565. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/1991-513

[17] DĚDIČ, Jan. *Obchodní zákoník: komentář*. Praha: Polygon, 2002. ISBN 80-7273-071-1.

[18] Česká republika. *Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů*. In: Sbírka zákonů České republiky. 2009, částka 11, s. 354 - 464. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40?text=

[19] Vláda České republiky. *Vládní návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* In: Úřad vlády České republiky. *2.1.*2014 [cit. 2019-12-30]. Dostupné z: https://apps.odok.cz/attachment/-/down/KORN9F6H6BCH

[20] Česká republika. *Zákon č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony*. In: Sbírka zákonů České republiky. 2017, částka 39, s. 1137 - 1147. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-104

[21] Česká republika. *Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony*. In: Sbírka zákonů České republiky. 2017, částka 74, s. 2234 - 2252. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

[22] Evropská unie. *Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii*. In: Úřední věstník Evropské unie. 2016, L 194. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L1148

[23] Česká republika. *Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů*. In: Sbírka zákonů České republiky. 1993, částka 1, s. 3 - 16. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-1

[24] Česká republika. *Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů*. In: Sbírka zákonů České republiky. 1993, částka 1, s. 17 - 23. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-2

[25] MIKEŠ, Petr a NEUMANOVÁ, Tereza. K zadávání veřejných zakázek dotovanými zadavateli postupy podle dotačních pravidel s ohledem na přechodná ustanovení novely zákona o veřejných zakázkách. In: *epravo.cz: články* [online]. Česká republika. 11.9.2012 [cit. 2020-01-02]. Dostupné z: https://www.epravo.cz/top/clanky/k-zadavani-verejnych-zakazek-dotovanymi-zadavateli-postupy-podle-dotacnich-pravidel-s-ohledem-na-prechodna-ustanoveni-novely-zakona-o-verejnych-zakazkach-85193.html

[26] ČSN ISO/IEC 27000*. Informační technologie - Bezpečnostní politiky – Systémy řízení bezpečnosti informací – Požadavky*. 2. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018.

[27] ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní politiky – Systémy řízení bezpečnosti informací – Přehled a slovník*. 5. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[28] Česká republika. *Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších zákonů*. In: Sbírka zákonů České republiky. 1997, částka 6, s. 128 - 136. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/1997-22

[29] Česká republika *Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostní incidentech, reaktivních opatřeních a o stavení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)*. In: Sbírka zákonů České republiky. 2014, částka 127, s. 3972 - 4006. ISSN 1211-1244. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-316

[30] GOLL, Jan. Zákon o kybernetické bezpečnosti versus ISO 27001: aneb jak vyhovět oběma normám. In: *SystemOnline* [online]. Česká republika. 28. 8. 2019 [cit. 2020-01-02]. Dostupné z: http://m.systemonline.cz/sprava-it/zakon-o-kybernetricke-bezpecnosti-versus-iso-27001.htm

[31] GURYČOVÁ, Kristýna a CIBULKA, Jan. ‚Máme mlčenlivost, a to i vůči klientům.' T-Mobile neupozornil zákazníky na masivní únik citlivých dat. In: *IRozhlas.cz* [online]. Česká republika. 27.2. 2019 [cit. 2020-01-05]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/t-mobila-unik-dat-osobni-udaje-zamestnanec-obzaloba_1902270605_kno

[32] MCAFEE LABS. Cyber Criminals Gain in Sophistication With Integrity Attacks. *McAfee.com* [online]. Santa Clara - Kalifornie. 26.1.2016 [cit. 2020-01-05]. Dostupné z: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cyber-criminals-gain-sophistication/

[33] ČESKÁ TISKOVÁ KANCELÁŘ (ČTK). Benešovskou nemocnici ochromil počítačový virus, pacienti musí jinam. Na místo dorazil specializovaný tým NÚKIB. In: *Ihned.cz* [online]. Česká republika. 11.12.2019 [cit. 2020-01-05]. Dostupné z: https://domaci.ihned.cz/c1-66692450-provoz-benesovske-nemocnice-ochromil-pocitacovy-virus-nemohou-spustit-zadny-pristroj

[34] BOYES, Hugh. Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review* [online]. Kanada: Talent First Network, 2015, 28-34 [cit. 2020-01-05]. Dostupné z: https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_April2015.pdf#page=28

[35] ČERMÁK, Miroslav. CIA: Je důvěrnost, integrita a dostupnost dostačující? In: *Cleverandsmart.cz* [online]. Česká republika. 2.12.2018 [cit. 2020-01-05]. Dostupné z: https://www.cleverandsmart.cz/cia-je-duvernost-integrita-a-dostupnost-dostacujici/

[36] PENDER-BEY, Georgie. *THE PARKERIAN HEXAD: The CIA Triad Model Expanded*. In: Lewis University. *Department of Computer and Mathematical Science* [online]. [cit. 2020-01-05]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

[37] Vláda České republiky. *Metodická pomůcka pro přípravu návrhů právních předpisů.* In: Vláda České republiky. *Vláda České republiky: České republiky: pracovní a poradní orgány* [online]. Česká republika. 11. 7. 2006 [cit. 2020-02-08]. Dostupné z: https://www.vlada.cz/cz/ppov/lrv/dokumenty/metodicka-pomucka-pro-pripravu-navrhu-pravnich-predpisu-iii--cast-18197/

[38] Národní úřad pro kybernetickou a informační bezpečnost. *Provozovatel informačního nebo komunikačního systému podle §2 písm. g) zákona o kybernetické bezpečnosti*. In: Národní úřad pro kybernetickou a informační bezpečnost. *Národní centrum kybernetické bezpečnosti: REGULACE A KONTROLA.* PODPŮRNÉ MATERIÁLY [online]. Brno. 2019 [cit. 2020-02-09]. Dostupné z: https://www.govcert.cz/download/kii-vis/obecne/Provozovatel-informacniho-nebo-komunikacniho-systemu_v2.1.pdf

[39] Národní úřad pro kybernetickou a informační bezpečnost. *Povinné osoby*. In: Národní úřad pro kybernetickou a informační bezpečnost. *Národní centrum kybernetické bezpečnosti: REGULACE A KONTROLA* [online]. Brno. [cit. 2020-03-02]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/povinne-osoby/

[40] Národní úřad pro kybernetickou a informační bezpečnost. *Kritická informační infrastruktura: Proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb*. In: Národní úřad pro kybernetickou a informační bezpečnost. *Národní centrum kybernetické bezpečnosti: REGULACE A KONTROLA.* PODPŮRNÉ MATERIÁLY [online]. Brno. 2018 [cit. 2020-03-02]. Dostupné z: *https://www.govcert.cz/download/kii-vis/Schema_KII.pdf*

[41] Národní úřad pro kybernetickou a informační bezpečnost. *Významné informační systémy: Proces určování podle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích*. In: Národní úřad pro kybernetickou a informační bezpečnost. *Národní centrum kybernetické bezpečnosti: REGULACE A KONTROLA.* PODPŮRNÉ MATERIÁLY [online]. Brno. 2018 [cit. 2020-03-02]. Dostupné z: *https://www.govcert.cz/download/kii-vis/Schema_VIS.pdf*

[42] Národní úřad pro kybernetickou a informační bezpečnost. *Základní služba: Proces určení provozovatele základní služby a informačního systému základní služby dle zákona o kybernetické bezpečnosti a vyhlášky o kritériích pro určení provozovatelů základních služeb*. *Národní centrum kybernetické bezpečnosti: REGULACE A KONTROLA.* PODPŮRNÉ MATERIÁLY [online]. Brno. 2018 [cit. 2020-03-02]. Dostupné z: https://www.govcert.cz/download/kii-vis/Schema_rozhodovani_PZS_v2.1.pdf

[43] Národní úřad pro kybernetickou a informační bezpečnost. *Varování Národního úřadu pro kybernetickou a informační bezpečnost, sp. zn. 110 – 536/2018, ze dne 17. prosince 2018, před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation*. *Národní úřad pro kybernetickou a informační bezpečnost: ÚŘEDNÍ DESKA* [online]. Brno. 17.12.2018 [cit. 2020-03-02]. Dostupné z: https://nukib.cz/cs/uredni-deska/

10 Přílohy

Obsah:

1. Seznam použitých zkratek
2. Metodika hodnocení dodavatelů
3. Použití metodiky hodnocení dodavatele – příklad
4. Oskenované zadání práce

Příloha 1: Seznam použitých zkratek

ČSN – česká technická norma

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OZ – občanský zákoníkzákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů [12]

PO – právnická osoba

VKB – vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) [7]

ZKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) [10]

ZOK – zákon č. 90/2012 Sb., o obchodních korporacích a družstvech, ve znění pozdějších předpisů [14]

Příloha 2: Metodika hodnocení dodavatelů

Obsah:

HODNOCENÍ RIZIKA

Hodnocené podpůrné aktivum (předmět dodávky)	Primární aktivum[1]	Hodnocení důležitosti primárního aktiva	Hodnocení důležitosti podpůrného aktiva[2]			Primární cíl hrozby	Hrozba[3]	Zkratka	Hodnocení závažnosti hrozby[2]	Hodnocení závažnosti dopadů (tj. dopad porušení důvěrnosti, dostupnosti nebo integrity aktiva)[2] [1]										Riziko, včetně korekce hodnocením primárního aktiva[2]
			Důvěrnost	Dostupnost	Integrita					Bezpečnost a zdraví osob	Ochrana osobních údajů	Zákonné a smluvní povinnosti	Trestně-právní řízení	Veřejný pořádek	Mezinárodní vztahy	Řízení organizace	Ztráta důvěryhodnosti	Finanční ztráty	Zajišťování nezbytných služeb	
služby v oblasti vývoje software, nezahrnující podporu a údržbu software	*Primární aktivum 1*	*Hodnocení 1*				Technická aktiva (hardwarové a softwarové vybavení, média a dokumenty)[4]	porucha zařízení nebo chybné fungování aplikačního programového vybavení	H1												0
	Primární aktivum 2	*Hodnocení 2*					nedbalostní nebo úmyslné poškození, chyba použití	H2												0
	Primární aktivum 3	*Hodnocení 3*					ztráta, odcizení médií nebo dokumentů	H3												0
							zneužití vnitřních prostředků (použití pro osobní účely, použití k jinému než legálnímu účelu), zneužití oprávnění	H4												0
							zneužití identity, falšování zpráv	H5												0
							zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)	H6												0
							zneužití vyměnitelných technických nosičů dat a mobilních zařízení	H7												0
							poškození dat použitím aplikačních programů na špatná data z hlediska času	H8												0
							provedení neoprávněných činností, tj. činností k nimž uživatel nemá oprávnění	H9												0
							zneužití oprávnění ze strany uživatelů[5] a administrátorů	H10												0
							vzdálená špionáž	H11												0
							odposlech	H12												0
							cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	H13												0
							instalace zákeřného kódu	H14												0
							neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	H15												0
							dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky el. energie nebo jiných důležitých služeb	H16												0
							přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	H17												0
							porušení bezpečnostní politiky	H18												0
							chybná identifikace technických aktiv	H19												0
						Personální aktiva	nedodržení smluvního závazku ze strany subdodavatele	H20												0
							pochybení ze strany zaměstnanců (včetně trestné činnosti)	H21												0
							nedostatečná odborná úroveň nebo bezpečnostní kvalifikace	H22												0
							přechod klíčového personálního aktiva ke konkurenci	H23												0
							vyzrazení informací	H24												0
							nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance ze společnosti	H25												0
							chybná identifikace personálních aktiv	H26												0

POZNÁMKY POD ČAROU

1 Primárním aktivem je vždy služba, kterou zpracovává nebo poskytuje informační a komunikační systém.

2 Viz. návod pro vyplnění.

3 Hrozby, kterými jsou ohrožena daná aktiva, nikoli hrozby, jejichž aktéry jsou daná aktiva. Př. Zaměstnanci mohou být původci většiny hrozeb, které ohrožují technická aktiva.

4 Zahrnuje hrozby ohrožující fyzická média, data na nich uložená, jakož i dokumentu ve fyzické podobě.

5 Uživatelé zahrnují jak zaměstnance povinné osoby, tak jejích dodavatelů.

Návod pro vyplnění

Tento list obsahuje návod pro kategorizaci vyžadovanou při hodnocení rizika či určení okruhu bezpečnostní opatření.

OBSAH

HODNOCENÍ DŮLEŽITOSTI PODPŮRNÉHO AKTIVA

DŮVĚRNOST

Stupeň důležitosti	Definice	Vložit do tabulky
Nízká	Aktivum je veřejně přístupné nebo určeno ke zveřejnění. Narušení důvěrnosti neohrožuje zájmy povinné osoby a nebude mít negativní dopad.	1
Střední	Aktivum není veřejně přístupné a tvoří know-how povinné osoby. Jeho ochrana není vyžadována žádným právním předpisem ani smluvním ujednáním.	2
Vysoká	Aktivum není veřejně přístupné a tvoří know-how povinné osoby. Jeho ochrana je vyžadována právním předpisem nebo smluvním ujednáním (př. obchodní tajemství, osobní údaje).	3
Kritická	Aktivum není veřejně přístupné a vyžaduje nadstandardní míru ochrany nad rámec předchozí kategorie (př. strategické obchodní tajemství, zvláštní kategorie osobních údajů).	4

Zdroj: [2, příloha 1]

DOSTUPNOST

Stupeň důležitosti	Definice	Vložit do tabulky
Nízká	Narušení dostupnosti není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do1 týdne).	1
Střední	Narušení dostupnosti by nemělo překročit dobu 1 pracovního dne. Dlouhodobější výpadek může ohrozit oprávněné zájmy povinné osoby.	2
Vysoká	Narušení dostupnosti by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	3
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k závažnému ohrožení opráněných zájmů povinné osoby.	4

Zdroj: [2, příloha 1]

INTEGRITA

Stupeň důležitosti	Definice	Vložit do tabulky
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje zájmy povinné osoby.	1
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	2
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	3
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	4

Zdroj: [2, příloha 1]

HODNOCENÍ ZÁVAŽNOSTI HROZEB

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.	1
Střední	Hrozba je málo pravděpodobná až nepravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.	2
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.	3
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.	4

Zdroj: [2, příloha 2]

HODNOCENÍ DOPADU

BEZPEČNOST A ZDRAVÍ OSOB

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	2
Vysoká	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	3
Kritická	Může vést k přímému ohrožení či ztrátě života skupiny osob.	4

Zdroj: [1, příloha 1]

OCHRANA OSOBNÍCH ÚDAJŮ

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může způsobit prušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	1
Střední	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2% celkového ročního obratu - viz. čl. 83/4 GDPR).	2
Vysoká	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 20 mil. EUR nebo 4% celkového ročního obratu - viz. čl. 83/5 GDPR).	3
Kritická	Žádné vodítko.	4

Zdroj: [1, příloha 1]

ZÁKONNÉ A SMLUVNÍ POVINNOSTI

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může zapříčinit porušení interních předpisů a postupů, nikoli však k porušení zákonných a smluvních povinností.	1
Střední	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo náhradě škody.	2
Vysoká	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	3
Kritická	Žádné vodítko.	4

Zdroj: [1, příloha 1]

TRESTNĚ-PRÁVNÍ ŘÍZENÍ

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	2
Vysoká	Může vést k narušení vyšetřování trestné činnosti nebo soudnímu řízení (méně závažná kriminalita, krátkodobé, v jednotlivých případech).	3
Kritická	Může vést k závažnému dlohodobému narušení schopnosti vyšetřovat trestnou činnosti, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	4

Zdroj: [1, příloha 1]

VEŘEJNÝ POŘÁDEK

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	2
Vysoká	Může zapříčinit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	3
Kritická	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit pořádek s celostátními dopady.	4

Zdroj: [1, příloha 1]

MEZINÁRODNÍ VZTAHY

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v 1 státě.	2
Vysoká	Může vytvářet negativní obraz ČR ve světě.	3
Kritická	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	4

Zdroj: [1, příloha 1]

ŘÍZENÍ A PROVOZ ORGANIZACE

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může narušit řádné řízení nebo fungování části nebo celé organizace.	1
Střední	Může omezit provádění důležitých činností organizace.	2
Vysoká	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	3
Kritická	Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti.	4

Zdroj: [1, příloha 1]

ZTRÁTA DŮVĚRYHODNOSTI

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může negativně ovlivnit vztahy s jinými částmi organizace nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhého trvání.	1
Střední	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	2
Vysoká	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	3
Kritická	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	4

Zdroj: [1, příloha 1]

FINANČNÍ ZTRÁTY

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	1
Střední	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05% a 2% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	2
Vysoká	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2% a nižším či rovným 10% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	3
Kritická	Může přímo či nepřímo vést ke ztrátám přesahujícím 10% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	4

Zdroj: [1, příloha 1]

ZAJIŠŤOVÁNÍ NEZBYTNÝCH SLUŽEB

Stupeň závažnosti	Definice	Vložit do tabulky
Nízká	Žádné vodítko.	1
Střední	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.	2
Vysoká	Může způsobit závažné omezení, narušení či nedostupnost nezbytných služeb pro více než 25.000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivá odvětví, viz. vyhláška č. 437/2017 Sb.)	3
Kritická	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiný závažný zásah do každodenního života postihující více než 125.000 osob.	4

Zdroj: [1, příloha 1]

HODNOCENÍ RIZIKA

Stupeň významnosti	Definice	Hodnota v tabulce
Nízké	Riziko je považováno za akceptovatelné.	1
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti je riziko akceptovatelné.	2
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	3
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	4

Zdroj: [2, příloha 2]

HODNOCENÍ VÝZNAMU OPATŘENÍ

Stupeň významnosti	Definice	Hodnota v tabulce
Nízký	Význam opatření z hlediska předcházení realizace hrozby nebo snižování jejich dopadů je spíše podružný. V případě, že vyhodnocený stupeň rizika je 1 až 3, opatření není třeba implementovat.	1
Střední	Význam opatření z hlediska předcházení realizace hrozby nebo snižování jejich dopadů je střední. V případě, že vyhodnocený stupeň rizika je 1 nebo 2, opatření není třeba implementovat.	2
Vysoký	Význam opatření z hlediska předcházení realizace hrozby nebo snižování jejich dopadů je vysoký. V případě, že vyhodnocený stupeň rizika je 1, opatření není třeba implementovat.	3
Kritický	Opatření je třeba implementovat vždy, je považováno za minimální zabezpečení.	4
Podmíněný	Opatření je omezeno na specifické systémy či specifické situace, jeho aplikovatelnost je třeba vyhodnotit s přihlédnutím k hodnoceným aktivům a zvažovaným činnostem. Význam opatření nemůže být vyhodnocen v obecné rovině.	5

Zdroj: vlastní zpracování

TECHNICKÁ AKTIVA	DRUH OPATŘENÍ A JEHO VÝZNAM PRO PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																										
	ORGANIZAČNÍ OPATŘENÍ														TECHNICKÁ OPATŘENÍ												
HROZBA	Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídicí a obdobné systémy
porucha zařízení nebo chybné fungování aplikačního programového vybavení				2			2	4	3		5	3											1		2	5
nedbalostní nebo úmyslné poškození, chyba použití							4					2			3			3	3	2	2	2				5
ztráta, odcizení médií nebo dokumentů		2					4	2				3			3	1	4	4	3	3	3	3	1	2		5
zneužití vnitřních prostředků		4		4			4	5		3							3			2	2	2	1				
zneužití identity, falšování zpráv							4			4							4						2				
zničení nebo poškození zařízení v důsledku změn prostředí													3		4												
zneužití vyměnitelných technických nosičů dat		3					4			2									2								
poškození dat použitím aplikačních programů na špatná data z hlediska času																				4		4					
provedení neoprávněných činností, tj. provedení činností k nimž uživatel nemá oprávnění				4			4	4								1	4	3		2		2	2				5
zneužití oprávnění ze strany uživatelů a administrátorů				4			4	4		4								2									
vzdálená špionáž																3	4							2			
odposlech																4								2			
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik		1					4			2						3	3										
instalace zákeřného kódu		1					4	4	5	1	5	2				3			4		2	2					
neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění				4		4																					
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb						4		4				3	3			2				3		3			3	5	
přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie						4		4				2	2			2				2		2					5
porušení bezpečnostní politiky							4					1		1													
chybná identifikace technických aktiv	4																										

PERSONÁLNÍ AKTIVA	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																								
	ORGANIZAČNÍ OPATŘENÍ														TECHNICKÁ OPATŘENÍ										
HROZBA	Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činnosti	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídicí a obdobné systémy
nedodržení smluvního závazku ze strany subdodavatele				3		4	3																		
pochybení ze strany zaměstnanců (včetně trestné činnosti)				4			4																		
nedostatečná odborná úroveň					2		4																		
přechod klíčového personálního aktiva ke konkurenci				4																					
vyzrazení informací				4			4	1																	
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance / dodavatele				4			4																		
chybná identifikace personálních aktiv	4																								

URČENÍ VÝZNAMNOSTI OPATŘENÍ - TECHNICKÁ AKTIVA

Na tomto listu je provedeno určení významnosti jednotlivých opatření stanovených VKB pro minimalizaci naplnění hrozby, využití zranitelnosti či snížení dopadu.

PRACOVNÍ METODIKA URČENÍ VÝZNAMNOSTI OPATŘENÍ

Kategorie opatření	Přiřazená vstupní hodnota
Preventivní opatření - podpůrné, omezená aplikovatelnost	1
preventivní opatření - méně významné	2
preventivní opatření - stěžejní	3
reaktivní opatření - stěžejní	3
reaktivní opatření - méně významné nebo omezená aplikovatelnost	2

Hrozba	Kategorie opatření	Dle mapovací tabulky	Převod na stupnici 1-4	Výsledná hodnota, vč. korekce	Stručný popis
Porucha zařízení nebo chybné fungování aplikačního programového vybavení	Průmyslové, řídící a obdobné systémy	2	1	5	ochrana technického aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu - omezeno na průmyslové, řídící a obdobné specifické systémy
	Akvizice, vývoj a údržba	4	1	5	řízení významných změn v souvislosti s plánovanou akvizicí a údržbou, zahrnutí bezpečnostních požadavků do projektu, provádění bezpečností testování před jejich zavedením do
	Řízení provozu a komunikací	14	4	4	stanovení práv a povinností administrátorů a uživatelů, řízení tech. zranitelností, řízení a schvalování provozních změn, sledování a plánování kapacity lidských a technických zdrojů, zajištění kontaktu na osoby systémové a technické podpory
	Zvládní kybernetických událostí	5	2	3	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
	Řízení změn	10	3	3	přezkoumávání možných dopadů změny, určení významných změn, rozhodntí o provedení testování zranitelností
	Zajišťování úrovně dostupnosti informací	3	1	2	zajištění dostupnosti a redundance technických aktiv nezbytných pro provoz informačního a komunikačního systému, a to s ohledem na hodnocení podpůrných aktiv
	Organizační bezpečnost	3	1	2	zajištění dostupnosti zdrojů, dostatečné pravomoci a zdroje k požadované údržbě, dostatečné interní priority
	Bezpečnost lidských zdrojů	3	1	2	bezpečnostní školení administrátorů, osob zastávajících bezpečnostní role a dodavatelů
	Aplikační bezpečnost	1	1	1	penetrační testy před uvedením významné změny do provozu - omezeno na důležitá aktiva a významané změny
nedbalostní nebo úmyslné poškození, chyba použití	Průmyslové, řídící a obdobé systémy	1	1	5	omezení fyzického přístupu k zařízením průmyslových, řídících a obdobných specifických systémů; vyčlenění komunikační sítě určené pro průmyslové, řídící a obdobné specifické systémy od ostatní infrastruktury
	Bezpečnost lidských zdrojů	6	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, stanovení pravidel a postupů pro řešení případů bezpečnostních pravidel uživateli
	Fyzická bezpečnost	3	2	3	předchází poškození, krádeži nebo zneužití aktiv
	Ochrana před škodlivým kódem	2	1	3	nasazení nástroje pro nepřetržitou automatickou ochranu, řízení oprávnění ke spouštění kódu, řízení automatického spouštění obsahu výměnných zařízení a datových nosičů
	Řízení přístupových oprávnění	3	2	3	řízení přístupu k informačnímu a komunikačnímu systému a přijetí opatření, která slouží k zajištění ochrany a obrana proti zneužití
	Bezpečnost komunikačních sítí	3	2	2	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
	Zvládání kybernetických událostí	3	2	2	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
	Řízení změn	2	1	0	není relevantní
ztráta, odcizení médií nebo dokumentů	Průmyslové, řídící a obdobné systémy	1	1	5	omezení fyzického přístupu k zařízením průmyslových, řídících a obdobných specifických systémů

	Bezpečnost lidských zdrojů	15	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	Správa a ověřování identit			4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
	Řízení přístupových oprávnění	6	2	4	řízení přístupu k jednotlivým aktivům
	Ochrana před škodlivým kódem	3	1	3	nasazení nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace; nasazováno s ohledem na důležitost aktiv
	Fyzická bezpečnost	3	1	3	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů			3	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
	Kryptografické prostředky	2	1	2	použití aktuálně odolných kryptografických algoritmů a klíčů
	Řízení aktiv	3	1	2	určení způsobu likvidace dat, provozních údajů, informací a jejich kopií nebo likvidace technických nosičů
	Řízení provozu a komunikací	7	2	2	oddělení vývojového, testovacího a provozního prostředí, provádění pravidelných záloh, zajištění bezpečnosti informací v průběhu celého životního cyklu
	Bezpečnost komunikačních sítí	3	1	1	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
	Aplikační bezpečnost	1	1	1	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností
	Zvládání kybernetických událostí	4	1	1	proces detekce kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů
	Akvizice, vývoj a údržba	1	1	0	není relevantní
Zneužití vnitřních prostředků	Řízení provozu a komunikací	3	1	5	oddělení vývojového, testovacího a provozního prostředí
	Řízení aktiv	6	2	4	stanovení přípustných způsobů používání aktiva, určení způsobu likvidace dat, provozních údajů, informací a jejich technických nosičů
	Bezpečnost lidských zdrojů	15	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
	Organizační bezpečnost	3	1	4	zajištění, aby byla zachovávána mlčenlivost administrátorů a osob zastávajících bezpečnostní role
	Správa a ověřování identit			3	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
	Řízení přístupu	3	1	3	řízení přístupu k jednotlivým aktivům
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	3	1	2	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
	Aplikační bezpečnost	1	1	1	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností
	Akvizice, vývoj a údržba	1	1	0	oddělení vývojového, testovacího a provozního prostředí
zneužití identity, falšování zpráv	Bezpečnost lidských zdrojů	3	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
	Řízení přístupu	3	4	4	odebrání nebo změna přístupových oprávnění při změně pozice, zařazení, změně smluvního vztahu
	Správa a ověřování identit	3	4	4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus

	Aplikační bezpečnost	3	4	2	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností
Zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)	Fyzická bezpečnost	3	4	4	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
	Řízení kontinuity činností	3	4	3	havarijní plány
Zneužití vyměnitelných technických nosičů dat	Bezpečnost lidských zdrojů	6	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
	Řízení aktiv	5	3	3	určení způsobu likvidace technických nosičů dat s ohledem na úroveň aktiv, určení přípustného způsobu používání aktiva
	Ochrana před škodlivým kódem	3	2	2	monitoring používání výměnných zařízení a datových nosičů
	Řízení přístupu	3	2	2	stanovení bezpečnostních opatření pro používání mobilních zařízení a jiných technických zařízení, kt. povinná osoba nemá ve své správě
poškození dat použitím aplikačních programů na špatná data z hlediska času	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	3	3	4	zajištění synchronizace jednotného času technických aktiv nejméně jednou za 24h
Provedení neoprávněných činností, tj. provedení činností k nimž uživatel nemá oprávnění	Průmyslové, řídící a obdobné systémy	1	1	5	omezení vzdáleného přístupu k těmto systémům
	Bezpečnost lidských zdrojů	9	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
	Správa a ověřování identit	3	1	4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
	Organizační bezpečnost	3	1	4	stanovení pravidel pro určení administrátorů
	Řízení provozu a komunikací	3	1	4	stanovení práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role
	Řízení přístupových oprávnění	3	1	3	použití centralizovaného nástroje pro řízení přístupových oprávnění k aktivům
	Aplikační bezpečnost	3	1	2	ochrana aplikací, informací a transakcí před neoprávněnou činností
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	3	1	2	zaznamenávání bezpečnostních a potřebných provozních údálostí důležitých aktiv
	Bezpečnost komunikačních sítí	2	1	1	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
Zneužití oprávnění ze strany uživatelů a administrátorů, tj. provedení činností k nimž uživateli bylo uděleno oprávnění k jinému než zamýšlenému účelu	Organizační bezpečnost	2	1	4	stanovení pravidel pro určení administrátorů
	Řízení provozu a komunikací	2	1	4	stanovení práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role
	Řízení přístupu	3	2	4	odebrání nebo změna přístupových oprávnění při ukončení nebo změně smluvního vztahu nebo pozice
	Bezpečnost lidských zdrojů	6	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
	Řízení přístupových oprávnění	2	1	2	použití centralizovaného nástroje pro řízení přístupových oprávnění k aktivům
Vzdálená špionáž	Správa a ověřování identit	3	4	4	zajištění odolnosti uložených a přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití, vynucování minimálních standardů pro tvorbu hesla
	Bezpečnost komunikačních sítí	3	4	3	segmentace stě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
	Kryptografické prostředky	3	4	2	použití aktuálně odolných kryptografických algoritmů a klíčů

Odposlech	Bezpečnost komunikačních sítí	6	4	4	segmentace stě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
	Kryptografické prostředky	3	2	2	použití aktuálně odolných kryptografických algoritmů a klíčů
Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	Bezpečnost lidských zdrojů	6	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
	Bezpečnost komunikačních sítí	6	4	3	aktivní blokace nežádoucí komunikace
	Správa a ověřování identit	3	2	3	zajištění odolnosti uložených a přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití, vynucování minimálních standardů pro tvorbu hesla
	Řízení přístupu	3	2	2	omezení a kontrola používání programových prostředků schopných překonat systémové nebo aplikační kontroly
	Řízení aktiv	2	1	1	stanovení přípustných způsobů používání aktiv, a pravidla manipulace s aktivy s ohledem na úroveň aktiv
Instalace zákeřného kódu	Akvizice, vývoj a údržba	1	1	5	stavenovení požadavků na technické aktivum v projektu akvizice, vývoje a údržby
	Řízení změn	1	1	5	provádění analýzy rizik, přijetí opatření za účelem snížení nepříznivých dopadů změny
	Ochrana před škodlivým kódem	3	2	4	použití nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace - nasazováno s ohledem na důležitost aktiv
	Řízení provozu a komunikací	2	1	4	pravidla a postupy pro zajištění bezpečnosti síťových služeb, pravidla a postupy pro ochranu před škodlivým kódem
	Bezpečnost lidských zdrojů	6	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky uživateli
	Bezpečnost komunikačních sítí	5	3	3	segmentace stě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
	Zvládní kybernetických událostí	3	2	2	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
	Řízení aktiv	2	1	1	stanovení přípustných způsobů používání aktiva a pravidel manipulace s aktivy s ohledem na úroveň aktiv
	Řízení přístupu	3	2	1	omezení a kontrola používání programových prostředků schopných překonat systémové nebo aplikační kontroly
Neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	Řízení dodavatelů	3	2	4	užívat data, c) - autorství programového kódu; požadevek dle písm. f) jsou omezeny na významné dodavatele; předpokladem je stanovení garanta aktiva a udělení dostaečných pravomocí a zdrojů k pořízení licence
	Organizační bezpečnost	6	4	4	zajištění integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu akvizice předmětů chráněných duševním vlastnictvím
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	Průmyslové, řídící a obdobné systémy	2	1	5	ochrana tech. aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezp. incidentu, vyčlenění od ostatní infastruktury - omezeno na průmyslové, řídící a obdobné specifické systémy
	Řízení provozu a komunikací	5	3	4	postupy pro sledování kybernetických bezpečnostních událostí, zajištění spojení na kontaktní osoby pověřené výkonem systémové a technické podpory
	Řízení dodavatelů	3	2	4	stanovení pravidel pro dodavatele a jejich pravidelné přezkoumávání, u významných též dle přílohy 7 VKB písm. k) - specifikace podmínek pro řízení kontinuity činností
	Zvládní kybernetických událostí	6	4	3	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	6	4	3	zaznamenávání bezpečnostních a potřebných provozních údálostí důležitých aktiv
	Zajišťování úrovně dostupnosti informací	6	4	3	zajištění dostupnosti a redundance tech. aktiv nezbytných pro provoz informačního a komunikačního systému a to s ohledem na hodnocení podpůrných aktiv.

	Řízení kontinuity činností	3	2	3	plány kontinuity činností
	Bezpečnost komunikačních sítí	3	2	2	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Průmyslové, řídící a obdobné systémy	2	1	5	ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu, vyčlenění od ostatní infastruktury - omezeno na průmyslové, řídící a obdobné specifické systémy
	Řízení dodavatelů	3	2	4	stanovení pravidel pro dodavatele a jejich pravidelné přezkoumávání, u významných též dle přílohy 7 písm. k) - specifikace podmínek pro řízení kontinuity činností
	Řízení provozu a komunikací	5	3	4	postupy pro sledování kybernetických bezpečnostních událostí, Zajištění spojení na kontaktní osoby pověřené výkonem systémové a technické podpory
	Bezpečnost komunikačních sítí	3	2	2	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
	Zvládní kybernetických událostí	6	4	2	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	6	4	2	zaznamenávání bezpečnostních a potřebných provozních údálostí důležitých aktiv
	Řízení kontinuity činností	3	2	2	plány kontinuity činností
porušení bezpečnostní politiky	Bezpečnost lidských zdrojů	6	4	4	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní, kontrola dodržování bezpečnostní politiky ze strany uživatelů
	Zvládní kybernetických událostí	2	1	1	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
	Audit kybernetické bezpečnosti	2	1	1	pravidelný audit kybernetické bezpečnosti
chybná identifikace technických aktiv	Systém řízení bezpečnosti informací	3	4	4	určení organizačních částí a aktiv, kterých se systém řízení bezpečnosti týká

URČENÍ VÝZNAMNOSTI OPATŘENÍ- PERSONÁLNÍ AKTIVA

Na tomto listu je provedeno určení významnosti jednotlivých opatření stanovených VKB pro minimalizaci naplnění hrozby, využití zranitelnosti či snížení dopadu.

PRACOVNÍ METODIKA URČENÍ VÝZNAMNOSTI OPATŘENÍ

Kategorie opatření	Přiřazená vstupní hodnota
Preventivní opatření - podpůrné, omezená aplikovatelnost	1
preventivní opatření - méně významné	2
preventivní opatření - stěžejní	3
reaktivní opatření - stěžejní	3
reaktivní opatření - méně významné nebo omezená aplikovatelnost	2

Hrozba	Kategorie opatření	Dle mapovací tabulky	Převod na stupnici 1-4	Výsledná hodnota, vč. korekce	Stručný popis
nedodržení smluvního závazku ze strany subdodavatele	Řízení dodavatelů	8	4	4	dodavatele, stanovení pravidel pro dodavatele, seznámení dodavatele s pravidly, u významných stanovení způsobů a urovní realizace bezpečnostních oprávnění a rozsah vzájemné smluvní odpovědnosti
	Organizační bezpečnost	3	2	3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu výběru dodavatelů
	Bezpečnost lidských zdrojů	6	3	3	poučení dodavatelů, pravidelné školení a ověřování bezpečnostního povědomí, kontrolu dodržování bezpečnostní politiky uživateli
pochybení ze strany zaměstnanců (včetně trestné činnosti)	Bezpečnost lidských zdrojů	9	4	4	poučení dodavatelů, pravidelné školení a ověřování bezpečnostního povědomí, kontrolu dodržování bezpečnostní politiky uživateli
	Organizační bezpečnost	4	2	4	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu výběru zaměstnanců a stanovení pracovních nápní zaměstnanců
nedostatečná odborná úroveň	Bezpečnost lidských zdrojů	6	4	4	pravidelné školení a ověřování bezpečnostního povědomí zamětnanců v souladu s jejich pracovní náplní
	Bezpečnostní role	2	1	2	dodržení minimální předepsané úrovně odbornosti - stanoveno pouze pro základní bezpečnostní role, nikoli celou organizační strukturu
přechod klíčového personálního aktiva ke konkurenci	Organizační bezpečnost	4	4	4	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu vyjednávání a uzavírání pracovních smluv
vyzrazení informací	Organizační bezpečnost	3	2	4	zajištění, aby byla zachovávána mlčenlivost administrátorů a osob zastávajících bezp. role. - vztahuje se pouze na vybrané skupiny
	Bezpečnost lidských zdrojů	6	4	4	poučení dodavatelů, pravidelné školení a ověřování bezpečnostního povědomí, kontrolu dodržování bezpečnostní politiky uživateli
	Řízení provozu a komunikací	2	1	1	pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu
nedostatečné předání agendy nebo ztráta know-how při odchodu zaměstnance nebo dodavatele	Bezpečnost lidských zdrojů	3	4	4	zajištění, aby v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role byla předána odpovědnost - omezeno na vybrané skupiny
	Organizační bezpečnost	3	4	4	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu odchodu zaměstnance nebo dodavatele
chybná identifikace personálních aktiv	Systém řízení bezpečnosti informací	3	4	4	určení organizačních částí a aktiv, kterých se systém řízení bezpečnosti týká

MAPOVACÍ TABULKA

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H1	zastaralost a nedostatečná údržba technického aktiva	Řízení změn	§11(1)(3)	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity	přezkoumávání dopadu změny, rozhodnutí o penetračním testování, testování zranitelností
porucha zařízení nebo chybné fungování aplikačního programového vybavení		Akvizice, vývoj a údržba	§13(f)	**Akvizice, vývoj a údržba** §13, písm. a), b), c), **Řízení změn** §11	bezpečnostní testování významných změn před uvedením do provozu, zákon požaduje jen u významných změn
		Organizační bezpečnost	§6(1)(c)(k)(g)	**Organizační bezpečnost** §6(3)(b - architekt KB), (c-garant aktiva), **Systém řízení bezpečnosti informací** §3	dostupnost zdrojů, dostatečné pravomoci nebo zdroje k požadované údržbě, dostatečná interní priorita
		Řízení provozu a komunikací	§10(1)(a)(e)(h)(f)	**Řízení aktiv, Řízení rizik, Organizační opatření** (metodiky chování uživatelů, definování komunikací)	řízení tech. zranitelnostní, sledování, plánování a řízení kapacity technického aktiva
		Řízení provozu a komunikací	§10(1)(b)	§15 **Řízení kontinuity činností**	pravidla spouštění, restartu systému, ošetření chybových stavů a mimořádných jevů; postup a zodpovědnosti dle plánu kontinuity činností či interních směrnic
		Zvládní kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	automatizovaný proces detekce kybernetických bezp. událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
		Zajišťování úrovně dostupnosti informací	§27	§15 **Řízení kontinuity činností**, **Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity, **Řízení prozovu a komunikací**	zajištění dostupnosti a redundance technických aktiv nezbytných pro provoz informačního a komunikačního systému, a to s ohledem na hodnocení podp. aktiv
		Průmyslové, řídící a obdobné systémy	§28 (e)(f)	**Řízení aktiv** §4, **Řízení rizik** §5	ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu - omezeno na průmyslové, řídící a obdobné specifické systémy
	nesprávná konfigurace technického aktiva	Řízení provozu a komunikací	§10(1)(a)(j)(g)	**Bezpečnost lidských zdrojů** §9(1)(a)(c)	pravidla a postupy pro instalaci technických aktiv a postupy řízení a schvalování provozních změn
		Bezpečnost lidských zdrojů	§9(1)(c)	opatření dle písm. a) a b)	bezpečnostní školení administrátorů, osob zastávajících bezpečnostní role a dodavatelů
		Akvizice, vývoj a údržba	§13(f)	opatření dle §13, písm. a), b), c)	bezpečnostní testování významných změn před uvedením do provozu, zákon požaduje jen u významných změn
		Řízení změn	§11(1)(3)	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity	přezkoumávání dopadu změny, rozhodnutí o penetračním testování, testování zranitelností
		Zvládní kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
	nejasné nebo neúplné zadání pro vývojáře, neodladěný nebo nový program	Akvizice, vývoj a údržba	§13(c)(d)(f)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	stanovení bezpečnostních požadavků a jejich zahrnutí do projektu vývoje a údržby informačního a komunikačního systému
		Řízení změn	§11	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity, **Organizační bezpečnost** §6, odst. 1, písm. c), k), g), §6(3)(b - architekt KB), na to navazuje **Bezpečnost lidských zdrojů** §9(1)(d)	přezkoumávání dopadu změny, rozhodnutí o penetračním testování, testování zranitelností
	žádné nebo nedostatečné testování programů	Aplikační bezpečnost	§25(1)	**Řízení změn** §11(1), **Řízení provozu a komunikací** §10(1)(g), **Řízení aktiv** §4	provádění penetračních testů se zaměřením na důležitá aktiva
		Řízení provozu a komunikací	§10(1)(a)(g)	**Řízení aktiva** §4, **Řízení rizik** §5	postupy řízení a schvalování provozních změn
	použití nevhodného nebo nekompatibilního technického aktiva (př. aktiva obsahujícího známé chyby)	**Řízení změn**	§11(1)	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity, **Organizační bezpečnost** §6, odst. 1, písm. c), k), g), §6(3)(b - architekt KB), na to navazuje **Bezpečnost lidských zdrojů** §9(1)(d)	přezkoumávání dopadu změny, u významných změn též provedení analýzy rizik
		Řízení provozu a komunikací	§10(1)(e)(g)	**Řízení změn** §11(1)	řízení technických zranitelností, schvalování provozních změn
		Průmyslové, řídící a obdobné systémy	§28(a)	**Řízení aktiv** §4, **Řízení rizik** §5	použití technických a programových prostředků určených do specifického prostředí - omezeno na průmyslové, řídící a obdobné specifiké systémy
		Akvizice, vývoj a údržba	§13(d)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	stavenovení požadavků na technické aktivum v projektu akvizice, vývoje a údržby, zákon vyžaduje pouze u významných změn

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H2	nedostatečná ochrana vnějšího perimetru, nesprávné uskladnění	**Fyzická bezpečnost**	§17(a)(c)	**Systém řízení bezpečnosti informací** §3, §17(b)	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
nedbalostní nebo úmyslné poškození, chyba použití		Ochrana před škodlivým kódem		§4(1)(h) - **Řízení aktiv,** odst. 1, písm. a) až g) jsou další podpůrná opatření	použití nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace; nasazováno s ohledem na důležitost aktiv
		Bezpečnost komunikačních sítí	§18(a)(b)(d)(e)	§4(1)(h) - **Řízení aktiv,** odst. 1, písm. a) až g) jsou další podpůrná opatření	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
		Průmyslové, řídící a obdobé systémy	§28(b)(c)	**Řízení aktiv** §4, **Řízení rizik** §5	omezení fyzického přístupu k zařízením průmyslových, řídících a obdobných specifických systémů; vyčlenění komunikační sítě určené pro průmyslové, řídící a obdobné specifické systémy od ostatní infrastruktury
		Řízení přístupových oprávnění	§12(1)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	řízení přístupu k jednotlivým aktivům
		Zvládání kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
	nedostatečné bezpečnostní povědomí uživatelů a nesprávná manipulace	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; předpokladem opatření jsou opatření v oblasti Bezpečnosti lidských zdrojů, ustanovení potřebných bezpečnostních rolí a Řízení provozu a komunikací
		Bezpečnost lidských zdrojů	§9(1) (i)	Bezpečnost lidských zdrojů - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	složité uživatelské rozhraní, nedostatečná dokumentace	Řízení změn	§11	**Řízení aktiv** §4, odst. 1, písm. f), g), opatření dle §4 odst. 1, písm. a) až e) jsou další prerekvizity.	přezkoumávání možných odpadů změny, funkční a nefunkční požadavky jsou zvažovány v širším kontextu hodnocení změny; hodnocení rizika změny je zákonem požadováno pouze u významných změn
		Bezpečnost lidských zdrojů	§9(1)(e)	**Organizační bezpečnost** §6	pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H3	nedostatečná ochrana perimetru - fyzického i virtuálního, nesprávné uskladnění	**Fyzická bezpečnost**	§17(a)(c)	§17(b), §4(1)(h) - **Řízení aktiv**, odst. 1, písm. a) až g) jsou další podpůrná opatření	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
ztráta, odcizení médií nebo dokumentů		Průmyslové, řídící a obdobné systémy	§28(b)	§4(1)(h) - **Řízení aktiv**, odst. 1, písm. a) až g) jsou další podpůrná opatření	omezení fyzického přístupu k zařízením průmyslových, řídících a obdobných specifických systémů
		Řízení přístupových oprávnění	§12(1)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	řízení přístupu k jednotlivým aktivům
		Správa a ověřování identit	§19	**Řízení přístupu** §12, **Řízení aktiv** §4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
		Bezpečnost lidských zdrojů	§9(1)(a)(c)(e)	**Systém řízení bezpečnosti informací** §3	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní
		Ochrana před škodlivým kódem	§21(1)(a)(e)	§4(1)(h) - **Řízení aktiv,** odst. 1, písm. a) až g) jsou další podpůrná opatření	nasazení nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace - nasazováno s ohledem naúdležitost aktiv
		Kryptografické prostředky	§26	**Řízení aktiv** §4(1)(i), **Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l), **Bezpečnost komunikačních sítí** §18	použití aktuálně odolných kryptografických algoritmů a klíčů
		Bezpečnost komunikačních sítí	§18(a)(b)(d)(e)	§4(1)(h) - **Řízení aktiv,** odst. 1, písm. a) až g) jsou další podpůrná opatření	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
		Aplikační bezpečnost	§25(2)	**Řízení přístupu** §12, **Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností
		Zvládání kybernetických událostí	§14(1)	§22-24 **Zaznamenávání událostí informačního systému**, §9 **Bezpečnost lidských zdrojů** - odst. 1, písm. a), c), d),e), h)	proces detekce kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů
	nedostatečné postupy likvidace	**Řízení aktiv**	§4(1)(j)	**Řízení aktiv** §4 odst. 1, písm. a) až g), §3 **Systém řízení bezpečnosti informací** §3	určení způsobu likvidace dat, provozních údajů, informací a jejich kopií nebo likvidace technických nosičů
	nekontrolované kopírování	Řízení provozu a komunikací	§10(1)(a)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g)	stanovení pravidel a postupů pro ochranu informací a dat v průběhu celého životního cyklu
		Bezpečnost lidských zdrojů	§9(1)(a)(c)(e)	**Systém řízení bezpečnosti informací** §3	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	nedostatečné bezpečnostní povědomí uživatelů (př. nedostatečné dodržování pravidel prázdného stolu a prázdné obrazovky monitoru)	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; předpokladem opatření jsou opatření v oblasti Bezpečnosti lidských zdrojů, ustanovení potřebných bezpečnostních rolí a Řízení provozu a komunikací
	nedostatečné monitorování činnosti uživatelů a neschopnost odhalit jejich nevhodné a závadné způsoby chování (př. nedostatečná kontrola práce externích zaměstnanců nebo	**Bezpečnost lidských zdrojů**	§9(1)(i)	**Systém řízení bezpečnosti informací** §3, **Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů** §22 odst.1, písm. a)	proces detekce kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů
	nedostatečný proces zálohování dat	**Řízení provozu a komunikací**	§10(1)(k)	§15 **Řízení kontinuity činností**, písm. b), bod 3	provádění pravidelného zálohování a kontroly použitelnosti provedených záloh
	nedostatečný schvalovací proces prostředků pro zpracování informací	**Řízení přístupových oprávnění**	§12(1)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	řízení přístupu k jednotlivým aktivům
		Bezpečnost lidských zdrojů	§9(1)(i)	**Organizační bezpečnost** §6	stanovení pravidel a postupů pro řešení případů porušení
	nedostatečná ochrana dat v testovacím a/nebo vývojovém prostředí	**Řízení provozu a komunikací**	§10(3)	**Řízení aktiv** §4(1)(i)	oddělení vývojového, testovacího a provozního prostředí
		Akvizice, vývoj a údržba	§13(e)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	zajištění bezpečnost vývojového a testevacího prostředí a ochrany používaných testovacích dat

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H4	nedostatečně či nevhodně stanovené přípustné způsoby užívání a manipulace s technickým aktivem	**Řízení aktiv**	§4(1)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g), **Systém řízení bezpečnosti informací** §3, **Bezpečnostní role** §7(3)	stanovení přípustných způsobů používání aktiva
zneužití vnitřních prostředků (např. použití pro osobní účely, použití k jinému než legálnímu účelu)	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů; předpokladem opatření jsou opatření v oblasti Bezpečnosti lidských zdrojů, ustanovení potřebných bezpečnostních rolí a Řízení provozu a komunikací
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	nedostatečné monitorování činnosti uživatelů a neschopnost odhalit jejich nevhodné a závadné způsoby chování (vč. neprovádění logování, nedostatečné postupy pro zjištění bezpečnostních slabin)	**Bezpečnost lidských zdrojů**	§9(1)(i)	**Systém řízení bezpečnosti informací** §3, **Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
		Aplikační bezpečnost	§25(2)	**Řízení přístupu** §12, **Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
	vyřazení nebo opětovné použití záznamových médií bez důkladného vymazání	**Řízení aktiv**	§4(1)(j)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4 odst. 1, písm. a) až g)	určení způsobu likvidace dat, provozních údajů, informací a jejich technických nosičů
	chybné přiřazení přístupových práv	**Řízení přístupu**	§12(1)(2)	**Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	řízení přístupu k jednotlivým aktivům
	nedostatečné postupy při identifikaci uživatele	**Správa a ověřování identit**	§19	**Řízení přístupu** §12, **Řízení aktiv** §4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
	použití produkčních dat ve vývojovém a/nebo testovacím prostředí	**Řízení provozu a komunikací**	§10(3)	**Řízení aktiva** §4	oddělení vývojového, testovacího a provozního prostředí
		Akvizice, vývoj a údržba	§13(e)	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	zajištění bezpečnosti vývojového a testovacího prostředí a ochrany používaných testovacích dat
	porušení mlčenlivosti uživatelů (smluvní nebo zákonné)	**Organizační bezpečnost**	§6(1)(j)	**Systém řízení bezpečnosti informací** §3	zajištění, aby byla zachovávána mlčenlivost administrátorů a osob zastávajících bezpečnostní role
		Bezpečnost lidských zdrojů	§9(1)(c)(e)(h)(f)	**Systém řízení bezpečnosti informací** §3, **Bezpečnost lidských zdrojů** §9 opatření dle písm. a) a b)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů; předpokladem opatření jsou opatření v oblasti Bezpečnosti lidských zdrojů, ustanovení potřebných bezpečnostních rolí a Řízení provozu a komunikací
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H5	nedostatečná identifikace a autentizace, např. autentizace uživatele, nechráněné tabulky s hesly, špatná správa hesel	**Aplikační bezpečnost**	§25(2)(a)	**Řízení přístupu** §12, **Systém řízení bezpečnosti informací** §3, **Řízení aktiv** §4(1)(a)-(i), **Bezpečnostní role** §7(3), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností
zneužití identity	nedostatečné postupy při identifikaci uživatele	**Správa a ověřování identit**	§19	**Řízení přístupu** §12, **Řízení aktiv** §4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
	neodhlášení se při opuštění pracovní stanice	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Systém řízení bezpečnosti informací** §3, **Bezpečnost lidských zdrojů** §9 opatření dle písm. a) a b)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů
	neodebrání přístupu při skončení zaměstnání / změně pozice	**Řízení přístupu**	§12(2)(m)(l)	§20(a) **Řízení přístupových oprávnění**	odebrání nebo změna přístupových oprávnění při změně pozice, zařazení, změně smluvného vztahu
H6	nedostatečná ochrana vnějšího perimetru (př. poloha v záplavové oblasti; prašné, vlhké prostředí)	**Fyzická bezpečnost**	§17(a)(c)	§17(b), §4(1)(h) - **Řízení aktiv**, odst. 1, písm. a) až g) jsou další podpůrná opatření	předcházení poškození, krádeži, zneužití aktiva nebo přerušení poskytování služeb, stanovení fyzického bezpečnostního perimetru
Zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)		**Řízení kontinuity činností**	§15(e)	§4 **Řízení aktiv**, **Řízení rizik** §5	havarijní plány
H7	použití neautorizovaného HW (vyměnitelné technické nosiče ve vlastnictví 3. osoby), nedostatky ve formální politice pro používání mobilních zařízení	**Ochrana před škodlivým kódem**	§21(1)(b)	**Řízení aktiv** §4(1)(i)**, Řízení přístupu** §12	monitoring používání výměnných zařízení a datových nosičů
Zneužití vyměnitelných technických nosičů dat		**Řízení přístupu**	§12(2)(e)	**Řízení aktiv** §4(1)(i)	stanovení bezpečnostních opatření pro používání mobilních zařízení a jiných technických zařízení, která povinná osoba nemá ve své správě
	vyřazení nebo opětovné použití záznamových médií bez důkladného vymazání	**Řízení aktiv**	§4(1)(j)	**Řízení aktiv** §4 odst. 1, písm. a) až g)	určení způsobu likvidace technických nosičů dat s ohledem na úroveň aktiv
	nedostatečné kontroly zařízení mimo lokalitu	Řízení aktiv	§4(1)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g)	stanovení přípustných způsobů používání aktiva
	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
H8	použití aplikačních programů na špatná data z hlediska času	**Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů**	§22(2)(e)	**Systém řízení bezpečnosti informací** §3	zajištění synchronizace jednotného času technických aktiv nejméně jednou za 24h
poškození dat použitím aplikačních programů na špatná data z hlediska času					

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H9	užití programových prostředků schopných překonat systémové nebo aplikační kontroly	**Aplikační bezpečnost**	§25(2)(a)	**Řízení provozu a komunikací** §10	ochrana aplikací, informací a transakcí před neoprávněnou činností
provedení neoprávněných činností, tj. provedení činností k nimž uživatel nemá oprávnění		Průmyslové, řídící a obdobné systémy	§28(d)	**Řízení aktiv** §4, **Řízení rizik** §5	omezení vzdáleného přístupu k těmto systémům
		Bezpečnost komunikačních sítí	§18(a)(b)(d)(e)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní; zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** - §9, odst. 1, písm. c), e)	pravidla a postupy pro řešení případů bezpečnostních pravidel uživateli
	nedostatečné postupy při identifikaci uživatele	**Správa a ověřování identit**	§19	**Řízení přístupu** §12, **Řízení aktiv** §4	nasazení nástroje pro správu a ověření identity uživatelů, autentizační mechanismus
	nedostatečné monitorování činnosti uživatelů a administrátorů, neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	**Bezpečnost lidských zdrojů**	§9(1)(i)	**Bezpečnost lidských zdrojů** §9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Zvládání kybernetických bezpečnostní incidentů** §14, **Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
	nedostatečné nastavení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**Organizační bezpečnost**	§6(i)	**Systém řízení bezpečnosti informací** §3	stanovení pravidel pro určení administrátorů
		Řízení přístupových oprávnění	§20(b)	**Řízení aktiv** §4	použití centralizovaného nástroje pro řízení přístupových oprávnění k akivům
		Řízení provozu a komunikací	§10(1)(a)	**Řízení aktiv** §4	stanovení práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role
H10	nedostatečné nastavení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	Organizační bezpečnost	§6(i)	**Systém řízení bezpečnosti informací** §3	stanovení pravidel pro určení administrátorů
zneužití oprávnění ze strany uživatelů a administrátorů, tj. provedení činností k nimž uživateli bylo uděleno oprávnění k jinému než zamýšlenému účelu		Řízení přístupových oprávnění	§20(b)	**Řízení aktiv** §4	použití centralizovaného nástroje pro řízení přístupových oprávnění k aktivům
		Řízení provozu a komunikací	§10(1)(a)	**Řízení aktiv** §4	stanovení práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role
	neodebrání přístupových oprávnění při skončení zaměstnání / změně pozice	**Řízení přístupu**	§12(1)(m)(l)		odebrání nebo změna přístupových oprávnění při ukončení nebo změně smluvního vztahu nebo pozice
	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** §9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
H11	nedostatečně bezpečná síťová infastruktura, nechráněné komunikační linky	**Bezpečnost komunikačních sítí**	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace stě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
vzdálená špionáž	přenos odkrytých hesel, použití nedostatečně odolných hesel	**Správa a ověřování identit**	§19	**Řízení přístupu** §12(1)(2)(b), **Kryptografické prostředky** §26	zajištění odolnosti uložených a přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití; vynucování minimálních standardů pro tvorbu hesla
	nechráněný citlivý provoz přenosu	**Kryptografické prostředky**	§26	**Řízení aktiv** §4(1)(i), **Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l), **Bezpečnost komunikačních sítí** §18	použití aktuálně odolných kryptografických algoritmů a klíčů

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H12	nedostatečně bezpečná síťová infastruktura, nechráněné komunikační linky	**Bezpečnost komunikačních sítí**	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace sítě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
odposlech	nechráněné připojení do veřejné sítě	**Kryptografické prostředky**	§26	**Řízení aktiv** §4(1)(i), **Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l), **Bezpečnost komunikačních sítí** §18	použití aktuálně odolných kryptografických algoritmů a klíčů
		Bezpečnost komunikačních sítí	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace sítě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
H13	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik		**Bezpečnost lidských zdrojů**	§9(1)(i)	**Bezpečnost lidských zdrojů** §9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
	nekontrolované stahování a užívání programů, nedostatečné postupy pro instalaci software do operačních systémů	Řízení aktiv	§4(1)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g), **Organizační bezpečnost** §6(3)(c) - stanovení garanta aktiva	stanovení přípustných způsobů používání aktiva a pravidla manipulace s aktivy s ohledem na úroveň aktiv
		Řízení přístupu	§12(2)(g)	**Aplikační bezpenost** §25(2), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	omezení a kontrola používání programových prostředků schopných překonat systémové nebo aplikační kontroly
		Bezpečnost komunikačních sítí	§18(d)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(j)(e)	aktivní blokace nežádoucí komunikace
	nechráněné připojení do veřejné sítě	**Bezpečnost komunikačních sítí**	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace sítě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
	použití nedostatečně odolných hesel	**Správa a ověřování identit**	§19	**Řízení přístupu** §12(1)(2)(b)	zajištění odolnosti uložených a přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití, vynucování minimálních standardů pro tvorbu hesla
H14	nechráněné připojení do veřejné sítě	**Bezpečnost komunikačních sítí**	§18	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(l)	segmentace sítě, řízení komunikace v rámci sítě, kryptografie, blokace nežádoucí komunikace, využití nástroje pro ochranu integrity komunikační sítě
instalace zákeřného kódu		**Zvládní kybernetických událostí**	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobyklého chování a podezření na zranitelnosti uživateli
		Ochrana před škodlivým kódem	§21(1)(a)(e)	**Řízení provozu a komunikací** §10	použití nástroje pro nepřetržitou automatizovanou ochranu před škodlivým kódem a jeho pravidelná aktualizace - nasazováno s ohledem na důležitost aktiv
		Řízení provozu a komunikací	§10(l)(d)	**Řízení aktiv** §4, **Řízení rizik** §5	pravidla a postupy pro zajištění bezpečností síťových služeb, pravidla a postupy pro ochranu před škodlivým kódem
	nedostatečné školení uživatelů a kontrola dodržování ze strany managementu	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, administrátorů, osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
		Bezpečnost lidských zdrojů	§9(1)(i)	**Bezpečnost lidských zdrojů** §9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
	veřejná publikace zdrojového kódu software	Akvizice, vývoj a údržba	§13	**Systém řízení bezpečnosti informací** §3(b), Řízení aktiv §4(1)(h), **Řízení rizik** §5, **Řízení změn** §11	stavenovení požadavků na technické aktivum v projektu akvizice, vývoje a údržby
		Řízení změn	§11	**Systém řízení bezpečnosti informací** §3	analýza rizik, přijetí opatření za účelem snížení nepříznivých dopadů změny
	nekontrolované stahování a užívání programů, používání programů obsahujících známé chyby	Řízení aktiv	§4(1)(i)	**Řízení aktiv** §4 odst. 1, písm. a) až g), **Organizační bezpečnost** §6(3)(c) - stanovení garanta aktiva	stanovení přípustných způsobů používání aktiva a pravidel manipulace s aktivy s ohledem na úroveň aktiv
		Řízení přístupu	§12(2)(g)	**Aplikační bezpenost** §25(2), **Správa a ověřování identit** §19, **Řízení přístupových oprávnění** §20	omezení a kontrola používání programových prostředků schopných překonat systémové nebo aplikační kontroly
		Bezpečnost komunikačních sítí	§18(d)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(j)(e)	aktivní blokace nežádoucí komunikace

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H15	neexistence potřebné smlouvy (licenční, nájemní, kupní), nedostatečná oprávnění druhé smluvní strany (poskytovatele licence, prodávajícího, pronajímatele), nevhodná formulace smluvních ustanovení	**Řízení dodavatelů**	§8(1)(a),(f)	**Organizační bezpečnost -** §6 odst. 1, písm. c), k), §6(3)(c)	příloha 7, písm. b) - oprávnění užívat data, c) - autorství programového kódu; požadevek dle písm. f) omezen na významné dodavatele
neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	nedostatečné postupy pro zajištění souladu se zákony na ochranu duševního vlastnictví	**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti informací** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu akvizice předmětů chráněných duševním vlastnictvím
	nedostatky ve formálním procesu pro autorizaci veřejně přístupných informací (>> data pocházejí z nedůvěryhodných zdrojů)	**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti informací** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu využití veřejně dostupných dat
H16	nedostatečné postupy při identifikování a odhalení bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	Řízení provozu a komunikací	§10(1)(c)	**Řízení rizik** §5	postupy pro sledování kybernetických bezpečnostních událostí
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb		**Zvládání kybernetických událostí**	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobvyklého chování a podezření na zranitelnosti uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
	nedostatečná nebo neúplná smlouva o úrovni služeb, porušení smlouvy o úrovni služeb	**Řízení dodavatelů**	§8(1)(a),(d) - všichni, §8(2)(a),(b), příl. 7 písm. k) - významní	**Řízení kontinuity činností** §15(c)	stanovení pravidel pro dodavatele a jejich pravidelné přezkoumávání, u významných též dle přílohy 7 písm. k) - specifikace podmínek pro řízení kontinuity činností
		Řízení provozu a komunikací	§10(1)(a)(f)	**Bezpečnost lidských zdrojů** §9(1)(a)(c)(e)	spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory
	selhání v důsledku přetížení sítě (odolnost směřování)	**Bezpečnost komunikačních sítí**	§18(a)(b)(d)(e)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(j)(e)	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobvyklého chování a podezření na zranitelnosti uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
		Průmyslové, řídící a obdobné systémy	§28(c)(e)(f)	**Řízení aktiv** §4, **Řízení rizik** §5	ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu, vyčlenění od ostatní infastruktury - omezeno na průmyslové, řídící a obdobné specifické systémy
		Zajišťování úrovně dostupnosti informací	§27	§15(c) **Řízení kontinuity činností** , §4 **Řízení aktiv**, **Řízení rizik** §5, **Organizační bezpečnost** §6(3)	zajištění dostupnosti a redundance technických aktiv nezbytných pro provoz informačního a komunikačního systému a to s ohledem na hodnocení podpůrných aktiv
	nedostatky v plánech kontinuity	**Řízení kontinuity činností**	§15	**Systém řízení bezpečnosti informací** §3	plány kontinuity činností
	celkové selhání služby	**Zajišťování úrovně dostupnosti informací**	§27	**Řízení provozu a komunikací** §10, **Řízení kontinuity činností** §15	zajištění redundancie aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému; předpokladem je stanovení dostatečné doby pro obnovení chodu

Technická aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H17	nedostatečná nebo neúplná smlouva o úrovni služeb, porušení smlouvy o úrovni služeb	**Řízení dodavatelů**	§8(1)(a),(d) - všichni, §8(2)(a),(b), příl. 7 písm. k) - významní	**Řízení kontinuity činností** §15(c)	stanovení pravidel pro dodavatele a jejich pravidelné přezkoumávání, u významných též dle přílohy 7 písm. k) - specifikace podmínek pro řízení kontinuity činností
přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie		**Řízení provozu a komunikací**	§10(1)(a)(f)	**Bezpečnost lidských zdrojů** §9(1)(a)(c)(e)	spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory
	selhání v důsledku přetížení sítě (odolnost směřování)	**Bezpečnost komunikačních sítí**	§18(a)(b)(d)(e)	**Systém řízení bezpečnosti informací** §3(c), **Řízení provozu a komunikací** §10(1)(j)(e)	segmentace komunikační sítě, řízení komunikace, blokace nežádoucí komunikace a využití nástroje pro ochranu integrity komunikační sítě
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobvyklého chování a podezření na zranitelnosti uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
		Průmyslové, řídící a obdobné systémy	§28(c)(e)(f)	**Řízení aktiv** §4, **Řízení rizik** §5	ochrana technických aktiv před využitím známých zranitelností a obnova chodu po kybernetickém bezpečnostním incidentu, vyčlenění od ostatní infastruktury - omezeno na průmyslové, řídící a obdobné specifické systémy
		Řízení kontinuity činností	§15	§4 **Řízení aktiv**, **Řízení rizik** §5, **Organizační bezpečnost** §6(3)	stanovení politiky a plánu kontinuity činností a provádí opatření ke zvýšení odolnosti systému
	nedostatečné postupy při identifikování a odhalení bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	Řízení provozu a komunikací	§10(1)(c)	**Řízení rizik** §5	postupy pro sledování kybernetických bezpečnostních událostí
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	automatizovaný proces detekce kybernetických bezpečnostních událostí a hlášení neobvyklého chování a podezření na zranitelnosti uživateli
		Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	§22	**Řízení aktiv** §4	zaznamenávání bezpečnostních a potřebných provozních událostí důležitých aktiv
H18	nedostatečné bezpečnostní školení	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Systém řízení bezpečnosti informací** §3	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
porušení bezpečnostní politiky		**Bezpečnost lidských zdrojů**	§9(1)(i)	§9(1)(c)(e)(h)(f), **Systém řízení bezpečnosti informací** §3	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
		Zvládání kybernetických událostí	§14(1)	**Zaznamenávání událostí informačního systému** §22-24	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
	nedostatečné provádění pravidelných auditů / dohledu	Audit kybernetické bezpečnosti	§16	**Systém řízení bezpečnosti informací** §3	pravidelný audit kybernetické bezpečnosti
H19	nedostatky v postupech pro identifikaci a posouzení rizik	**Systém řízení bezpečnosti informací**	§3	N/A	určení organizačních částí a aktiv, kterých se systém řízení bezpečnosti týká
chybná identifikace technických aktiv					

Personální aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H20	neschopnost ověřit kvalifikaci subdodavatele v rámci výběrového řízení	Řízení dodavatelů	§8(2)	**Řízení rizik** §5	hodnocení rizik v rámci výběrového řízení a před uzavřením smlouvy - omezeno na významné dodavatele
nedodržení smluvního závazku ze strany subdodavatele		**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu výběru subdodavatelů
	nejednoznačná / nedostatečná definice závazku subdodavatele	**Řízení dodavatelů**	§8(1)(a)(d)(f)(2)(b)	**Systém řízení bezpečnosti** §3	stanovení pravidel pro dodavatele, seznámení dodavatele s pravidly, u významných stanovení způsobů a úrovní realizace bezpečnostních oprávnění a rozsah vzájemné smluvní odpovědnosti
	neschopnost včasného odhalení pochybení ze strany subdodavatelů	**Řízení dodavatelů**	§8(1)(g)(2)(c)	**Systém řízení bezpečnosti** §3, **Řízení rizik** §5	pravidelné přezkoumávání smluv s významnými dodavateli, hodnocení rizik a pravidelná kontrola zavedených bezpečnostních opatření - omezeno na významné dodavatele
		Bezpečnost lidských zdrojů	§9(1)(c)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení dodavatelů o jejich povinnostech, pravidelné školení, kontrola dodržování, hodnocení účinnosti
		Bezpečnost lidských zdrojů	§9(1)(i)	§9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
H21	nedostatečné poučení / vzdělávání zaměstnanců	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)(h)(f)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b), **Řízení aktiv §4(1)(i), Organizační bezpečnost** - §6, odst. 1, písm. c) - g), k) a dále stanovení **Bezpečnostních rolí** - §6(3)(a - manažer), b - architekt KB), (c-garant aktiva), **Řízení provozu a komunikací** - §10(1)(a)(b)(g)(i)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení
pochybení ze strany zaměstnanců (včetně trestné činnosti)	nejednoznačná / nedostatečná definice povinností zaměstnance	Organizační bezpečnost	§6(1)(b)	**Systém řízení bezpečnosti informací** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu stanovení pracovních nápní zaměstnanců
	neschopnost včasného odhalení pochybení ze strany zaměstnanců	**Bezpečnost lidských zdrojů**	§9(1)(f)(h)	§9(1)(c)(e) - **Bezpečnost lidských zdrojů**	kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů, osob zastávající bezpečnostní role, hodnocení účinnosti plánu rozvoje bezpečnostního povědomí
		Bezpečnost lidských zdrojů	§9(1)(i)	§9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
	neschopnost identifikace problematických vzorců chováním v rámci výběrového řízení	Organizační bezpečnost	§6(1)(b)	**Systém řízení bezpečnosti informací** §3	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu výběru zaměstnanců

Personální aktiva					
Hrozba	Zranitelnost	Kategorie opatření	Ustanovení	Prerekvizity opatření	Stručný popis opatření
H22	nedostatečné vzdělávání zaměstnanců	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení
nedostatečná odborná úroveň	neschopnost ověřit kvalifikaci uchazeče v rámci výběrového řízení	Bezpečnostní role	§7	§6 **Organizační bezpečnost** - odst. 3 až 6 - povinnost ustanovit bezpečnostní role	úroveň vzdělání stanovena pouze pro vymezené bezpečnostní Rrole
	nedostatečná míra nezávislé kontroly s cílem včas identifikovat chybějící odbornost	**Bezpečnost lidských zdrojů**	§9(1)(i)	§9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
H23	absence konkureční doložky ve smlouvě	**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu vyjednávání a uzavírání pracovních smluv
přechod klíčového personálního aktiva ke konkurenci					
H24	absence ujednání o zachovávání mlčenlivosti i po odchodu / zákonného povinnosti mlčenlivosti	**Organizační bezpečnost**	§6(1)(j)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	zajištění, aby byla zachovávána mlčenlivost administrátorů a osob zastávajících bezpečnostní role - vztahuje se pouze na vybrané skupiny
vyzrazení informací		Řízení provozu a komunikací	§10(1)(i)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu
	nedostatečné poučení příjemců	**Bezpečnost lidských zdrojů**	§9(1)(c)(e)	**Bezpečnost lidských zdrojů** - §9, opatření dle písm. a) a b)	poučení uživatelů, administrátorů , osob zastávajících bezpečností role a dodavatelů o jejich povinnostech, pravidelné školení
		Bezpečnost lidských zdrojů	§9(1)(i)	§9(1)(c)(e)(h)(f)	pravidla a postupy pro řešení případů porušení bezpečnostních pravidel uživateli
H25	neexistující / nedostatečná exit procedura	**Bezpečnost lidských zdrojů**	§9(1)(g)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	zajištění, aby v případě ukončení sml. vztahu s administrátory a osobami zastávajícími bezp. role byla předána odpovědnost - omezeno na vybrané skupiny
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance / dodavatele		**Organizační bezpečnost**	§6(1)(b)	**Systém řízení bezpečnosti informací** §3, **Řízení rizik** §5	integrace systému řízení bezpečnosti informací do procesů povinné osoby, tj. i do procesu odchodu zaměstnance / dodavatele
H26	nedostatky v postupech pro identifikaci a posouzení rizik	**Systém řízení bezpečnosti informací**	§3	N/A	určení organizačních částí a aktiv, kterých se systém řízení bezpečnosti týká
chybná identifikace personálních aktiv					

SEZNAM POUŽITÝCH ZDROJŮ:

[1] *Metodika k vodítkům pro hodnocení dopadů* [online]. Národní úřad pro kybernetickou a informační bezpečnost. 1.2. Česká republika, 2018 [cit. 2019-12-30]. Dostupné z https://www.govcert.cz/download/kii-vis/Metodika_k_voditkum_pro_hodnoceni_dopadu_NUKIB_v.1.2_s_prilohou.pdf

[2] *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)* . In: *Sbírka zákonů* . 28.5.2018. ISSN 1211-1244

Příloha 3: Použití metodiky hodnocení dodavatele – příklad

Obsah:

HODNOCENÍ RIZIKA

Hodnocené podpůrné aktivum (předmět dodávky)	Primární aktivum[1]	Hodnocení důležitosti primárního aktiva	Hodnocení důležitosti podpůrného aktiva[2]			Hodnocení rizika podpůrného aktiva	Hrozba[3]	Zkratka	Hodnocení závažnosti hrozby[2]	Hodnocení závažnosti dopadů (tj. dopad porušení důvěrnosti, dostupnosti nebo integrity aktiva)[2] [1]				Riziko, včetně korekce hodnocením primárního aktiva[2]
			Důvěrnost	Dostupnost	Integrita					Ochrana osobních údajů	Zákonné a smluvní povinnosti	Ztráta důvěryhodnosti	Finanční ztráty	
zakázkový vývoj software, nezahrnuje služby podpory a údržby software v produkčním prostředí. Nepředpokládá se předání osobních údajů Nepředpokládá se přístup dodavatele na produkční prostředí.	*Primární aktivum 1*	1	4	1	3	Technická aktiva (hardwarové a softwarové vybavení, média a dokumenty)[4]	porucha zařízení nebo chybné fungování aplikačního programového vybavení	H1	4	2	2	3	3	3
	Primární aktivum 2	3					nedbalostní nebo úmyslné poškození, chyba použití	H2	1	1	1	1	1	1
							ztráta, odcizení médií nebo dokumentů	H3	2	1	1	1	3	3
							zneužití vnitřních prostředků (použití pro osobní účely, použití k jinému než legálnímu účelu), zneužití oprávnění	H4	0					0
							zneužití identity, falšování zpráv	H5	0					0
							zničení nebo poškození zařízení v důsledku změn prostředí (změny vlhkosti, teploty ale i přírodní katastrofy)	H6	1	1	1	1	1	1
							zneužití vyměnitelných technických nosičů dat a mobilních zařízení	H7	2	1	1	1	3	3
							poškození dat použitím aplikačních programů na špatná data z hlediska času	H8	0					0
							provedení neoprávněných činností, tj. činností k nimž uživatel nemá oprávnění	H9	0					0
							zneužití oprávnění ze strany uživatelů[5] a administrátorů	H10	2	2	1	3	3	3
							vzdálená špionáž	H11	1	1	1	1	1	1
							odposlech	H12	1	1	1	1	1	1
							cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	H13	2	1	1	1	1	2
							instalace zákeřného kódu	H14	3	2	3	1	3	3
							neoprávněné užití technického aktiva, tj. použití bez licence, použití nad rámec licence, použití bez oprávnění	H15	4	1	3	1	3	3
							dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky el. energie nebo jiných důležitých služeb	H16	2	1	1	1	2	2
							přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	H17	0					
							porušení bezpečnostní politiky	H18	3	1	1	1	1	2
							chybná identifikace technických aktiv	H19	2	1	1	1	1	2
						Personální aktiva	nedodržení smluvního závazku ze strany subdodavatele	H20	3	1	1	1	1	2
							pochybení ze strany zaměstnanců (včetně trestné činnosti)	H21	4	1	1	1	1	3
							nedostatečná odborná úroveň nebo bezpečnostní kvalifikace	H22	4	2	1	1	2	3
							přechod klíčového personálního aktiva ke konkurenci	H23	3	1	1	1	1	2
							vyzrazení informací	H24	4	1	1	3	2	3
							nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance ze společnosti	H25	3	1	1	1	2	3
							chybná identifikace personálních aktiv	H26	2	1	1	1	1	2

POZNÁMKY POD ČAROU

1 Primárním aktivem je vždy služba, kterou zpracovává nebo poskytuje informační a komunikační systém.

2 viz. návod pro vyplnění

3 Hrozby, kterými jsou ohrožena daná aktiva, nikoli hrozby, jejichž aktéry jsou daná aktiva. Př. Zaměstnanci mohou být původci většiny hrozeb, které ohrožují technická aktiva.

4 Zahrnuje hrozby ohrožující fyzická média, data na nich uložená, jakož i dokumentu ve fyzické podobě

5 Uživatelé zahrnují jak zaměstnance povinné osoby, tak jejích dodavatelů

TECHNICKÁ AKTIVA	Riziko	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																								
		ORGANIZAČNÍ OPATŘENÍ													TECHNICKÁ OPATŘENÍ											
HROZBA		Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídící a obdobné systémy
porucha zařízení nebo chybné fungování aplikačního programového vybavení	3				2			2	4	3		4	3												2	
nedbalostní nebo úmyslné poškození, chyba použití	1							4																		
ztráta, odcizení médií nebo dokumentů	3		2					4	2				3			3		4	4	3	3	3	3		2		
zničení nebo poškození zařízení v důsledku změn prostředí	1															4											
zneužití vyměnitelných technických nosičů dat	3		3					4			2									2							
zneužití oprávnění ze strany uživatelů a administrátorů	3				4			4	4		4								2								
vzdálená špionáž	1																	4									
odposlech	1																4										
cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	2							4									3	3									
instalace zákeřného kódu	3							4	4	2		4	2				3			4		2	2				
neoprávněné užití technického aktiva	3				4		4																				
dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2						4		4				3	3							3		3			3	
porušení bezpečnostní politiky	2							4																			
chybná identifikace technických aktiv	2	4																									

PERSONÁLNÍ AKTIVA	Riziko	DRUH OPATŘENÍ A JEHO VÝZNAM Z HLEDISKA PŘEDCHÁZENÍ ČI SNIŽOVÁNÍ DOPADŮ HROZBY																								
		ORGANIZAČNÍ OPATŘENÍ														TECHNICKÁ OPATŘENÍ										
HROZBA		Systém řízení bezpečnosti informací	Řízení aktiv	Řízení rizik	Organizační bezpečnost	Bezpečnostní role	Řízení dodavatelů	Bezpečnost lidských zdrojů	Řízení provozu a komunikací	Řízení změn	Řízení přístupu	Akvizice vývoj a údržba	Zvládání kybernetických bezpečnostních událostí a incidentů	Řízení kontinuity činností	Audit kybernetické bezpečnosti	Fyzická bezpečnost	Bezpečnost komunikačních sítí	Správa a ověřování identit	Řízení přístupových oprávnění	Ochrana před škodlivým kódem	Zaznamenávání událostí informačního a komunikačního systému	Detekce kybernetických bezpečnostních událostí	Sběr a vyhodnocování kybernetických bezpečnostních událostí	Aplikační bezpečnost	Kryptografické prostředky	Zajišťování úrovně dostupnosti informací	Průmyslové, řídící a obdobné systémy
nedodržení smluvního závazku ze strany subdodavatele	2				3		4	3																		
pochybení ze strany zaměstnanců (včetně trestné činnosti)	3				4			4																		
nedostatečná odborná úroveň	3					2		4																		
přechod klíčového personálního aktiva ke konkurenci	2				4																					
vyzrazení informací	3				4			4																		
nedostatečné předání agendy / ztráta know-how při odchodu zaměstnance / dodavatele	3				4			4																		
chybná identifikace personálních aktiv	2	4																								

SEZNAM OPATŘENÍ K IMPLEMENTACI

ORGANIZAČNÍ OPATŘENÍ			
Kategorie opatření	Potřebná úroveň	Hrozba	Požadavky na dodavatele
Systém řízení bezpečnosti informací	4	H19	Pravidelně vyhodnotuje organizační části a aktiva, která jsou využívaná k poskytování plnění odběratelské společnosti
Organizační bezpečnost	4	H15	Stanovil pravidla pro užití statků chráněných právy duševního vlastnictví.
			Vede evidenci platných licencí, vč. data jejich expirace.
	4	H10	Stanovil pravidla pro určení administrátorů a osob zastávajících bezpečnostní role
	4	H21	Stanovil pravidla pro výběr zaměstnanců.
			Ověřuje kvalifikaci uchazečů o zaměstnání (př. testování).
			Ověřuje reference předchozích zaměstnavatelů uchazečů o zaměstnání.
			Zaměstnanci mají jasně definovanou pracovní náplň a zodpovědnosti.
	4	H23	V pracovních smlouvách klíčových zaměstnanců a sub-dodavatelů je upravena konkurenční doložka zakazující práci pro subjekt v konkurečním postavení k dodavateli po určitou dobu po skončení smluvního vztahu s dodavatelem.
	4	H24	Zaměstnanci a dodavatelé jsou vázáni zákonnou povinností mlčenlivosti.
			Zaměstnanci a dodavatelé jsou vázáni smluvní povinností mlčenlivosti.
			Zaměsnanci a dodavatelé byli poučeni o důvěrnosti zpracovávaných informací.
	4	H25	Sub-dodavatelé jsou smluvně vázáni poskytnout podporu dodavateli při ukončení spolupráce.
			Zajišťuje předání práce zaměstnancem při ukončení pracovního poměru.
			Odcházející zaměstnanec je povinen zaškolit zaměstnance, kterému jsou předávány úkoly odcházejícího zaměstnance.
	3	H20	Stanovil pravidla pro výběr dodavatelů.
			Ověřuje reference potenciálního dodavatele.
			Ověřuje kvalifikaci (dostupné zdroje - personální i finační) potenciálního dodavatele.
	2	H1	Osoby zastávající bezpečnostní role mají dostatečné zdroje (vč. finančních).
			Osoby zastávající bezpečnostní role mají dostatečné pravomoci.
			Dodavatel prosazuje systém řízení bezpečnosti informací a věnuje mu dostatečné zdroje.
Bezpečnostní role	2	H22	Osoby zastávající bezpečnostní role mají předepsanou kvalifikaci.
Řízení dodavatelů	4	H15	Smlouvy se sub-dodavateli zajišťují oprávnění k užívání dat.

			Smlouvy s sub-dodavateli obsahují dostatečné licenční ujednání.
	4	H20	Stanovil pravidla pro sub-dodavatele, která zohledňují požadavky řízení bezpečnosti informací.
			Seznamuje sub-dodavatele s pravidly týkajícími se řízení bezpečnosti informací
			V případě významných dodavatelů, provádí v průběhu výběrového řízení a před uzavřením smlouvy, provádí hodnocení rizik.
			Zajišťuje, aby se jeho významní dodavatele zavázali dodržovat pravidla bezpečnosti informací ve stejném rozsahu, v jakém je zavázán dodavatel ve vztahu k objednateli.
	4	H16	Stanovil pravidla pro sub-dodavatele (zejm. z hlediska dostupnosti služeb).
			V případě významných dodavatelů smluvně upravuje řízení kontinuity činností souvisejících s dodavateli.
Bezpečnost lidských drojů	4	H1, H2, H3, H7, H10, H13, H14, H18	Zajišťuje pravidelná školení zaměstnanců, uživatelů, administrátorů, osob zastávajících bezpečnostních role o jejich povinnostech a bezpečnostní politice.
	4		Zajišťuje pravidelná bepečnostní školení sub-dodavatelů o jejich povinnostech a bezpečnostní politice.
	4		Provádí pravidelné ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.
	4		Zajišťuje pravidelná odborná školení osob zastávajících bezpečnostní role.
	4		Zajišťuje kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
	4		Zajišťuje, aby v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role byla předána odpovědnost osobě, která bude nadále pozici zastávat.
	4		Určil pravidla a postupy řešení případů porušení stanovených bezpečnostních pravidel.
Řízení provozu a komunikací	4	H1	Stanovil práva a povinnosti administrátorů, uživatelů a osob zastavajících bezpečnostní role.
			Řídí technické zranitelnosti
			Stanovil postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.
			Identifikoval kontaktní osoby pověřené výkonem systémové a technické podpory. Zajistil spojení na tyto osoby.
	2	H3	Vývojové, testovací a provozní prostředí jsou oddělené.
			Provádí pravidelné zálohování dat
			Provádí pravidelnou kontrolu použitelnosti provedených záloh.

			Stanovil pravidla a postupy pro ochranu informací a dat v průběhu celého životného cyklu.
	4	H10	Stanovil práva a povinnosti administrátorů, uživatelů a osob zastavajících bezpečnostní role.
	4	H14	Stanovil pravidla a postupy pro zajištění bezpečnosti síťových služeb.
			Stanovil pravidla a postupy pro ochranu před škodlivým kódem.
	4	H16	Stanovil postupy pro sledování kybernetických bezpečnostních událostí.
			Přijal opatření pro ochranu přístupu k záznamům o kybernetických bezpečnostních událostech.
			Identifikoval kontaktní osoby pověřené výkonem systémové a technické podpory. Zajistil spojení na tyto osoby.
Řízení změn	3	H1, H14	Při provádění změn v rámci plnění přezkoumává mořné dopady změn.
			Určuje významné změny.
			U významných změn dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření ke snížení nepříznivých dopadů změny
			Provádí testování před provedením významné změny.
			V případě významné změny zajišťuje možnost navrácení do původního stavu.
Řízení přístupu	2	H7	Stanovil bezpečnostní opatření pro používání mobilních zařízení a jiných technických zařízení, které nejsou ve správě dodavatele.
	4	H10	Při ukončení smluvního vztahu odebírá přístupové oprávnění.
			Při ukončení změně smluvního vztahu změní přístupové oprávnění.
Akvizice, vývoj a údržba	2	H1, H14	Řídí rizika plnění dle VKB
			Řídí významné změny plnění dle VKB
			Stanovil bezpečnostní požadavky a zahrnul je do projektu vývoje.
			zajišťuje bezpečnost vývojového a testovacího prostředí a ochranu používaných testovacích dat.
			Provádí bezpečnostní testování významných změn před jejich zavedením do provozu, ev. předáním objednateli.
Zvládání kybernetických bezpečnostních událostí a incidentů	3	H1, H3, H14, H16	Zavedl proces detekce a vyhodnocování bezpečnostních událost a zvládání kybernetických bezpečnostních incidentů
Řízení kontinuity činností	3	H16	Vypracal, pravidelně aktualizuje a testuje plány kontinuity činností.

TECHNICKÁ OPATŘENÍ

Fyzická bezpečnost	4	H3	Předchází poškození, krádeži nebo zneužití aktiv využívaných pro poskytování plnění nebo přerušení poskytování plnění
	4	H6	Stanovil fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány nebo zpracovávány informace a umístěna technická aktivy využívaná pro poskytování plnění.
Bezpečnost komunikačních sítí	4	H12, H14	Vyčlenil komunikační síť využívanou pro poskytování plnění.
			Zajišťuje řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě
			Zajišťuje důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií pomocí kryptografie.
			Aktivně blokuje nežádoucí komunikaci
			Při segmentaci sítě a řízení komunikace mezi jejími segmenty využívá nástroj, který zajistí ochranu integrity komunikační sítě.
Správa a ověřování identit	4	H3, H11	Používá autentizační mechanismus založený na vícefaktorové autentizaci nejméně s 2 různými typy faktorů
			Používá autentizační mechanismus založený na autentizaci pomocí kryptografických klíčů zajišťující obdobnou úroveň jako vícefaktorová autentizace s 2 různými typy faktorů
			Identity uživatelů, administrátorů a aplikací, je ověřována pomocí nástroje, který používá k autentizaci identifikátor účtu a heslo, vynucuje 12 znaků u uživatelů a 17 znaků u administrátorů a vymáhá povinnou změnu hesla v intervalu maximálně po 18
			Implementace nástroje pro správu a ověření identity uživatelů, administrátorů a aplikací
Řízení přístupových oprávnění	4	H3	Používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění pro přístup k jednotlivým aktivům využívaným pro poskytování plnění povinné osobě.
	2	H10	Používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění pro pro čtení, zápis dat a změnu oprávnění.
Ochrana před škodlivým kódem	3	H3, H14	Implementoval nástroj zajišťující nepřetržitou automatickou ochranu před škodlivým kódem.
			Řídí oprávnění ke spouštění kódu
			Řídí automatické spouštění obsahu výměnných zařízení a datových nosiců
			Provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.
	2	H7	Monitoruje používání výměnných zařízení a datových nosičů.
Zaznamenávání událotí informačního a komunikačního systému	3	H3, H16	Zaznamenává bezpečnostní a potřebné provozní události aktiv důležitých pro poskytování plnění povinné osobě.
Detekce kybernetických bezpečnostních událostí, Sběr a vyhodnocování kybernetických	3	H3, H14	V komunikační síti užívané pro poskytování plnění povinné osobě používá nástroj pro detekci kybernetických bezpečnostních událostí.

bezpečnostních událostí			Nasadil nástroj pro ověření a kontrolu přenášených dat v rámci komunikační sítě nebo mezi komunikačními sítěmi využívanými pro poskytování plnění.
			Nasadil nástroj pro ověření a kontrolu přenášených dat na perimetru komunikační sítě využívané k poskytování plnění.
			Blokuje nežádoucí komunikaci.
Kryptografické prostředky	2	H3	Používá aktuálně odolné kryptografické algoritmy a kryptografické klíče pro ochranu aktiv užívaných k poskytování plnění.
Zajišťování úrovně dostupnosti informací	2	H1	Zajišťuje redundanci aktiv nezbytných pro poskytování plnění povinné osobě.

Příloha 4: Oskenované zadání práce

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2018/2019

Studijní program: Aplikovaná informatika
Forma: Kombinovaná
Obor/komb.: Aplikovaná informatika (ai3-k)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Mgr. Michalcová Lenka	Hálkova 120, Heřmanův Městec	I1600478

TÉMA ČESKY:

Návrh bezpečnostního hodnocení dodavatele

TÉMA ANGLICKY:

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je navrhnout metodiku hodnocení bezpečnosti u dodavatele založenou na tzv. principu bezpečnostní maturity zohledňující legistlativní požadavky plynoucí ze zákona o kybernetické bezpečnosti 181/2014 Sb., vyhlášky o kybernetické bezpečnosti 82/2018 Sb. a ve vztahu ke standardům~ISO 27001 a ISO 27002.

SEZNAM DOPORUČENÉ LITERATURY:

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ze dne 21. května 2018.
Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů, ze dne 23. července 2014.

Podpis studenta: Michalcová ..... Datum: 17.1.2019

Podpis vedoucího práce: ..... Datum: 17. 1. 2019

(c) IS/STAG , Portál - Podklad kvalifikační práce , I1600478 , 17.01.2019 11:19