

Vysoká škola ekonomická v Praze
Fakulta managementu

Diplomová práce

Bc. Lucie Minaříková
2018



Vysoká škola ekonomická v Praze

Fakulta managementu

Katedra exaktních metod

Analýza a hodnocení aktiv a rizik informačního systému

Autor diplomové práce: Bc. Lucie Minaříková

Vedoucí diplomové práce: Ing. Vladimír Příbyl, Ph.D.

Rok obhajoby: 2018

Čestné prohlášení

*Prohlašuji, že diplomovou práci na téma
„Analýza a hodnocení aktiv a rizik informačního systému“
jsem vypracovala samostatně a veškerou použitou literaturu a další prameny
jsem řádně označila a uvedla v přiloženém seznamu.*

V Jindřichově Hradci dne 27. dubna 2018

podpis

ZADÁNÍ DIPLOMOVÉ PRÁCE

Zpracovatelka: **Bc. Lucie Minaříková**
Studijní program: Ekonomika a management
Obor: Management
Název tématu: **Analýza a hodnocení aktiv a rizik informačního systému**

Zásady pro vypracování:

1. Práce bude zaměřena na metodologii analýzy a hodnocení rizik informačního systému podle požadavků ZKB a Vyhlášky k ZKB. Práce bude tedy kromě uvedení do problematiky kybernetické bezpečnosti a souvisejících témat obsahovat i volbu a popis vhodné metody pro identifikaci a hodnocení aktiv a rizik konkrétního informačního systému (IS). Práce bude samozřejmě obsahovat také zhodnocení výsledků provedené analýzy.

Rozsah práce: 60

Seznam odborné literatury:

1. ANDERSON, R., 2008. Security engineering. Indianapolis: Wiley Publishing. ISBN 978-0-470-06852-6.
2. ČERMÁK, Miroslav, 2009. Řízení informačních rizik v praxi. V Tribunu EU vyd. 1. Brno: Tribun EU. ISBN 978-80-7399-731-1.
3. MERNA, Tony a Faisal F. AL-THANI, 2007. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press. ISBN 978-80-251-1547-3.

Datum zadání diplomové práce: duben 2017

Termín odevzdání diplomové práce: duben 2018

Bc. Lucie Minaříková
Řešitelka

Ing. Vladimír Příbyl, Ph.D.
Vedoucí práce

Ing. Vladimír Příbyl, Ph.D.
Vedoucí ústavu

doc. Ing. Vladislav Bína, Ph.D.
Děkan FMJH VŠE

Název diplomové práce:

Analýza a hodnocení aktiv a rizik informačního systému

Abstrakt:

V diplomové práci se věnuji problematice řízení rizik v rámci bezpečnosti informací. Mým záměrem je objasnění procesu analýzy rizik, včetně popisu vybraných metodik. Na základě zvolené metodiky identifikuji a hodnotím rizika na vybrané organizaci. V návaznosti na získané výsledky navrhuji potřebná opatření na kvantifikovaná rizika. Tyto výstupy jsou podkladem pro vznik či aktualizaci vnitropodnikové dokumentace v oblasti systému řízení bezpečnosti informací. Analýza rizik je zpracována v souladu s požadavky Zákona o kybernetické bezpečnosti a jeho prováděcích předpisech.

Klíčová slova:

Kybernetická bezpečnost, analýza rizik, hrozba, opatření, aktiva, riziko, řízení rizik, zranitelnost, bezpečnost informací.

Poděkování:

Děkuji panu Ing. Vladimíru Příbylovi, Ph.D. za odborné vedení práce, pomoc a poskytování cenných rad při zpracování diplomové práce.

Obsah

Seznam použitých zkratk.....	17
Úvod	19
1 Systém řízení bezpečnosti informací	22
1.1 Vymezení pojmů.....	22
1.2 Bezpečnostní inženýrství	22
1.3 Standardy	26
1.4 Legislativa a právní rámec v České republice	27
1.4.1 Zákon o kybernetické bezpečnosti	28
1.5 GDPR	29
1.5.1 Legislativa GDPR a aplikace v ČR	29
1.5.2 GDPR v praxi	30
1.5.3 Princip odpovědnosti a k riziku	31
1.5.4 Kodexy a osvědčení.....	32
1.6 ISMS.....	32
1.6.1 Rozsah ISMS	33
1.6.2 Organizační bezpečnost	34
1.7 Proces řízení rizik	35
1.7.1 Řízení rizik.....	35
1.7.1 PDCA cyklus	37
1.7.1 Rozsah	39
1.7.2 Analýza rizik a metody	40
1.7.3 Základní předpoklady pro analýzu rizik	42
1.7.4 Vymezení vybraných metodik	43
2 Metodika.....	46
2.1 Výběr metodiky pro analýzu rizik informačního systému	46
2.2 Identifikace a dekompozice aktiv.....	47
2.2.1 Vlastníci aktiv	48
2.2.2 Identifikace aktiv	48

2.2.3 Dekompozice aktiv	49
2.3 Hodnocení aktiv.....	50
2.3.1 Postup při hodnocení.....	51
2.3.2 Celková hodnota aktiva	54
2.4 Identifikace hrozeb a zranitelností	55
2.5 Hodnocení hrozeb a zranitelností	56
2.5.1 Stanovení úrovně dopadu hrozeb - UDH.....	56
2.5.2 Pravděpodobnost hrozby - UPH	56
2.5.3 Úroveň zranitelnosti - UZH	57
2.6 Hodnocení rizik.....	58
3 Analýza rizik ve vybrané organizaci	61
3.1 Kontext organizace.....	61
3.1.1 Vize	62
3.1.2 Charakteristika informačního systému.....	62
3.2 Zahájení projektu	62
3.2.1 Inicie projektu.....	63
3.2.2 Identifikace zainteresovaných stran	64
3.3 Plánování projektu	64
3.4 Realizace projektu	66
3.4.1 Rozdílová analýza dokumentace	67
3.4.1 Výsledky identifikace a dekompozice aktiv	69
3.4.1 Identifikace a hodnocení rizik	73
3.5 Stanovení úrovně rizika	76
3.5.1 Porovnání úrovní rizik s kritérii pro přijatelnost rizik.....	76
3.5.1 Základní přístup k určení přijatelných rizik	76
3.5.2 Posouzení dopadu na aktiva.....	78
3.6 Ukončení projektu	79
3.6.1 Registr rizik.....	79
3.6.2 Přístupy pro zvládání rizik.....	79
3.6.3 Návrh způsobu zvládání rizik pro vybranou společnost	80

3.6.4 Návrh a realizace opatření	80
3.6.5 Plán zvládání rizik	80
3.6.6 Prohlášení o aplikovatelnosti	83
4 Závěr	85
Seznam literatury	87
Přílohy.....	90
Příloha č. 1 – Dotazník.....	91
Příloha č. 2 – Katalog rizik	92
Příloha č. 3 – Katalog opatření	95
Příloha č. 4 – Návrh zvládání rizik.....	99
Příloha č. 5 – Návrh opatření	101
Příloha č. 6 – Vypořádání navrhovaného opatření	103
Příloha č. 7 – Prohlášení o aplikovatelnosti.....	105

Seznam obrázků

Obrázek 1: Rámec bezpečnostního inženýrství.....	24
Obrázek 2: Bezpečnostní atributy.....	25
Obrázek 3: Proces řízení rizik.....	38
Obrázek 4: PDCA cyklus ISMS.....	39
Obrázek 5: Proces analýzy rizik.....	47
Obrázek 6: CAFM model IS Facility.....	63
Obrázek 7: Ukázka hodnocení rizik.....	73

Seznam tabulek

Tabulka 1: Vymezení pojmů	23
Tabulka 2: Příklad k definici uplatnění rizika	36
Tabulka 3: Fáze procesu řízení rizik	40
Tabulka 4: Faktory externí a interní analýzy rizik	41
Tabulka 5: Příklad dekompozice IS	49
Tabulka 6: Stupnice pro hodnocení důležitosti aktiva.....	51
Tabulka 7: Stupnice pro hodnocení důvěrnosti primárního aktiva - DU	52
Tabulka 8: Stupnice pro hodnocení integrity primárního aktiva - IN	53
Tabulka 9: Stupnice pro hodnocení dostupnosti primárního aktiva - DO	53
Tabulka 10: Stupnice normovaných hodnot DDI - Ux.....	54
Tabulka 11: Modelový výpočet pro důležitost.....	54
Tabulka 12: Modelový výpočet hodnocení DDI.....	55
Tabulka 13: Modelový výpočet, hodnota aktiva.....	55
Tabulka 14: Stupnice pro hodnocení pravděpodobnosti hrozby	57
Tabulka 15: Stupnice pro hodnocení úrovně zranitelnosti.....	58
Tabulka 16: Příklad výpočtu HR z pohledu bezpečnostních atributů	59
Tabulka 17: Normování hodnoty rizika (HR).....	60
Tabulka 18: Inicie projektu	65
Tabulka 19: Zainteresované strany	66

Tabulka 20: Zadávací listina projektu	67
Tabulka 21: WBS projektu.....	68
Tabulka 22: Organizační opatření.....	69
Tabulka 23: Technická opatření	70
Tabulka 24: Identifikace a dekompozice IS.....	71
Tabulka 25: Hodnocení aktiv	72
Tabulka 26: Hodnocení hrozeb	74
Tabulka 27: Hodnocení zranitelností a opatření.....	75
Tabulka 28: Normalizace hodnoty rizika úrovně rizika	76
Tabulka 29: Ukázka z Katalogu rizik	77
Tabulka 30: Hodnota rizika pro Přerušení konektivity do internetu	77
Tabulka 31: Hodnota rizika pro Selhání softwarového vybavení	77
Tabulka 32: Hodnota rizika pro Hacking.....	78
Tabulka 33: Hodnota rizika pro Porušení licenčního ujednání.....	79

Seznam použitých zkratek

IT	Informační technologie
HW	Hardware
SW	Software
ISO	International Organization for Standardization
ISMS	Information Security Management System
ČSN	Označení českých technických norem
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
PDCA	Plan-Do-Check-Act
GDPR	General Data Protection Regulation
ÚOUU	Úřad pro ochranu osobních údajů
WAF	Web Application Firewall
DLP	Data Loss Prevention
DRP	Disaster Recovery Plan
BCP	Business Continuity Plan
ISP	Internet Service Provider

Úvod

Žijeme v době, ve které si málokdo dokáže představit život bez internetu, počítače, mobilního telefonu či jiného elektronického pomocníka, zkrátka bez informačních technologií. Vzhledem k rychlému pokroku, jakým se informační technologie ženou vřed, je v naší společnosti téma kybernetická bezpečnost stále častěji diskutováno. V tendenci neustále se zvyšujících nároků na úspěšné podnikání, a při narůstající intenzitě sofistikovaných útoků, není již otázkou *zda*li, ale *kdy* se bude muset organizace s pokusy o narušení bezpečnosti své sítě potýkat a správně se chránit před kybernetickými hrozbami.

Informační kriminalita obecně patří v současnosti mezi nejrychleji rostoucí kriminality. Důvodů k zavádění nebo vylepšování systému řízení bezpečnosti informací může být hned několik. Prvním důvodem je legislativa. V České republice je v platnosti Zákon o kybernetické bezpečnosti č. 205/2017 Sb. (dále jen „ZKB“), který spolu s prováděcími předpisy stanovuje pro konkrétní orgány a subjekty povinnosti vyplývající ze systému řízení bezpečnosti informací. V kostce se jedná o skutečnost, kdy povinný subjekt musí zavést systém řízení bezpečnosti informací (více v teoretické části této práce), v rámci kterého pravidelně analyzovat rizika svého informačního systému. V prováděcích předpisech výše uvedeného ZKB jsou vymezeny kategorie, nebo jsou v případě např. významných informačních systémů (VIS) přímo v vyjmenovány.

Negativní kybernetické události ovlivní ale i ekonomiku organizace. Zastavení produkce způsobí ušlý zisk. Firma musí odškodnit újmy způsobené klientům. Organizace také může ztratit kredibilitu dojde-li ke zneužití dat jejich klientů. Nedůvěra klientů může spočívat i v podvrhu firemních stránek. Dalším důvodem pro řízení bezpečnosti informací je riziko vzniku průmyslové špionáže. Úspěšná organizace by si měla udržet know-how svých obchodních nabídek, strategických záměrů či vědeckých výzkumů. Jako poslední důvod uvádím kybernetickou kriminalitu, kdy se organizace stává obětí kriminálních činů, zcizení dat o klientech konkurencí nebo přímo zaměstnanci.

V této práci se zaměřuji na problematiku z pohledu firem a organizací. IT infrastruktura, s daty a informacemi jsou jedním z primárních zdrojů v podnikání, na kterém je firma bezprostředně závislá. S informačními daty pracují organizace denně, pomáhají na vstupu i na výstupu v procesu výroby produktů i služeb. Běžně se s nimi obchoduje a manipuluje. Tento primární zdroj v podnikání ale často kompromituje jejich neopatrné majitele. Proto je nezbytné celou svoji IT infrastrukturu chránit. Aby nedošlo k narušení bezpečnosti firemní sítě, musí

organizace vynaložit úsilí, náklady, na jejich dostatečné zabezpečení. Úspěšný kybernetický útok, nebo nedbalost či úmyslné jednání ze strany zaměstnanců značně znepříjemní organizaci existenci.

Dle nového Ustanovení EU o ochraně osobních údajů musí firmy a organizace výrazně zpřísnit ochranu osobních dat svých klientů a jiných třetích osob. Pro spoustu firem mohou být postihy za nedodržování pravidel přímo likvidační. V práci se tomuto novému Ustanovení věnuji v teoretické části. V aplikační části vycházím z povinností ZKB a po provedené analýze navrhuji potřebná opatření k implementaci vhodného zabezpečení osobních dat klientů a jiných osob.

V rámci neustále se zvyšujícímu konkurenčnímu boji, rychle rostoucím změnám, náročnějších požadavků od zákazníků, je pro organizaci téměř nezbytné zavést komplexní strategii pro řízení rizik. Nepodaří-li se včas identifikovat všechna klíčová rizika, určit jejich pravděpodobnost a možné dopady na organizaci, může to být pro ni nežádoucí až kritické. Pokud má vlastník subjektu zájem na zachování kontinuity, musí znát rizika a hrozby a způsob jak jim čelit.

„Jestliže nemůžete řídit riziko, nemůžete ho kontrolovat. Pokud ho nemůžete kontrolovat, nemůžete ho řídit. To znamená, že hrajete hazardní hru a doufáte, že budete mít štěstí (Hooten,2000 in Merna, 2007)“.

Povinnost řídit rizika v informační bezpečnosti je nařízena subjektům, které jsou definovány v ZKB a jeho prováděcích předpisech. Jedná se zejména o státní instituce. Ostatním subjektům, kterým tato povinnost není povinována, se však doporučuje vycházet z požadavků tohoto zákona jeho prováděcích předpisů. Soukromé subjekty většinou zavádějí opatření na úrovni mezinárodních norem. Tyto bezpečnostní standardy popisují vhodné přístupy a doporučení pro dosažení vytyčených cílů v této oblasti.

Motivací ke zpracování tohoto tématu je jeho aktuálnost v praxi. Díky mé mnohaleté praxi mám k oblasti IT blízko. Proto těchto svých načerpaných znalostí a zkušeností využiji ku prospěchu této práce.

Struktura práce

V první části práce provedu rešerši literatury. Pojednává o bezpečnostním inženýrství, vymezuje se na systém řízení bezpečnosti informací. Zmiňuji normy a legislativu, které jsou v této oblasti využívány, jak pro Českou republiku, tak i na mezinárodní úrovni. Řízení rizik je v současnosti předpokladem k úspěšnému řízení a plnění podnikových cílů. Celý proces analýzy rizik mnoho autorů vymezuje různým způsobem. Velmi však záleží na tom, co je objektem analýzy. Dle použité literatury a

vlastních zkušeností definuji proces analýzy rizik. Pojmy z oblasti informační technologie vysvětluji pomocí Výkladového slovníku od autorů Jirásek a spol. (2013).

V této části také vymezím podstatu nového Obecného nařízení EU o ochraně osobních údajů, protože souvisí s hlavním cílem práce. K tématu uvedu postřehy, doporučení a reakce z podnikatelského prostředí, které zastřešují různé asociace.

V druhé části představím metodiku práce obsahující jednotlivé kroky při procesu analýzy rizik. Metodika je v souladu s požadavky ZKB a obsahuje popis řady matematických transformací. Předpokladem její úspěšné implementace je využití nástroje – MS Excel, který umožní získaná data poloautomaticky zpracovat.

Pro snadnější pochopení realizuji v třetí části práce případovou studii, která vychází z reálného prostředí. Na základě provedené analýzy rizik vybrané organizace budou navržena opatření na základě vyhodnocených rizik. Pro neakceptovatelná rizika vypracuji návrh na způsob zvládnutí rizik a navrhnu opatření k realizaci. Výsledky provedené analýzy závěrem zhodnotím.

Hlavním cílem práce je upozornit na význam ochrany informačních systémů a důležitost systému řízení bezpečnosti informací. Teoretickou i praktickou částí vzniká báze pro přípravu další vnitropodnikové dokumentace, která by měla být součástí nového procesu založeném na neustálém zlepšování systému řízení bezpečnosti informací.

Přínosem práce uvažuji přiblížit čtenáři problematiku aktuálního tématu kybernetické bezpečnosti. Popíši metody často používané pro analýzu rizik, zvolím vhodnou metodiku pro praktickou část práce. Praktickou část povedu jako projekt, neboť se tak analýza rizik v praxi provádí standardně.

1 Systém řízení bezpečnosti informací

V této kapitole jsem provedla literární rešerši k hlavnímu tématu práce. Věnuji se systému řízení informací, legislativě v ČR a mezinárodním normám vymezených pro tuto oblast. Vysvětluji proces řízení rizik a popisuji příslušné metodiky k řízení rizik.

1.1 Vymezení pojmů

Pro lepší orientaci v této problematice vymezuji hned v úvodu základní pojmy informační bezpečnosti. Tyto pojmy vysvětluje jak Čermák (2009, s. 131–134), jeden z mých primárních zdrojů, tak i prováděcí předpis příslušného zákona (2009, s. 131–134), viz Tabulka 1: Vymezení pojmů.

Zákon o kybernetické bezpečnosti. Zákon č. 205/2017 Sb., dále jen „ZKB“ (MVČR, 2018b).

Prováděcí předpis ZKB použitá v této práci je Vyhláška č. 316/2014 (dále jen „VKB“) (MVČR, 2018a). Existuje ještě Vyhláška č. 317/2014, kterou však dále necituji.

1.2 Bezpečnostní inženýrství

S tímto pojmem se můžeme setkat v mnoha různých souvislostech napříč mnoha oblastmi. Z pohledu prevence a zajištění bezpečnosti IS v organizaci se jedná o disciplínu zaměřenou na nástroje, procesy, metody potřebné pro návrh, implementaci nebo testování již dokončených informačních systémů. Důležitým úkolem tohoto oboru je také přizpůsobit systémy požadavkům prostředí, které se neustále vyvíjí (Anderson, 2008).

Tato disciplína vyžaduje odborné znalosti, od kryptografie a počítačové bezpečnosti, jako odolnosti proti manipulaci hardwaru, znalosti metod ekonomie, aplikované psychologie, organizace a práva.

Existuje mnoho bezpečnostních systémů s kritickými požadavky na zajištění, jejich selhání může ohrozit lidský život a životní prostředí (například jaderná bezpečnost, různé kontrolní systémy), poškodit ekonomickou oblast (bankovní systémy, daňové systémy), ohrozit osobní soukromí (lékařský záznam, elektronický recept), usnadnit zločin (alarmy proti krádeži). Podle Andersona (Anderson, 2008) může dokonce naše vnímání systému o jeho zranitelnosti než ve skutečnosti je, negativně zhoršit hospodářský vývoj (např. lidé budou méně platit kreditní kartou prostřednictvím internetu).

Tabulka 1: Vymezení pojmů

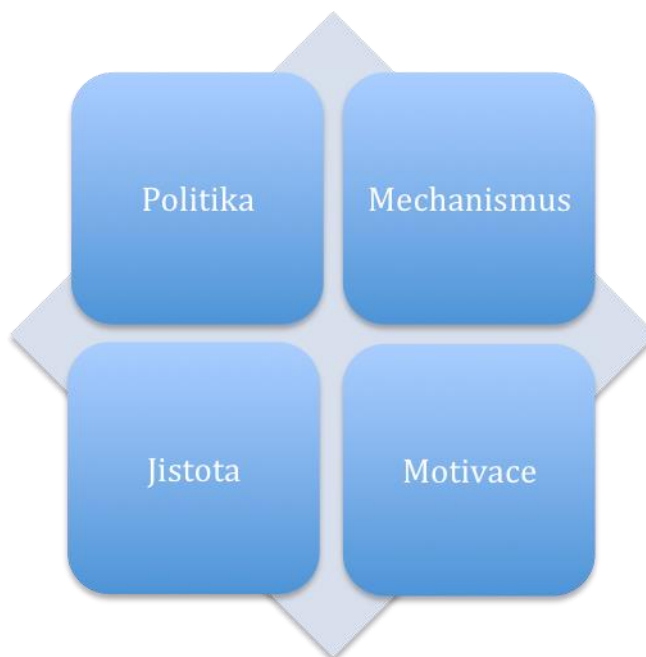
Pojem	Popis
Aktivum (Asset)	jsou data, hardware, systémový software (dále jen „systémový SW“), aplikační SW (dále jen „aplikace“), technická infrastruktura, komunikační systémy, služby na bázi IS, znalosti obslužného personálu, dokumentace apod.
Bezpečnostní opatření	Prostředek, postup a procedura implementovaná v prostředí pro minimalizaci rizik.
Dopad hrozby	Nepříznivá změna ovlivňující úroveň dosažených cílů organizace.
Dostupnost aktiva	Úroveň, do které jsou aktiva k dispozici v případě potřeby jejich užití.
Důvěrnost aktiva	Zajištění, že jakékoli nakládání s aktivy je umožněno pouze oprávněným subjektům.
Hrozba	Potencionální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být poškození aktiva.
Informační bezpečnost	Ochrana důvěrnosti, integrity a dostupnosti informací.
Informační činnost	Získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na hmotné nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na hmotných nosičích.
Integrita aktiva	Neporušenost, zajištění toho, aby nebylo možné s aktivy nepozorovaně manipulovat.
Podpůrná aktiva	Technické aktivum. Zaměstnanci, dokumentace, dodavatelé a lokality podílející se na provozu, rozvoji, správě nebo bezpečnosti IS.
Podstoupení rizik	Přijetí břemene ztráty nebo prospěchu ze zisku vyplývajícího z určitého rizika. V kontextu řízení rizik bezpečnosti informací jsou v rámci podstoupení rizik uvažovány pouze negativní dopady.
Pravděpodobnost hrozby	Hodnota, která určuje, jak často se hrozba může vyskytnout.
Riziko	Možnost, že určitá hrozba využije zranitelnosti IS a způsobí poškození aktiva.
Řízení rizik	Činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládnutí rizik, sdílení informací o riziku a sledování a přezkoumání rizik.

Pojem	Popis
Systém řízení bezpečnosti informací	Část systému řízení orgánu a osoby uvedené založené na přístupu k rizikům informačního systému, které stanoví způsob ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací. V textu budu používat zkratku „ISMS“.
Vyhnutí se riziku	Rozhodnutí nedopustit zapojení se do rizikových situací, nebo je vyloučit.
Zranitelnost	Slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

Zdroj: Vlastní zpracování dle (MVČR, 2018a) .

Požadavky na zabezpečení systémů se velmi liší jeden od druhého svými nároky na odolnosti vůči chybám, zachování důvěrnosti, autenticity, integrity. Neúspěšná ochrana bezpečnosti IS může spočívat v tom, že jsou chráněné špatné věci, nebo naopak správné věci jsou chráněné špatným způsobem (Anderson, 2008).

Obrázek 1: Rámec bezpečnostního inženýrství



Zdroj: Vlastní zpracování dle (Anderson, 2008).

Zmíněný autor tvrdí, že dobré bezpečnostní inženýrství vyžaduje soulad mezi 4 faktory, viz Obrázek 1:

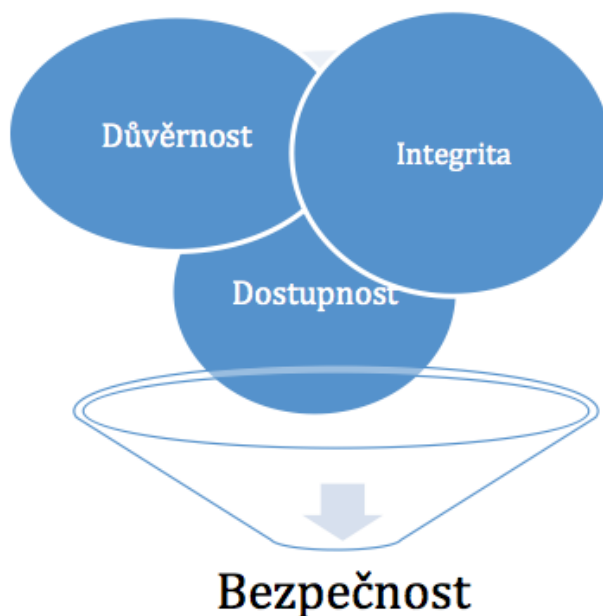
- Politika. Čeho bychom měli dosáhnout;

- Mechanismus. Existence šifer, kontroly přístupu, hardwarové odolnosti proti manipulaci apod.;
- Jistota. Spolehnout se na každý konkrétní mechanismus;
- Motivace. Motiv pro dohled a údržbu systému, motiv útočníků vedoucí k poražení zásad IS.

Co je bezpečnost informací? Pokud chceme něco chránit před zneužitím, ztrátou, poškozením či zničením, lze tuto naši snahu charakterizovat jako zajištění bezpečnosti. Bezpečnost informací vymezuje Čermák (2009) tak, že se jedná o proces zajišťování ochrany informací na cílené úrovni z hlediska 3 vlastností. V této souvislosti hovoříme o zachování 3 aspektů, důvěrnosti, integrity a dostupnosti (dále budu používat také výraz „DDI“).

Dostupnost výše zmíněný autor definuje jako vlastnost informace, která opravňuje osobu s ní pracovat v daném okamžiku. Vlastnost, která umožňuje seznamovat s informací pouze oprávněné osoby je stejným autorem nazývána důvěrností. Třetí vlastnost, integrita, zabezpečuje neporušenost informace během její manipulace, a tak můžeme informaci důvěřovat.

Obrázek 2: Bezpečnostní atributy



Zdroj: Vlastní zpracování dle (Čermák, 2009).

Obrázek 2 definuje, že musí být učiněna taková opatření, aby nedošlo k nežádoucímu odhalení¹, modifikaci² nebo zničení³ vedoucí k finanční ztrátě, poškození dobrého jména firmy a v nejhorším případě i ohrožení života osob. Proto je nutné informace před narušením bezpečnostních indikátorů chránit po celou dobu jejich životnosti. V praxi se však často stává, že proti sobě stojí dva protichůdné požadavky a nelze implementovat všechna příslušná opatření, která vyplývají z této teorie.

1.3 Standardy

Pro řízení bezpečnosti informací existují právní předpisy, standardy, normy a doporučení, které lze chápat jako soubor zkušeností a dobrých praxí přijatých širokou odbornou veřejností. Normy v tomto oboru jsou zaměřeny na systémy řízení bezpečnosti informací a jsou často označovány jako ISMS, anglicky Information Safety Management System (dále „ISMS“). Jedná se o systematický přístup k řízení citlivých informací o společnosti tak, aby zůstal bezpečný. Zahrnuje lidi, procesy a systémy IT aplikací procesu řízení rizik. Pro úspěšné řízení bezpečnosti informací musí být v celém procesu všechny normy dodržovány (ISO.org, 2017).

Mezinárodní normy ISO, anglicky International Organization for Standardization (dále jen „ISO“) jsou plně respektovány širokou veřejností. Pro použití jakéhokoli standardu se používají normy jakosti ISO 9000, které poskytují základ.

Záměrem většiny společností je řídit bezpečnost informací a koordinovat implementaci bezpečnostních opatření dle stanovené působnosti a odpovědnosti vedoucích zaměstnanců a zlepšit řízení a koordinaci bezpečnosti informací dle normy ČSN ISO/IEC 2700x⁴.

Informačním technologiím, bezpečnostním technikám, systémům řízení bezpečnosti informací, Přehledu a slovníku je vymezena série norem ISO/IEC 27000:2016, vydána v únoru 2016. V České republice byla její česká verze ČSN ISO/IEC 2700x vydána 1.5.2017. Do rodiny těchto norem patří (NORMY.cz, 2010):

- ISO/IEC 27000 – Přehled a slovník;

.....

¹ anglicky Disclosure

² anglicky Alteration

³ anglicky Destruction

⁴ ČSN je česká technická norma a tomto kontextu mezinárodní norma ISO přeložená do češtiny.

- ISO/IEC 27001 – Požadavky. Nejznámějším a nejpoužívanějším standardem celé skupiny je ISO/IEC 27001, který poskytuje požadavky na ISMS. Norma byla vytvořena pro soukromý sektor a vychází ze zahraničních standardů;
- ISO/IEC 27002 - Soubor postupů pro opatření bezpečnosti informací pro cloudové služby;
- ISO/IEC 27003 - Směrnice pro implementaci systému řízení bezpečnosti informací;
- ISO/IEC 27004 - Řízení bezpečnosti informací – Měření;
- ISO/IEC 27005 - Řízení rizik bezpečnosti informací;
- ISO/IEC 27006 - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

Skupina standardů ISO/IEC 2700x pomáhá organizacím udržet jejich aktivům informační bezpečnost. Použitím této rodiny standardů je zajištění subjektům řídit bezpečnost jejich aktiv, jako jsou finanční informace, duševní vlastnictví, informace svěřené třetími stranami, detaily o svých zaměstnancích. Význam této normy se opírá nejen o autoritu organizace ISO, ale také o použití této normy mezinárodní organizací certifikovaných auditorů IRCA⁵ pro certifikaci firemních systémů bezpečnosti informací ISMS (ISO.org, 2017).

1.4 Legislativa a právní rámec v České republice

V České republice je ústředním orgánem státní správy vykonávající správu v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti Národní bezpečnostní úřad (dále jen „NBÚ“). Tento úřad byl donedávna též garantem kybernetické bezpečnosti v ČR a podílel se na vzniku návrhu ZKB, v jehož struktuře je ukotveno nové Národní centrum pro kybernetickou bezpečnost (GOVCERT.cz, 2018).

V roce 2017 došlo ke změně garanta kybernetické bezpečnosti, od 1. 8. 2017 se ústředním správním orgánem stal Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“). Podle webového portálu zřízeného vládou má NÚKIB v kompetenci dohled kybernetické bezpečnosti „....včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany (GOVCERT.cz, 2018)“. Mezi hlavní oblasti činnosti patří provoz vládní CERT⁶, tedy

.....

⁵ zkratkou názvu International Register of Certificated Auditors

⁶ Skupina pro reakci na počítačové hrozby

skupiny, která vznikla roku 1988 po aféře s jedním z prvních počítačových červů⁷. Úřad NÚKIB má za úkol spolupracovat s ostatními národními i mezinárodními CERT týmy a CSIRT týmy.

Je potřeba také vysvětlit další pojem CSIRT⁸. Co má za úkol CSIRT? Jde o bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích provozovaných v ČR. Bezpečnostní tým v ČR provozuje sdružení CZ.NIC, správcem české národní domény, a to na základě memoranda uzavřeného v roce 2012 s NBÚ.

Úřad NÚKIB má dále v kompetenci připravovat bezpečnostní standardy pro IS definovaných právními předpisy. Provádět osvětu a podporovat vzdělávání v oblasti kybernetické bezpečnosti, chránit utajované informace ve své oblasti informačních komunikačních systémů, a provádět další aktivity v oblasti výzkum a vývoj (GOVCERT.cz, 2018).

1.4.1 Zákon o kybernetické bezpečnosti

ZKB je v České republice účinný od 1. ledna 2015, publikace ve Sbírce zákonů pod č. 181/2014 Sb. (AION CS, 2018).

1. srpna 2017 byl tento zákon změněn tzv. malou novelou. Novým zákonem je Zákon č. 205/2017 Sb. Obsahem změny je „...úprava definice provozovatele informačních a komunikačních systému, zavádí se nový povinný subjekt, mění se pokuty či lhůty pro splnění povinností (CZ.NIC, 2017)“.

Hlavním cílem ZKB je ochrana kritické infrastruktury (zkratkou KII) a informačních systémů, které jsou podstatné pro chod státu. Jde především o tvorbu právního rámce pro provoz národní a vládní skupiny CERT. Pojem kritická infrastruktura je v současné době velmi často zmiňován. Kritickou infrastrukturu je potřeba chránit a dobře zabezpečit, aby nedošlo k jejímu selhání, které by mělo za následek výpadek její funkce s fatálními dopady na životy, zdraví, majetek a životní prostředí. Narušení kritické infrastruktury způsobí ekonomické ztráty fyzickým nebo právnickým osobám, případně státu.

.....

⁷ Morrisův červ, který ke svému šíření využíval internet

⁸ Computer security incident response team je skupinou pro reakce na počítačové bezpečnostní incidenty (Jirásek et al., 2013).

Zákon definuje okruh dotčených osob, především jde o státní orgány, které poskytují veřejnou službu. Konkrétně definováno v prováděcím předpise Vyhláška č. 317/2014. Například jednotlivé resorty, Ředitelství silnic a dálnic, energetické společnosti, dopravní podniky, atd. (AION CS, 2018).

Zákon obsahuje další prováděcí předpisy, kterými se přesně definují jednotlivé požadavky vycházející z rodiny norem ISO 2700x. Požadavky se dají obecně definovat do kategorií na řízení, kontrolu a monitoring osob nebo aktiv (MVČR, 2018a).

Odpůrci tohoto zákona jsou však toho názoru, že bude úřad na základě získané velké moci odposlouchávat nebo přímo odpojovat nepohodlné osoby či organizace. Tyto obavy nebyly zatím podloženy, laická společnost neměla přístup k pracovním verzím tohoto zákona (SYSTEMONLINE.cz, 2015).

Národní centrum pro kybernetickou bezpečnost (dále jen „NCKB“) uvádí, na jakých principech je zákon založen. Je postaven na dvou zásadách a třech pilířích. „Zásady jsou:

- *minimalizace zásahu do práv soukromoprávních subjektů;*
- *individuální odpovědnost za bezpečnost vlastních informačních systémů.*

Tři pilíře:

- *bezpečnostní opatření (standardizace);*
- *hlášení kybernetických bezpečnostních incidentů a;*
- *protiopatření, tzn. reakce na incidenty (GOVCERT.cz, 2018).“*

ZKB definuje pojmy a systémy zajištění kybernetické bezpečnosti, bezpečnostních opatření v oblasti zabezpečení informačních a komunikačních systémů a tým, které systémy je mají plnit.

1.5 GDPR

Subjekty, kteří manipulují s osobními údaji budou pod větším drobnohledem. Požadavky na transparentnost a ochranu soukromí se musí držet svými pravidly. Novinka, kterou musí subjekty dodržet již od května 2018, bude zároveň velice sankcionována.

1.5.1 Legislativa GDPR a aplikace v ČR

Legislativní úprava ochrany osobních údajů v České republice platí v současné době od roku 2000 v podobě zákona č. 101/2000 Sb. o ochraně osobních údajů. Na základě tohoto zákona je zřízen Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) se sídlem v Praze. Dodržování tzv. Obecného nařízení na ochranu osobních údajů,

anglický název General Data Protection Regulation (dále jen „GDPR“) nabude platnosti 25. Května 2018 a od tohoto data bude závazné pro všechny země Evropské unie. Jedná se o Nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016, zřízené s cílem sjednotit pravidla ochrany osobních údajů, jeho univerzální použitelnost ve všech státech Evropské unie (GDPR.cz, 2018).

V rámci GDPR se jedná se o ucelení pravidel o ochraně osobních údajů občanů Evropské unie, které se dá nazvat revolucí a jejich nedodržování bude sankcionováno enormními pokutami. V právním prostředí České republiky GDPR nahradí současnou právní úpravu zákona č. 101/2000, resp. zákon bude po jeho novele upravovat jen některé aspekty nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou Obecným nařízením upraveny (UOOU.cz, 2018).

Nutnost zřízení GDPR je odůvodňována globalizací, rychlým technologickým vývojem, hospodářskou a sociální integrací (Martíšková et al., 2017).

1.5.2 GDPR v praxi

Jak se promítne nové nařízení do praxe? Zvýší se nároky na IT infrastrukturu v oblasti bezpečnostního monitoringu, vznikne povinnost dokumentovat incidenty a oznamovat příslušným orgánům narušení bezpečnosti osobních údajů, a o bude nutno o všem vést záznamy o prováděném zpracování. Pro snadnější orientaci byla Asociací malých a středních ČR, zkratka AMSP ČR a Českou asociací ochrany osobních údajů, zkratka ČAOUÚ zřízen webový portál s názvem podniků a živnostníků „GDPR bez obav“ s cílem informovat zejména malé a střední podniky (GDPR bez obav, 2018).

Nařízení platí pro subjekty napříč segmenty, odvětvími, instituce i jednotlivce, zasáhne všechny ty, kteří manipulují s osobními údaji. Dle ÚOOU „*Obecným nařízením se bude především, pokud jde o povinnosti, řídit subjekt, který provádí zpracování osobních údajů. Takový subjekt je nazýván správcem osobních údajů. Obecným nařízením se řídí i zpracovatel, což je subjekt, který pro správce osobní údaje zpracovává. Pokud jde o práva vyplývající z Obecného nařízení, ta vyplývají fyzické osobě, což je subjekt údajů. Dále se Obecným nařízením budou řídit i dozorové úřady, tj. i ÚOUU, který bude uplatňovat svěřené pravomoci za účelem plnění stanovených úkolů*“ (UOOU.cz, 2018).

V rámci GDPR je nově zavedená funkce, která bude pomocníkem a koordinátorem ochrany osobních údajů příslušného správce nebo zpracovatele. DPO neboli Data Protection Officer bude plnit funkci kontaktního bodu pro komunikaci s dozorovými úřady (v ČR s ÚOUU).

AMPS ČR organizuje cyklus bezplatných seminářů, ve kterých představuje legislativní rámec Nařízení a jeho dopady. Asociace také provádí různé průzkumy, například z října 2017 tvrdí, že GDPR zasáhne dvě třetiny podnikatelů. Ne všichni jsou však na GDPR připraveni. Přípravu v podobě školení zaměstnanců nebo analýza interních směrnic neprovedly všichni, ale pouze dvě třetiny z dotázaných (AMSP.CZ, 2017).

V článku od Martíškové a spol. (2017) je provedena slušná analýza reakcí podnikatelských subjektů na Obecné nařízení. Autoři shromáždili své podklady z webových stránek zřízených k diskuzi na toto téma. Výsledky ukazují na nedostatečnou informovanost subjektů, obavy z přílišné byrokracie, vyskytla se i kritika z některých pasáží, které nejsou příliš jasné. Obavy plynou také z nedůvěry k celému projektu, který v praxi stejně nic nedokáže.

1.5.3 Princip odpovědnosti a k riziku

Obecné nařízení je založeno na nových přístupech, principu odpovědnosti správce a přístupu odpovědnosti založený na riziku. „*Princip odpovědnosti znamená dodržení zásad:*

- *Vůči subjektu musí být při zpracování dodrženy zásady zákonnosti, korektnosti a transparentnosti;*
- *Shromažďovány pouze pro určité výslovně vyjádřené účely, v minimálním rozsahu;*
- *Obsahem přesné, aktualizované. Nepřesné musí být smazány či opraveny;*
- *Uloženy ve vhodné formě;*
- *Zpracovány tak, aby byla zachována jejich důvěrnost a integrita (ÚOÚ, 2018).“*

Princip založený na riziku lze definovat v širším a užším slova smyslu. V širším smyslu správce musí brát v potaz pravděpodobná rizika pro práva a svobody fyzických osob a přizpůsobit tak zabezpečení osobních údajů vůči povaze, rozsahu, kontextu a účelu pracovní (ÚOÚ, 2018).

V užším slova smyslu se jedná o některé povinnosti při zpracování či porušení bezpečnosti v případech, které představují riziko či vysoké riziko pro práva a svobody fyzické osoby. „*Jedná se zejména o nové povinnosti (ÚOÚ, 2018):*

- *Povinnost vést záznamy o činnostech zpracování osobních údajů;*
- *Posouzení vlivu na ochranu osobních údajů;*
- *Předchozí konzultace. Správce bude dále povinen konzultovat s ÚOÚ tyto bezpečnostní incidenty;*
- *Ohlašování případu porušení zabezpečení osobních údajů ÚOÚ;*
- *Oznamování případu porušení zabezpečení osobních údajů subjektu údajů;*
- *Ustanovení pověřence pro ochranu osobních údajů.“*

1.5.4 Kodexy a osvědčení

Ke splnění stanovené odpovědnosti správce za soulad zpracování se zásadami zpracování a schopnost tento soulad prokázat, mají správci, jak výslovně zmiňuje Obecné nařízení, napomáhat mimo jiné i kodexy, osvědčení (pečetě, známky) a záznamy o činnostech zpracování (Averia, 2018).

- Kodexy mají správcům sloužit jako vodítko správné praxe při zpracování osobních údajů právě s ohledem na specifčnost daného sektoru (např. bankovníctví, telekomunikace, internetové obchody, zdravotnictví).
- Osvědčení má sloužit k prokázání souladu zpracování s Obecným nařízením (UOOU.cz, 2018).

Záznamy o činnostech zpracování obsahují informace o prováděném zpracování, což správci umožní lehčí orientaci ohledně zpracování, která provádí.

Dokládání souladu zpracování však nelze omezit pouze na shora uvedené možnosti, ale dokládání souladu je komplexní činnost, zahrnující dílčí činnosti, mezi které lze zařadit nejen shora uvedené kodexy, osvědčení a záznamy o činnostech zpracování, ale například i zveřejňování informací, které Obecné nařízení ukládá správci zveřejňovat, vyhotovením vnitřních předpisů až po řádnou spolupráci s příslušným dozorovým úřadem.

1.6 ISMS

Jednou ze slabších oblastí firem je obvykle systém řízení bezpečnosti informací. Tato oblast bývá velmi často vedoucími pracovníky podceňována, a není řešena systematicky. Firmy většinou omezují implementaci ISMS na řešení pro ochranu dat – DLP⁹, a to v oblastech řízení práce s daty, pro reporting bezpečnostních incidentů, nebo klasifikaci dat atp. (TechTarget, 2018). Většinou jsou za ni odpovědni spíše vedoucí pracovníci IT, což může vést k případným potížím. Případné kybernetické útoky v sobě kombinují oblasti nejen IT, ale i sociální inženýrství, personální i objektové bezpečnosti. Zavedení procesu řízení informačních rizik v organizaci by mělo být z výše uvedených důvodů nezbytným krokem. Organizace by měla mít definovaný rozsah ISMS, jehož účelem je definovat cíle, principy a potřeby řízení

.....

⁹ Data Loss Preventio, jedná se o strategii pro zajištění ochrany citlivých a kritických informací mimo firemní síť. Termínem je také někdy nazýván software, který pomáhá administrátorům sítě kontrolovat jaká data mohou koncoví uživatelé volně užívat.

bezpečnosti informací, stanovit rozsah systému řízení a definovat pravidla a postupy nutné pro naplnění těchto cílů a principů. V rámci ISMS je nutno vytvořit tým kybernetické bezpečnosti, v jehož středu vše koordinuje role manažera kybernetické bezpečnosti (Anderson, 2008).

1.6.1 Rozsah ISMS

Jsou identifikovány 2 základní způsoby stanovení rozsahu:

1. ISMS je shodný s rozsahem organizace.
2. Rozsah ISMS je aplikován pouze na omezenou část organizace, tzn. zónování – například na jednu pobočku, bezpečnostní proces, nebo na ucelenou skupinu informačních systémů (ISO.org, 2017).

Pro implementaci opatření v souladu se ZKB, je použití metody 2 výhodnější, je rychlejší. Následně ji lze rozšířit na celou organizaci z důvodu efektivity jednotného přístupu k bezpečnosti (jednotného ISMS v rámci organizace).

Hlavní zásady ke stanovení rozsahu ISMS (MVČR, 2018a):

1. Vně vymezeného rozsahu ISMS nesmí zůstat žádná aktiva, jejichž narušení by mohlo způsobit narušení kteréhokoli požadovaného parametru aktiv, jež jsou předmětem ochrany dle ZKB.
2. Musí být naplněn smysl a účel ZKB, tj. zajistit kybernetickou bezpečnost pro dané systémy tak, že narušení jakéhokoli systému, jehož je organizace správcem či provozovatelem, stojícího vně bezpečnostního perimetru, nemůže způsobit narušení bezpečnosti informací chráněného systému stojícího uvnitř perimetru.
3. Každý systém, jehož je organizace provozovatelem a jehož narušení může přímo způsobit narušení bezpečnosti informací chráněného systému, musí být zahrnut v rozsahu ISMS.

Do bezpečnostního perimetru musí být zahrnuty všechny útvary, jejichž pracovníci mohou, z hlediska svých oprávnění vůči systémům zahrnutým v bezpečnostním perimetru, svým chováním ovlivnit bezpečnost informací v chráněných systémech a to i nepřímo prostřednictvím jejich vlivu na bezpečnost informací v podpůrných systémech (MVČR, 2018a).

K vymezení rozsahu lze s výhodou využít následující dokumentace IS a dokumentace infrastruktury, na níž je IS provozován:

- Určení systému;
- Funkčnost systému (určení produktů – primárních aktiv);
- Architektura IS (blokové schéma IS, topologie IS);
- Návaznost na související IS;
- IP adresní plán IS;

- Procesní schéma IS;
- Popis uživatelských rolí IS.

Podle autorů (Novák a Požár, 2011) je nutné určit rozsah ISMS víceřadově. V prvním kroku můžeme s výhodou využít výstupy Rozdílové analýzy ověřující hodnocení míry souladu aktuálního stavu s požadavky ZKB a příslušných vyhlášek a to jak v dokumentační části, tak i v reálném provádění opatření. Rozdílová analýza¹⁰ obsahuje kroky:

1. Identifikace současného stavu;
2. Identifikace bezpečnostních opatření (organizační a technická) organizace;
3. Identifikace shody opatření s povinnostmi ze ZKB;
4. Identifikace shody s tzv. *best practice*, podle Slovníku od autorů (Jirásek et al., 2013) se jedná o vyzkoušené a osvědčené praxe a postupy v oblasti pro bezpečnost informací.

Výstupem rozdílové analýzy je identifikace chybějících částí metodické základny, řídicích aktů a organizačních a technických opatření.

1.6.2 Organizační bezpečnost

V rámci ISMS je doporučeno mít zřízen Výbor pro řízení bezpečnosti informací, bezpečnostní role a jejich práva a povinnosti. Dle příslušného zákona (MVČR, 2018a) jsou v rámci tohoto Výboru určeny tyto bezpečnostní role:

- „*Manažer kybernetické bezpečnosti, osoba odpovědná za systém řízení bezpečnosti řízení informací, která je pro tuto činnost vyškolená a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let.*
- *Architekt kybernetické bezpečnosti, osoba zajišťující návrh a implementaci bezpečnostních opatření, která je pro tuto činnost vyškolená a prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let.*
- *Auditor kybernetické bezpečnosti, osoba provádějící audit kybernetické bezpečnosti, která je pro tuto činnost vyškolená a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let. Auditor KB vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu ostatních bezpečnostních rolí.“*

.....

¹⁰ Někdy také nazývána GAP analýza.

1.7 Proces řízení rizik

Nezbytnost řízení rizik vyplývá z potřeby kvalitního řízení procesu. Zavedení politiky řízení rizik vychází z jasného postoje managementu organizace k riziku. Podle autorů (Novák a Požár, 2011) jde o systematickou identifikaci, hodnocení, zvládání, monitorování a vykazování všech významných rizik jednotným způsobem tak, aby byly pokryty všechny rizikové oblasti činnosti organizace. Řízení rizik je ale nezbytné pro orgány jež jsou definovány legislativou.

Riziko je v kontextu této práce chápáno jako nebezpečí vzniku určité škody, poškození, ztráty či zničení. Chceme-li definovat význam tohoto slova v oblasti informačních technologií, lze jej popsat takto. Jedná se o hrozbu, která využila specifickou zranitelnost systému a překonala stávající opatření. Pakliže vůbec nějaké bylo. Jak ukazuje Obrázek 2, hrozba poruší zmíněné bezpečnostní atributy a způsobí škodu.

1.7.1 Řízení rizik

Pro účely pochopení řízení rizik považuji za výstižnou definici od citovaného autora: „Vlastník používá a zhodnocuje aktiva, a protože si je vědom jejich hodnoty, zavádí vhodná opatření vedoucí ke snížení zranitelností, kterých se snaží využít hrozba, vyvolaná agentem hrozby, za účelem zneužití a znehodnocení aktiv (Čermák, 2009, s. 13)“.

Pro zavedení systému řízení rizik je nezbytné postupně zvládnout řadu dílčích složek (Novák a Požár, 2011):

1. Strategie řízení rizik. Organizace si stanoví strategii, konzervativní nebo odvážnější, jejímž cílem je snaha eliminovat rizika, redukovat potenciální dopady, případně je co nejvíce omezit. Do politiky řízení rizik je vhodné stanovit hlavní zásady řízení rizik, například principy včasného varování spočívající ve včasném vydání výstražného signálu, princip transparentní komunikace o rizicích všem zainteresovaným stranám, atd.
2. Procesy řízení rizik. Postupné zavedení efektivních procesů řízení rizik. Jedná se o tyto jednotlivé procesy: identifikaci rizik; zpracování analýzy rizik (kvalitativní, kvantitativní či vlastní metody); vyhodnocení rizik z čehož vznikne katalog rizik; taktika řízení rizik; opatření pro zabezpečení rizik; monitorování, vykazování a reportování; včasné varování; časový plán hlavních aktivit řízení rizik. Měřítka pro vyhodnocení aktiv, hrozeb, zranitelností a výsledných rizik.
3. Organizace řízení rizik. Organizační struktura, role složek struktury, řídicí orgán, vedení, vlastník rizika, pravomoci a odpovědnosti, interní audit.

4. Personální zabezpečení. Systém vzdělávání v oblasti rizik obsahující úvodní školení, pravidelná a specializovaná školení.
5. Dokumentace a informační tok. Systém řízení rizik (dále více v kapitole o ISMS), katalog a mapa rizik, zprávy o riziku, apod.
6. Komunikace o rizicích. Pravidla pro základní, vnitřní, vnější komunikaci o rizicích, systému řízení apod.
7. IT podpora řízení rizik.. Například MS Office, databázové systémy – MS Access, moduly integrovaných systémů a datové sklady – SAP moduly, atd.

Tabulka 2: Příklad k definici uplatnění rizika

Pojem	Příklad
Vlastník	Majitel firmy, manažer
Aktivum	Počítač, operační systém, software, data
Opatření	Firewall, antivir, antispyware, patche
Hrozba	Škodlivý software
Agent hrozby	hacker

Zdroj: Vlastní zpracování dle (Čermák, 2009).

Pokud se řekne riziko, každému se intuitivně vybaví ohrožení. Opakem tohoto pojmu je příležitost. Pro profesionální řízení rizik je nutno rizika řídit. Tedy přesněji řečeno řídit to, co organizaci ohrožuje, ale i příležitosti vylepšující situaci. Existuje mnoho názorů a přístupů jak rizika řídit. Co to vlastně řízení rizik je? Autoři (Merna Tony a Al-Thani Faisal F., 2007) ve své knize uvádějí, že jde o soubor činností realizovaných organizací s cílem snížit nebo změnit riziko vznikající při podnikání.

Proces řízení rizik podle jiného autora (Smith, 2008) je spíše kontinuální smyčkou, založenou na cyklu zahrnující identifikaci, analýzu, řízení a hlášení rizik. V literatuře tohoto autora o projektovém řízení vychází celý proces řízení rizik z norem.

Díky stále se zvyšujícím nárokům na úspěšné podnikání, se analýza rizik stává rostoucím prvkem hlavních projektů. Stále více společností přistupuje ke svému podnikání prostřednictvím projektů, programů a portfolií. Neexistuje však žádná norma, na kterou by se mohly odkazovat postupy, faktory a přístupy. Pro překonání tohoto úskalí objevilo mnoho organizací a výzkumných pracovníků způsob jak proces rizika popsat. Např. Společnost pro projektové řízení, o. s. (zkratkou SPŘ), která zastřešuje profesní organizace projektových manažerů. Tato organizace informuje své členy a i celou odbornou veřejnost o aktuálním stavu znalostí a praxe v odborných oblastech, které se týkají řízení projektů, a tím i řízením rizik. Existuje více pozitivních efektů. Například slouží k lepší orientaci v této oblasti, čtenář ušetří

čas hledáním jiných informací. Společnost se opírá o existující standardy a normy a definuje kompetenci řízení rizik a příležitostí (Merna Tony a Al-Thani Faisal F., 2007).

Sbírka doporučené praxe pro řízení rizik, která vznikla ve spolupráci mezinárodní asociace pro projektové řízení a SPŘ o. s. tvrdí, že je smyslem procesu řízení rizik umět rizika a včas rizika identifikovat (IPMA.cz, 2013). Rozpoznat, zda je dané riziko důležité, zda se s ním zabývat. Není možné věnovat se všemu. Tento zdroj uvádí také doporučení shodně s normou ISO 3100x:

- Stanovení kontextu (establishing the context);
- Identifikaci rizik (risk identification);
- Analýzu rizik (risk analysis);
- Hodnocení rizik (risk evaluation)
- Ošetření rizik (risk treatment);
- Monitorování a přezkoumávání (monitoring and review);
- Komunikaci a konzultace (communication and consultation).

Obrázek 3 uvádí strukturu procesu řízení dle interpretace normy pojednávající o řízení rizik (ISO.org, 2009).

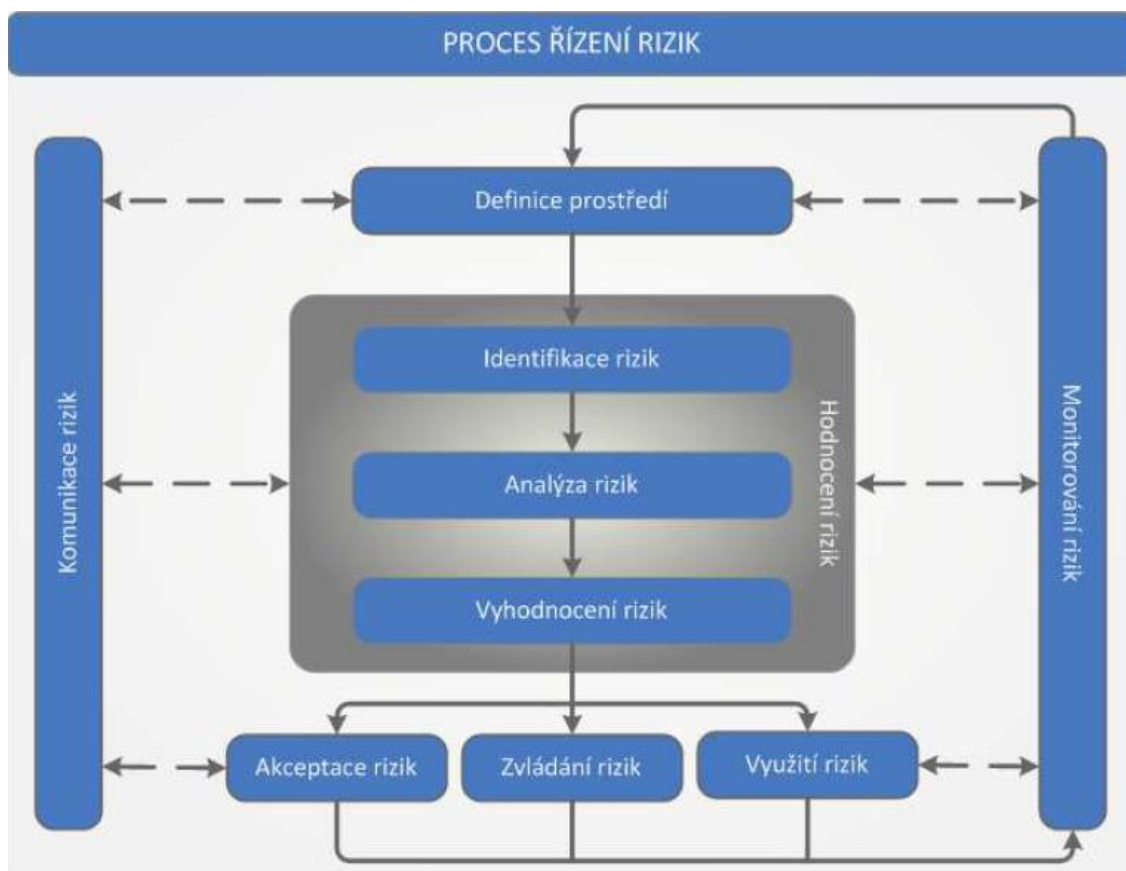
1.7.1 PDCA cyklus

Pokud organizace implementuje ISMS dle ISO 2700x, budou jí požadavky ZKB do značné míry vyhovovat.

Norma zavádí model Plánuj-Dělej-Kontroluj-Jednej, anglicky Plan-Do-Check-Act (dále jen „PDCA“) jako součást přístupu k vývoji, implementaci, zdokonalování efektivnosti ISMS. Obrázek 4 znázorňuje PDCA cyklus, který je znám též jako Demingův, dle jeho tvůrce. W. E. Deming tuto metodu představil jako proces spojený s neustálým zlepšováním procesů (Deming.org, 2018). Pokud je celý systém ISMS korektně implementován a poté i certifikován, je možné vycházet z doporučení a postupů navržených skupinou norem ISO 2700x.

Plánuj. Jde vlastně o ustanovení rozsahu ISMS. Obsahuje vytvoření bezpečnostní politiky, plánů, cílů, procesů a procedur, které souvisí s řízením rizik a zlepšováním bezpečnosti informací. Výsledky musí být v souladu s celkovou politikou a cíli organizace. Konkrétně se jedná určení rozsahu ISMS, nastavení systematického přístupu k řízení rizik, identifikace rizik, analýza a jejich vyhodnocení. Definice zvládání rizik a výběr cílů a opatření. Patří sem i získání souhlasu vedení se zbytkovými riziky, a příprava prohlášení o aplikovatelnosti (Brenner, 2007)

Obrázek 3: Proces řízení rizik



Zdroj: Vlastní zpracování dle (ISO.org, 2018a).

Dělej. V této fázi jde o implementaci systému řízení bezpečnosti informací a jeho provoz. Formulace plánu zvládání rizik a jeho implementace, Určení postupů pro měření účinnosti zavedených opatření. Implementace bezpečnostních opatření, školení a vzdělávacích programů, řízení zdrojů a provozu ISMS. Zavedení procedur pro zjištění a reakci na bezpečnostní incidenty (Brenner, 2007).

Kontroluj. Ověření úrovně, tam, kde je to možné, provádění procesu vůči bezpečnostní politice, cílům a praktické zkušenosti a oznámení výsledků řízení k posouzení (Brenner, 2007).

Jednej. Pro dosažení nepřetržitého zlepšování procesu ISMS využíváme výsledků analýzy řízení. Implementujeme nápravná opatření, provádíme preventivní činnosti. preventivní a nápravná opatření. Využití nápravných a preventivních činností, založených na výsledcích analýzy řízení tak, aby bylo dosaženo nepřetržitého zlepšování ISMS (Brenner, 2007).

Obrázek 4: PDCA cyklus ISMS



Zdroj: Vlastní zpracování dle (Brenner, 2007)

1.7.1 Rozsah

Pro úspěšné zvládnutí procesu doporučuje Čermák (2009) nejprve organizaci poznat, provést analýzu jejího vnitřního a vnějšího prostředí. Dle tohoto autora je třeba získat aktivní podporu vrcholového managementu a nakonec vytvořit firemní Politiku pro řízení rizik.

Analýza vnitřního a vnějšího prostředí se provádí pro zjištění hrozeb a příležitostí. Organizace má veliký vliv na vnitřní prostředí, neb si jej sama přímo vytváří. Naopak na vnější prostředí má vliv nepatrný. Definované hrozby a příležitosti nám pomohou zvolit vhodnou strategii k dosažení cílů a naplnit poslání organizace. Je potřeba si také uvědomit, že se prostředí subjektu uvnitř i vně neustále vyvíjí, stejně jako se vyvíjejí informační systémy a technologie. Proces řízení rizik musí na tyto změny reagovat. Analýzu rizik by měla organizace provádět pravidelně s ohledem na změny, které situace vyžaduje.

Získání aktivní podpory managementu. Vzhledem k nárokům na zapojení celé organizace a vedoucích pracovníků se jedná o jeden z náročnějších projektů v IT bezpečnosti. Právě kvůli nízké angažovanosti osob mimo IT oddělení tyto projekty v historii selhávaly. Pokud je zde však podpora shora a proaktivní přístup, může takové úsilí zachránit celý projekt a vzhledem ke značně sníženému riziku úniku dat i samotnou společnost. O provedení analýzy rizik by měl rozhodovat vlastník. Bez aktivní podpory vrcholového managementu se stává proces řízení rizik obtížným. Nemusí souhlasit všichni vedoucí pracovníci, nicméně úkolem manažera pro řízení rizik je získat maximální podporu a finanční prostředky od managementu společnosti a přesvědčit je o nutnosti zavedení procesu řízení rizik (Čermák, 2009).

Tabulka 3: Fáze procesu řízení rizik

Fáze	Jednotlivé kroky
Úvodní fáze	Analýza vnitřního a vnějšího prostředí. Získání aktivní podpory managementu. Zavedení politiky pro řízení rizik.
Analýza rizik	Rozhodnutí o způsobu provedení. Volba strategie analýzy. Volba metodiky pro analýzu.
Zahájení analýzy rizik	Identifikace a hodnocení aktiv. Identifikace a hodnocení hrozeb. Identifikace a hodnocení zranitelností.
Vyhodnocení rizik	Hodnocení rizik na základě dopadu hrozby, zranitelnosti a pravděpodobnosti. Vyhodnocení opatření, výběr vhodných opatření.
Zvládání rizik	Sepsání závěrečnou zprávu; Prezentace výsledků.
Monitorování a přezkoumání	Porovnání stávajícího stavu s plánovaným.

Zdroj: Vlastní zpracování dle (Čermák, 2009).

Zavedení politiky pro řízení rizik. Stanovení cílů řízení rizik v závislostech na strategických cílech organizace (přežití organizace, udržení její prosperity, zvýšení tržní hodnoty). Určení rizikové kapacity organizace jako největší velikosti ztráty, kterou je organizace schopna přežít. A na závěr stanovit přijatelnou (akceptovatelnou) míru rizika.

1.7.2 Analýza rizik a metody

V této fázi rozhodujeme o způsobu, strategii a metodice provedení.

Rozhodnutí o způsobu provedení. Pokládáme si otázku kdo bude analýzu provádět, interní zaměstnanci nebo externí dodavatel? Obě varianty mají své výhody a nevýhody. Pro jednu společnost může být výhodou faktor, který pro druhou může být nevýhodou, a naopak, viz Tabulka 4.

Volba strategie. Způsoby, jakými lze analýzu rizik provést je několik (Merna Tony a Al-Thani Faisal F., 2007).

- Základní, ve které organizace přijímá protipatření bez provedení podrobnější analýzy. Tento přístup je sice rychlý, ale neměla by jej využívat organizace, která je závislá na IT.

- Neformální způsob je založen na subjektivitě a znalostech jednotlivců, kteří nepoužívají žádnou definovanou metodu.
- Podrobná analýza, jak je patrné z jejího názvu, nejpřesnější. Je však náročná na čas a finančních nákladech.
- Kombinovaným přístupem je spojení základní a podrobné analýzy. V praxi bývá nejvíce používána.

Tabulka 4: Faktory externí a interní analýzy rizik

Faktory	Interní analýza rizik	Externí analýza rizik
1.	Znalost prostředí a procesů	Zkušenosti z jiných
2.	Zachování důvěrnosti	Porušení důvěrnosti
3.	Koupit nebo vyvinout metodiku	Není nutné kupovat nebo vyvíjet metodiku
4.	Koupit nebo vyvinout nástroj	Není nutné kupovat nebo vyvíjet nástroj
5.	Mít nebo vyškolit vlastní odborníky	Není nutné mít vlastní odborníky
6.	Všichni rozumí výstupům projektu	Výstup projektu není srozumitelný
7.	Neschopnost vést interview	Schopnost vést interview
8.	Nižší míra objektivit	Vyšší míra objektivit
9.	Nižší cena	Vyšší cena
10.	Více zatěžuje společnost	Méně zatěžuje společnost

Zdroj: Vlastní zpracování dle (Čermák, 2009).

Metodika pro analýzu a vyhodnocení rizik. Jakou firmu zvolí metodu pro analýzu rizik? Pro existenci velkého množství jednotlivých prvků a složitých vazeb mezi nimi je problematika krizového managementu značně rozsáhlá. Neexistuje však univerzální metoda. Proto je nutné nalézt optimální metodu, ve většině případů kombinovat různé metody nebo jejich části.

Metodika by měla být transparentní pro všechny zúčastněné strany. Mýlně se společnosti domnívají, že je předmětem know-how je samotná metodika. Skutečnou podstatou know-how je způsob získání co nejvíce relevantních informací, a po jejich zpracování vhodně interpretovat výsledky.

Pro vyhodnocení rizik existují hlavní dva typy metod, je to kvalitativní a kvantitativní analýza rizika (Merna Tony a Al-Thani Faisal F., 2007).

Kvantitativní analýza nevyužívá pro popis rizik slova, ale číselné hodnoty. Při kvantitativním vyjádření je riziko vyjádřeno na základě matematického výpočtu z frekvence/pravděpodobnosti výskytu a jeho dopadu. Použitím těchto metod je náročné na čas, provedení a prostředky. Pro přesnost je rozhodující dostupnost,

kvalita dat a výběr použitých modelů. Často zahrnuje použití softwarových modelů za použití statistiky (Merna Tony a Al-Thani Faisal F., 2007).

Kvalitativní analýza používá slov k popisu rozsahu možných následků a pravděpodobností. Jako subjektivní odhad skupiny respondentů, specialistů a expertů se používají strukturovaná interview a dotazníky. Vyjádření rizika charakterizujeme v určitém rozsahu. K určení výše dopadu hrozeb a zranitelnosti, a výsledného rizika používají tzv. Diskrétní škály (např. 1 až 10, nebo slovní popis nízká až velmi vysoká). Výhodou je rychlost a snadnější proveditelnost (Merna Tony a Al-Thani Faisal F., 2007).

1.7.3 Základní předpoklady pro analýzu rizik

Pro efektivní realizaci analýzy nutno ovládat minimálně některé SW nástroje:

- Pro řízení projektu – PROJECT nebo Gantt;
- Pro tvorbu dokumentace – WORD PROCESSOR, např. Word, Writer;
- Analýzu dat – SPREADSHEET, např. MS EXCEL;
- Prezentaci výsledků – POWERPOINT;
- Zpracování dat – postačí i ACCESS;
- Business modelování;
- E-mailovou komunikaci – POŠTOVNÍ KLIENT;
- Správa dokumentů pro verzovací systém, např. CVS.

Dalším předpokladem je příprava plánu analýzy rizik. Čermák (2009) jej doporučuje v tomto rozsahu:

- Stanovení hranic a hloubky analýzy rizik;
- Stanovení délky trvání;
- Stanovení nákladů;
- Sestavení analytického týmu.

Identifikace respondentů. Informace se získávají od odpovědných pracovníků nebo expertů. Je třeba věnovat této oblasti dostatečnou pozornost, a stanovit od jakých respondentů a jakým způsobem od nich budeme informace získávat.

Získávání informací. Informace lze získávat metodami některými metodami, např. uspořádat workshop, brainstorming, interview s vybranými respondenty, anonymní dotazníky, d'áblův advokát, atd. Každá metoda má své specifikum, volíme podle charakteru skupiny, množství respondentů a účastníků. Volba metody má velký dopad na efekt, kterého chceme při získávání informací dosáhnout. Chceme-li například objektivní a nikým neovlivněný názor respondenta, sejdeme se s ním sami na neutrálním prostředí. Jsme-li limitováni časem a prostředky, potřebujeme získat

informace od většího počtu respondentů zvolíme raději dotazník, a podobně. Podle Čermáka (2009) musíme informace vhodně:

- analyzovat. Zkontrolovat jejich formální stránku. Rozuměli respondenti všem otázkám? Nenapsali úmyslně chybné hodnoty? Případné velké rozdíly je třeba znovu ověřit.
- interpretovat. Použít vhodný SW nástroj. Výstup musí být srozumitelný a poskytovat relevantní podklad pro rozhodnutí.
- verifikovat. Kdokoli se může zeptat na získané informace. Je třeba si získané informace nechat dotyčným respondentem potvrdit.

V rámci další dokumentace by neměly chybět následující body:

- Šíření informací o riziku;
- Realizace jednotlivých opatření;
- Kontrola realizace;
- Zpráva o zvládání rizik.

1.7.4 Vymezení vybraných metodik

Seznam metod a standardů zabývajících se riziky v oblasti IT je mnoho. Zvolila jsem ke srovnání čtyři metody, i přesto že můj zdroj vytvořil soupis celkem 17 metod. Metody definovala ad hoc pracovní skupina ve složení odborníků z osmi členských států EU). Metody byly posouzeny odborníky v roce 2005, v případě novějších verzí nemusí být některé vlastnosti metod odpovídat aktuální verzi. Zvážené metody vyhovují pro technické i politické aspekty analýzy rizik (Enisa, 2018).

CRAMM. V praxi se často pro analýzu rizik využívá metodika CCTA Risk Analysis and Management Method. Součástí metodiky je celý postup od analýzy rizik až k návrhu opatření včetně výstupů pro dokumentace (Enisa, 2018).

Pro tuto metodu existuje stejnojmenný software sloužící k analýze rizik. Identifikace rizika, analýza rizik i hodnocení je možno provést přímo v softwarové nástroji. Dodavatel software je ze Spojeného království. Insight Consulting. Samotná metoda CRAMM je poměrně obtížně použitelná bez sw nástroje CRAMM. Jelikož tato metoda vznikla a je používána pro analýzy rizik ve vládě Spojeného království, je vhodná pro velké organizace jako jsou státní orgány.

Výhodou je jednoznačně využití softwarového nástroje. Pomocí kterého lze zavést a podporovat ISMS. Metodu lze používat pro rychlé (CRAMM Express)i detailní analýzy (CRAMM Expert) až po kontrolu souladu s bezpečnostními standardy (BS7799). Rozhodne-li se tedy organizace pro zavedení ISMS a certifikaci, lze použít typ BS7799 (ISO 27001). Software obsahuje knihovnu protiopatření a pokrývá svými doporučeními všechny oblasti bezpečnosti. Software vypočte míry rizika a následně

automaticky vybere protipatření, která jsou pro danou oblast nejvýhodnější. Obsahuje šablony pro tvorbu dokumentací.

Nevýhodou je uživatelsky méně přívětivé prostředí softwarového nástroje. Výstup v podobně generovaných reportů nelze dále modifikovat, prvky jsou pevně stanoveny a neměnné.

Rozhodne-li se organizace využívat tuto metodiku, musí předem počítat s většími finančními výdaji. Cena software se pohybuje ke statisícům Kč. Organizace musí také proškolit analytika, což jsou další nemalé náklady v desítkách tisíc korun (Enisa, 2018).

ISO/IEC 27001. Tato norma je považována také za jednu z metod. Je určena pro proces certifikace. Umožňuje porovnání systému řízení bezpečnosti informací prostřednictvím řady ovládacích prvků. Mylně se však organizace domnívají, že norma zahrnuje analýzu rizik nebo certifikaci řízení rizik. Tento standard byl přijat společností ISO s některými modifikacemi. Certifikát udělený podle této normy potvrzuje soulad organizace s definovanými požadavky s řízením bezpečnosti informací a sadou bezpečnostních kontrol (Enisa, 2018).

MEHARI¹¹. Metoda byla vyvinuta francouzskou asociací CLUSIF, která sjednocuje odborníky z IT. Metoda poskytuje kompletní model řízení rizik vyhovující požadavkům ISO 27005, popisuje modulární komponenty a procesy. V jednotlivých fázích klasifikujeme aktiva, pravděpodobnost hrozeb, opatření a zranitelnosti prostřednictvím auditu. Dále analyzuje obecný seznam rizikových situací a poskytuje úroveň závažnosti pro každý rizikový scénář. Analýza je založena na vzorcích a parametrech a umožňuje optimální výběr nápravných opatření. Poskytuje hodnocení v souladu s kontrolami dle norem ISO 27001-2005 a s procesem ISMS. Hlavním cílem této metodiky je poskytnutí potřebné podpory pro informační bezpečnost (Enisa, 2018).

Poskytuje podporu při tvorbě strategie bezpečnosti a bezpečnostních plánů, pomáhá implementovat bezpečnostní politiky. Metodika pomáhá při procesu hodnocení rizik a zvládání rizik. Lze dle ní provádět bezpečnostní osvětu, průběžně hodnotit efektivnost přijatých bezpečnostních opatření. Všechny tyto podporované činnosti mohou být realizované najednou, nebo na sebe mohou navazovat v rámci

.....

¹¹ Jedná se o zkratku pro MEthod for Harmonized Analysis of Risk

jednotlivých projektech. Metodika pomáhá začlenit bezpečnost do řízení a do provádění projektů.

Výhodou této metody je zejména skutečnost, že se dá aplikovat opakovaně na stejný IS. Díky tomu se analýza rizik provádí kontinuálně s cílem aktuálního stavu informační bezpečnosti. Nevýhodou je absence kvalitního softwarového nástroje, který by usnadnil používání. Pomocí Mehari lze využít rychlého nebo detailnějšího hodnocení bezpečnosti. V praxi však dochází většinou právě ke kombinaci obou přístupů, kdy se na celý IS aplikuje rychlé hodnocení a na kritické procesy, činnosti a aktiva je použito detailní hodnocení (Enisa, 2018).

OCTAVE-S¹². Metodika založená na komplexnosti při zkoumání IS je sestavená ze 3 fází. V první fázi jsou stanovena kritéria pro posuzování dopadů hrozeb, identifikována aktiva a zhodnoceny bezpečnostní postupy organizace. Pro kritická aktiva jsou určeny bezpečnostní požadavky a jsou vytvořeny profily hrozeb. Druhá fáze je zaměřená na zranitelnost infrastruktury a zjišťují se přístupové cesty, analyzují se procesy spojené s technologiemi. Ve třetí fázi vzniká bezpečnostní strategie a plány, které obsahují osm procesů. Zádním předpokladem je sestavení kvalitního analytického týmu z cca 3-5 odborníků na technologickou a bezpečnostní oblast a zaměstnanců, kteří jsou obeznámeni z cíli, strategií, organizační strukturou organizace. Tento definovaný tým pracuje ve všech fázích celého procesu analýzy rizik (Enisa, 2018).

Výhodou jsou principy hodnocení rizik, protože se Octave-S snaží do hodnocení rizik začlenit velké množství organizace. Nevýhodou je absence softwarového nástroje, v praxi se používá tabulkový procesor MS Excel, který neumožňuje efektivní prezentaci výsledků.

.....

¹² anglicky Operationally Critical Threat, Asset and Vulnerability Evaluation

2 Metodika

V této kapitole zvolím metodiku, dle které provedu v třetí části analýzu rizik informačního systému. Postup je založen na povinnostech plynoucích ze ZKB a jeho prováděcích předpisů. Při volbě vhodného postupu jsem zvážila výhody a nevýhody definovaných metodik. Metodiky nabízí moduly pro detailní, nebo rychlé provedení analýzy.

2.1 Výběr metodiky pro analýzu rizik informačního systému

Vzhledem k vymezenému cíli této práce provést analýzu rizik dle požadavků ZKB nelze použít ani jednu konkrétní definovanou metodiku.

CRAMM používají spíše specializované firmy, které analýzu rizik používají jako službu. Největší výhodou metodiky CRAMM je knihovna protipatření, která se automaticky přiřadí vypočítaným rizikům. Metodika je objektivní a komplexní. Nevýhodou jsou nepřehledné výstupy. Software stejného názvu nemám dostupný k instalaci, a nemohu tak CRAMM použít.

MEHARI tvoří spíše rámec pro hodnocení rizik, není z tohoto důvodu plnohodnotná pro účely této práce. Další nevýhodou je absence kvalitního softwarového nástroje.

Použila jsem metodiku vytvořenou na míru, ve které je stanoven vlastní postup. V podstatě se velmi svými fázemi podobá principu založeném na metodice OCTAVE-S. Výhodou je, že je postavena na míru a lze jí pro daný informační systém opakovat.

Dotazník pro identifikaci aktiv jsem pro tento projekt sestavila vlastními silami. Formát výstupů analýzy vychází z šablon, které jsou uvedeny v prováděcím předpisu ZKB.

Projektové řízení je pro úspěšné provedení analýzy rizik nezbytné, proto přistupuji v této práci k analýze rizik jako k projektu. Praktická část bude zpracována dle Příručky praktických zkušeností od Schwalbe (2011).

Jako nástroj pro zpracování je použit tabulkový procesor MS Excel. Tento nástroj je výtvorem třetí osoby, která si jej nepřeje zveřejňovat. Nejedná se o licencovaný SW, jde prakticky o know-how jak provést pomocí tabulkového procesoru analýzu rizik. Cílem této práce není popsat nástroj pro zpracování analýzy rizik.

Proces analýzy rizik znázorňuje Obrázek 1: Rámec bezpečnostního inženýrství.

Obrázek 5: Proces analýzy rizik

Zdroj: Vlastní zpracování

2.2 Identifikace a dekompozice aktiv

Abychom splnili Požadavky VKB, je třeba vyjádřit vazbu mezi primárním a podpůrným aktivem. V případě, že musíme požadavky splnit, identifikujeme primární a podpůrná aktiva. V další fázi zkoumáme vztah závislosti bezpečnostních atributů primárních aktiv na podpůrných aktivech. V této práci provádím analýzu informačního systému, kterému zákon neudává vyjádřit vazbu mezi primárním a podpůrným aktivem. Identifikaci a hodnocení aktiv provedu podle doporučení v praktické knize od Čermáka (2009).

ZKB vyžaduje od některých určených subjektů hodnocení a vyjádření závislosti primárních aktiv na podpůrných. Proto tyto skupiny aktiv charakterizují. Na primární aktiva lze pohlížet jako na produkty, tj. výsledky hlavní činnosti organizace. V souladu s VKB je produktem Služba nebo také informace – pokud jsou informace produktem hlavní činnosti. Jinak jsou jako data uložena, zpracovávána, přenášena podpůrnými aktivy, nebo jsou podpůrným aktivem samotným. Mezi primárním a podpůrným aktivem je určitý vztah. Bezpečnostní atributy CIA primárního aktiva jsou závislé na poškození některého z podpůrných aktiv. Hrozby způsobují škody primárních aktiv skrze podpůrná aktiva (MVČR, 2018a).

V zákoně ani prováděcích předpisech není uvedeno, které aktivum má být primární a které podpůrné. Proto je doporučeno hledat v normě ISO/IEC 27005, příloha B, ve které se píše:

- „- *primární aktiva jsou informace, obchodní procesy a činnosti, které když jsou narušeny, tak organizace nemůže plnit své poslání;*
- - *podpůrná aktiva jsou HW, SW, síť, pracovníci, lokalita, organizace, na kterých jsou primární aktiva závislá (ISO.org, 2018b).“*

2.2.1 Vlastníci aktiv

Účelem role vlastníka/garanta aktiva je zajištění a udržení potřebné úrovně bezpečnosti daného konkrétního aktiva v průběhu celého životního cyklu. Aby konkrétní osoby mohli naplnit uvedený účel role vlastníka aktiva, jsou rolí vlastníka pověřovány osoby, které disponují odpovídající odbornou a výkonnou kompetencí.

Vlastníci aktiv jsou podstatnými účastníky procesů identifikace a hodnocení aktiv a rizik dle této metodiky Jsou odpovědní za poskytování všech potřebných informací o aktivech relevantních pro zpracování dokumentace – výstupů dle požadavků VKB.

Vlastníci jsou v uvedených procesech partnery bezpečnostní specialistů, kteří na základě informací poskytnutých vlastníky aktiv požadované výstupy zpracovávají v souladu s VKB. Při sběru primárních dat a informací vystupují garanti jako respondenti, osoby dotazované, poskytující data k dalšímu zpracování. Vlastníci aktiv následně verifikují výsledné výstupy a využívají je při naplňování výše uvedeného účelu své role v praxi.

Pro potřeby společnosti FACILITY s.r.o. byl okruh respondentů stanoven takto:

- manažer (vedoucí) organizační jednotky;
- jím pověření pracovníci.

2.2.2 Identifikace aktiv

Při identifikaci aktiv bereme v potaz kontext organizace. Vše, co má pro organizaci nějakou hodnotu lze nazvat aktivem.

Pro identifikaci aktiv jsem zvolila metodu „Interview“, která spočívá v dotazování definovaného okruhu pracovníků (dále respondentů) s cílem získat odpovědi na otázky předkládané v Dotazníku, viz Příloha č. 1 této práce. Podstatou úspěchu je využití interních pracovníků k provedení identifikace aktiv, protože právě oni nejlépe znají organizaci.

Na zpracování byla stanovena doba 14 dní. Po zpracování odešle vyplněný dotazník na projektového manažera. Sběr odpovědí k otázkám a zpracování

odpovědi (identifikace aktiv) provedl projektový manažer a evidoval získané odpovědi.

Respondenti nejdříve identifikují aktiva a přidělí jim úroveň Důležitosti (Otázka č. 1 a č. 2). Toto hodnocení je mnohdy subjektivní a je potřeba spolehnout se na osobní zkušenosti respondentů.

Otázka č. 1

- Jaká aktiva IS FACILITY považujete za důležitá pro Vaši práci?
- Jaká další aktiva IS FACILITY považujete za důležitá pro Vaši práci?

Otázka č. 2

- Jaká aktiva IS FACILITY považujete za důležitá pro práci organizace?
- Jaká další aktiva IS FACILITY považujete za důležitá pro práci organizace?

Za správnost vyplnění Dotazníku odpovídá vlastník/garant aktiva.

2.2.3 Dekompozice aktiv

Jakmile jsou zdokumentovaná aktiva, provedu jejich dekompozici a vhodně je seskupím. Důvodem je zejména pro pozdější hodnocení hrozeb, které působí na jednotlivá aktiva a jaké jsou jejich zranitelnosti vůči hrozbě. Čas ke zpracování analýzy je závislý na množství zpracovávaných aktiv. Seskupení aktiv provedu dle jejich účelu, či jejich společných vlastností.

Detailnější dekompozice IS by mohla vypadat tak, jak uvádí Tabulka 5.

Tabulka 5: Příklad dekompozice IS

Skupiny aktiv	aktiva
Prostory	Pozemky Budovy Místnosti
Software	Operační systémy Aplikace Databáze
Hardware	Servery Klienti

Zdroj: Vlastní zpracování dle (Čermák, 2009).

WBS¹³ projektu:

- Vytvořit dotazník k identifikaci aktiv
- Uspořádat workshop k identifikaci a dekompozici aktiv
- Identifikovat všechna aktiva
- Provést dekompozici aktiv
- Zdokumentovat všechna aktiva

2.3 Hodnocení aktiv

Pro ohodnocení aktiv se v rámci analýzy rizik standardně využívá kvalitativní metoda vzhledem k její menší náročnosti proti kvantitativní metodě. Nevýhodou je nesrovnatelné porovnání dopadů a horší kontrola nákladů ve fázi zvládnání rizik při výběru vhodných opatření. S ohledem na účel dokumentu a cíle organizace, a také z důvodu, že VKB používá k ohodnocení úrovně dopadů hrozeb kvantitativní ukazatele, volím pro IS kombinovanou metodu. Při prvním použití této metodiky použiji kvalitativní metodu pro základní identifikaci a ohodnocení rizik. Tato metoda se dá také použít pro určení úrovně (váhy) závislosti primárních aktiv na podpůrných. V této práci však tuto sílu vazby neuvažuji, budu hodnotit pouze aktiva bez rozdělení na primární a podpůrná.

Při dalším použití metody v rámci PDCA cyklu, za předpokladu existence podkladů pro kvantitativní hodnocení aktiv, lze provést s garanty aktiv odhad počtů dotčených osob a základní odhad materiálních dopadů narušení jednotlivých bezpečnostních atributů DDI. Při prvních užitích kvantitativní metody není cílem získat přesné hodnoty dopadů, ale nastavit základní úroveň dopadů na základě současných poznatků a připravit tak možnost v průběhu dalších cyklů zlepšování systému odhady zpřesňovat.

Hodnota aktiv se odvíjí od hodnoty těchto aktiv pro jejich majitele (organizaci), pro jeho hlavní činnosti (účel existence). Dopady na hlavní činnost organizace proto vyhodnocuji v případě bezpečnostních incidentů, viz Obrázek 2: Bezpečnostní atributy, kapitola 1.2, na základě možné škody, která by mohla vzniknout v případě úniku informací, jejich pozměnění nebo zničení a dále pak nedostupností nebo omezení služeb.

.....

¹³ anglicky Work based structure – rozpad projektu na jednotlivé činnosti, úkoly (Schwalbe, 2011).

Hodnocení aktiv je prováděno dle požadavků VKB. V tomto prováděcím předpisu ZKB je uveden výpočet aktiva na základě Vzorců č. 3 – 5, kapitola 2.3.2.

2.3.1 Postup při hodnocení

Použiji metodu BIA (Business Impact Analysis)¹⁴. Hodnocení aktiv provedu s jejich garanty v oblasti odhadu počtů osob dotčených osob a v oblasti odhadu materiálních dopadů narušení jednotlivých atributů bezpečnosti DDI při případném bezpečnostním incidentu. Zdrojem dat budou Dotazníky.

1. Dotčené osoby v případě potřeby rozdělím do kategorií typických pro IS. Půjde o interní uživatele.
2. Pro odhad materiálních resp. finančních dopadů uvažuji dopady do oblastí: Minimálně přímých škod (zaplacení smluvní pokuty za nedostupnost nebo porušení důvěrnosti, náklady na znovupořízení a / nebo obnovení provozu), ale také dopady vyplývající z porušení legislativních povinností, resp. další oblasti dle zkušenosti garanta primárního aktiva (Čermák, 2009).

Tabulka 6: Stupnice pro hodnocení důležitosti aktiva

Hodnota	Důležitost	Popis
1	Nedůležité	Aktiva, jejichž poškození nebo ztráta může mít pouze lokální, krátkodobý vliv na vedlejší, podpůrné procesy organizace. Bez tohoto aktiva není omezena hlavní činnosti oddělení.
2	Důležité	Aktiva, jejichž poškození nebo ztráta může mít zjistitelný/ověřitelný dopad na důležité podpůrné, řídicí nebo hlavní procesy resp. dobré jméno, výkonnost či zájmy organizace.
3	Velmi důležité	Aktiva, jejichž poškození nebo ztráta může mít dopad na fungování organizace či jiný IS. Bez tohoto aktiva se velmi omezí hlavní činnosti oddělení či výstupy z nich jsou omezeny.
4	Kritické	Bez tohoto aktiva se zcela zastaví hlavní činnosti oddělení či výstupy z nich nebudou validní, nebo nebudou k dispozici.

Zdroj: Vlastní vypracování dle (MVČR, 2018a).

Pro každé aktivum je dotazováno více respondentů, proto výsledné hodnoty z vrácených vyplněných Dotazníků spočítám jako vážený průměr zjištěných hodnot

.....

¹⁴ jedná se vlastně o What-If analýzu.

zaokrouhlený na celá čísla nahoru. Váhou pro výpočet váženého průměru je četnost určité hodnoty důležitostí/bezpečnostních atributů aktiva v odpovědích. Modelový výpočet je uveden v kapitole 2.3.2.

$$Hodnota = \frac{(w_1 * x_1) + (w_2 * x_2) + (w_n * x_n)}{w_1 + w_2 + w_n} \quad (1)$$

Hodnocení všech aktiv, které byly respondenty identifikovány, pokračuje zpřesňující Otázkou č. 3. Dotazník z Přílohy č. 1 této práce, byl upraven o níže uvedené bezpečnostní atributy DDI. Otázka č. 3:

- Ohodnoťte aktiva IS FACILITY z hlediska úrovně důvěrnosti.
- Ohodnoťte aktiva IS FACILITY z hlediska úrovně integrity.
- Ohodnoťte aktiva IS FACILITY z hlediska úrovně dostupnosti.

Při hodnocení důležitosti je především třeba posoudit:

- Rozsah a důležitost osobních údajů nebo obchodního tajemství;
- Dotčené právní povinnosti nebo jiné závazky;
- Narušení vnitřních řídicích a kontrolních činností;
- Možné finanční ztráty, atd.

Tabulka 7: Stupnice pro hodnocení důvěrnosti primárního aktiva - DU

Hodnota/váha	Úroveň	Popis
1	Nízká	Aktiva poskytují či zpracovávají informace veřejně přístupné nebo určené ke zveřejnění (např. na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů). Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy organizace.
2	Střední	Aktiva poskytují či zpracovávají informace, které nejsou veřejně přístupné a tvoří know-how organizace, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.
3	Vysoká	Aktiva poskytují či zpracovávají informace, které nejsou veřejně přístupné a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů).
4	Kritická	Aktiva poskytují či zpracovávají informace, které nejsou veřejně přístupné a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. daňové tajemství, citlivé osobní údaje, strategické informace).

Zdroj: Vlastní vypracování dle (MVČR, 2018a).

Tabulka 8: Stupnice pro hodnocení integrity primárního aktiva - IN

Hodnota/váha	Úroveň	Popis
1	Nízká	Narušení integrity primárního aktiva resp. informací jím poskytovaných či zpracovávaných neohrožuje oprávněné zájmy organizace. Aktivum nevyžaduje ochranu z hlediska integrity.
2	Střední	Narušení integrity primárního aktiva resp. informací jím poskytovaných či zpracovávaných může vést k poškození oprávněných zájmů organizace a může se projevit méně závažnými dopady na primární aktiva. Aktivum může vyžadovat ochranu z hlediska integrity.
3	Vysoká	Narušení integrity primárního aktiva resp. informací jím poskytovaných či zpracovávaných vede k poškození oprávněných zájmů organizace s podstatnými dopady na primární aktiva. Aktivum vyžaduje ochranu z hlediska integrity.
4	Kritická	Narušení integrity primárního aktiva resp. informací jím poskytovaných či zpracovávaných vede k velmi vážnému poškození oprávněných zájmů organizace s přímými a velmi vážnými dopady na primární aktiva. Aktivum vyžaduje speciální ochranu z hlediska integrity.

Zdroj: Vlastní vypracování dle (MVČR, 2018a).

Tabulka 9: Stupnice pro hodnocení dostupnosti primárního aktiva - DO

Hodnota/váha	Úroveň	Popis
1	Nízká	Narušení dostupnosti primárního aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
2	Střední	Narušení dostupnosti primárního aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů organizace.
3	Vysoká	Narušení dostupnosti primárního aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů organizace. Primární aktivum je považováno za velmi důležité.
4	Kritická	Narušení dostupnosti primárního aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů organizace. Primární aktivum je považováno za kritické.

Zdroj: Vlastní vypracování dle (MVČR, 2018a).

Hodnot, kterých mohou dílčí parametry DDI nabývat jsou v rozsahu <1 – 4> a jsou uvedeny v Tabulkách. Viz Tabulka 7, Tabulka 8, Tabulka 9.

2.3.2 Celková hodnota aktiva

Celková hodnota aktiva se vypočte podle následujícího vzorce.

$$\text{Hodnota aktiva (HA)} = \text{důležitost} \times (C + I + A) \quad (2)$$

Pro potřeby této práce vyčíslíme hodnotu aktiva pomocí jednotlivých bezpečnostních atributů (DDI) prostřednictvím parametrů UDU, UIN, UDO:

$$UDU = Kd \times \text{důvěrnost} \quad (3)$$

$$UIN = Kd \times \text{integrita} \quad (4)$$

$$UDO = Kd \times \text{dostupnost} \quad (5)$$

Kde U_x je úroveň aktiva dle jednotlivých atributů x , Kd je důležitost aktiva. Rozsah hodnot parametrů U_x je $\langle 1 - 16 \rangle$, tento rozsah transformujeme do čtyř úrovně stupnice normovaných hodnot, viz Tabulka 10.

WBS projektu:

- Workshop
- Provést hodnocení aktiv
- Zdokumentovat aktiva

Tabulka 10: Stupnice normovaných hodnot DDI - U_x

Normovaná hodnota	Úroveň hodnoty aktiva	Hodnota parametru U_x je v intervalu
1	Nízká	$\langle 1 - 4 \rangle$
2	Střední	$\langle 4 - 6 \rangle$
3	Vysoká	$\langle 7 - 9 \rangle$
4	Kritická	$\langle 10 - 12 \rangle$

Zdroj: Vlastní zpracování

Tabulka 11: Modelový výpočet pro důležitost

	Důležitost	Hodnota
Respondent 1	Velmi důležitá	3
Respondent 2	Kritická	4
Respondent 3	Nedůležitá	1
Vážený průměr		3

Zdroj: Vlastní zpracování.

Tabulka 12: Modelový výpočet hodnocení DDI

Katalog ID	Důvěrnost	Integrita	Dostupnost
Respondent 1	3	2	3
Respondent 2	1	3	4
Respondent 3	2	4	2
Vážený průměr	2	3	3

Zdroj: Vlastní zpracování.

Tabulka 13: Modelový výpočet, hodnota aktiva

Hodnota aktiva	UDU	UIN	UDO
Osobní data	6	9	9
Normovaná hodnota	2	3	3

Zdroj: Vlastní zpracování

Tabulka 11, Tabulka 12 a Tabulka 13 uvádí modelový výpočet. Celková hodnota důležitosti bude vypočtena jako průměr výsledných hodnot důležitosti. Výsledná hodnota důvěrnosti, integrity a důležitosti aktiva bude vypočtena jako vážený průměr zjištěných hodnot zaokrouhlený na celé číslo nahoru. Váhou pro výpočet váženého průměru je četnost určité hodnoty aktiva v odpovědích.

2.4 Identifikace hrozeb a zranitelností

Hrozbu definuje (Čermák, 2009) jako „náhodnou nebo úmyslně vyvolanou událost, která může mít negativní dopad na důvěrnost, integritu a dostupnost aktiv. „ Každý informační systém je vystaven působení mnoha různých hrozeb, a pokud chceme těmto hrozbám čelit, musíme je nejprve identifikovat.

Cílem procesu identifikace hrozeb je sestavení Katalogu hrozeb, které mohou ohrozit alespoň jedno z relevantních aktiv IS. Výchozím seznamem hrozeb je seznam generických hrozeb obvykle působících na IS, který je dostupný v odborné literatuře, doplněný o vlastní zkušenosti. Společně s hrozbami jsou identifikovány rovněž zdroje původu hrozeb.

Hrozby budou identifikovány obecně podle typu, např. neoprávněné akce, fyzické zničení, technické poruchy. Následně jsou, v případě potřeby, identifikovány v rámci obecné třídy jednotlivé hrozby do úrovně detailu potřebného pro následné určení míry rizika a příslušných protiopatření.

V Příloze č. 3 této práce je výstup Katalog hrozeb a opatření. Seznam hrozeb vychází z katalogu hrozeb a zranitelností, obsažených ve VKB, a doplněných o hrozby specificky identifikované.

WBS projektu:

- Workshop k identifikaci hrozeb a zranitelností
- Zdokumentovat hrozby a zranitelnosti

2.5 Hodnocení hrozeb a zranitelností

V této fázi je třeba stanovit úroveň hrozby pro každou dvojici hrozba-aktivum. Neexistuje zde žádný zásadní algoritmus. Je ještě více založen na subjektivním úsudku osob, kteří prováděli identifikaci a hodnocení aktiv. Lze vycházet ze statistik nebo z evidence dosavadních bezpečnostních incidentů, jsou-li však k dispozici. Zdrojem může být i zkušenosti převzaté z jiných organizací nebo informace na internetu.

2.5.1 Stanovení úrovně dopadu hrozeb - UDH

U každé hrozby je stanovena úroveň dopadu na aktiva, tedy možné nepříznivé následky působení hrozby s využitím určité zranitelnosti aktiv. Jelikož aktiva i hrozby jsou různého charakteru, i formy (působení hrozby na jednotlivé bezpečnostní atributy aktiv) a úrovně dopadů mohou být různé. Pro ohodnocení úrovně dopadu konkrétní hrozby (UDH) působící na konkrétní aktivum využitím jeho zranitelnosti použijí při kvalitativní metodě hodnotu tohoto aktiva postupem při hodnocení aktiv. Volím při tom nejvyšší možnou úroveň dopadu z hlediska bezpečnostních atributů a ovlivněných aktiv, $UDH = \max \{U_x\}$.

Příklad: Pokud tedy hrozba působí na více atributů např. na dostupnost (nejvyšší úroveň dopadu 3) a zároveň na integritu (nejvyšší úroveň dopadu 1) je $UDH = 3$. To znamená, nejzávažnější vliv na zasažená aktiva je v omezení dostupnosti.

2.5.2 Pravděpodobnost hrozby - UPH

Podle Čermáka (2009) se u každé hrozby pro účely analýzy rizik stanovuje pravděpodobnost výskytu hrozby. U náhodných hrozeb se jejich pravděpodobnost odhadne na základě historických dat a statistik. U úmyslných hrozeb a pokročilých hrozeb (někdy označovaných jako „pokročilé přetrvávající hrozby“ je nutné vyhodnotit faktory jako je velikost, významnost, známost a oblíbenost organizace a aktiva, protože lze předpokládat, že vždy existuje útočník s motivem, příležitostí a schopností danou hrozbu realizovat. Tím se dostáváme k tomu, že pravděpodobnost hrozby je v některých případech do značné míry závislá na hodnotě aktiva.

Pro analýzu pravděpodobností působení hrozeb vůči danému podpůrnému aktivu bude využito doporučení z Přílohy č.2 prováděcího předpisu VKB. Zde jsou definovány čtyři úrovně pravděpodobnosti hrozby (UPH), kterých může pravděpodobnost dopadu hrozby na aktivum nabývat, viz Tabulka 14.

Tabulka 14: Stupnice pro hodnocení pravděpodobnosti hrozby

Hodnota UPH	Úroveň	Popis
1	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
2	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace je v rozpětí od 1 roku – 5 let.
3	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
4	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Zdroj: Vlastní vypracování dle (MVČR, 2018a).

2.5.3 Úroveň zranitelnosti - UZH

Úroveň zranitelnosti aktiva hrozbou (UZH) se vyhodnocuje na úrovni podpůrného aktiva. Analyzuje se míra zranitelnosti daného aktiva vůči působení dané hrozby. Při stanovení úrovně zranitelnosti se bere v úvahu kvalita implementovaných bezpečnostních opatření, která účinnost hrozby snižují. Implementovaná bezpečnostní opatření zahrnují také schopnost detekce pokusů o překonání aplikovaných bezpečnostních opatření a úroveň a četnost kontroly účinnosti bezpečnostních opatření. Pro provedení analýzy budou využity 4 úrovně zranitelností s modifikovanými kritérii, jejichž popis je uveden zde Tabulka 15.

Tabulka 15: Stupnice pro hodnocení úrovně zranitelnosti

Hodnota UZH	Úroveň	Popis
1	Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, které jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
2	Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.
3	Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známy dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známy úspěšné pokusy překonání bezpečnostních opatření.

Zdroj: Vlastní vypracování dle (MVČR, 2018a).

2.6 Hodnocení rizik

Jakmile jsou známy všechny tři parametry: úroveň dopadu hrozby, pravděpodobnost hrozeb a míra zranitelnosti aktiv, je možné přistoupit k výpočtu hodnoty rizika.

Mezinárodní standardy požadují jednu klíčovou podmínku pro stanovení metodiky výpočtu rizika – metoda výpočtu musí být popsána, musí poskytovat porovnatelné a měřitelné výsledky a v případě, že dojde ke změně hodnoty aktiva, hrozby nebo zranitelnosti, musí dojít také ke změně hodnoty rizika (Enisa, 2018).

Pro účely ohodnocení rizika využijí postup z VKB, který ukazuje výpočet hodnoty rizika jako funkci, založenou na třech parametrech. Pro každé aktivum stanovují hodnotu rizika (HR) působení hrozby na aktivum dle vzorce:

$$\text{Hodnota rizika (HR)} = \text{UDH} \times \text{UPH} \times \text{UZH} \quad (6)$$

Pozn.: UZH je úroveň zranitelnosti hrozbou,

UPH je úroveň pravděpodobnosti hrozby,

UDH je úroveň dopadu hrozby.

Úroveň dopadu hrozby bude, při výpočtu HR pro účely výběru opatření na zvládnutí rizik, odvozovat z maximální hodnoty dopadu hrozby na bezpečnostní atribut nejvíce ovlivněného aktiva, tj. hodnoty $\max \{U_x\}$.

Jestliže hrozba, kterou může být např. únik informací, může způsobit škodu jen z pohledu důvěrnosti, bude do výpočtu rizika vstupovat hodnota dopadu pro důvěrnost. Jestliže se bude jednat o hrozbu DDoS¹⁵, tak bude do výpočtu rizika vstupovat hodnota dopadu pro dostupnost. A jestliže hrozba např. hacking může způsobit jak únik informací, tak i jejich nežádoucí změnu nebo zničení, bude do výpočtu vstupovat nejvyšší hodnota dopadu. Tabulka 16 uvádí příklad výpočtu hodnoty rizika.

Tabulka 16: Příklad výpočtu HR z pohledu bezpečnostních atributů

Hrozba	Zranitelnost	Max {H _{Ax} } (x = DU)	Max {H _{Ax} } (x = DO)	Max {H _{Ax} } (x = IN)	UDH	UPH	UZH	HR
Únik informací	Nedostatečné řízení přístupu	3	4	4	3	4	3	36
DDoS	Není ochrana proti zahlcení	4	3	3	3	2	3	18
Hacking	Obsahuje chyby	1	3	4	4	1	2	8

Zdroj: Vlastní zpracování

Každý z parametrů UDH, může nabývat hodnot z rozsahu <1 – 4> a tedy celková hodnota rizika se pohybuje v intervalu <1 – 64>. Vypočtená hodnota rizika bude normalizována do rozsahu hodnot z intervalu <1 – 4>, viz Tabulka 17.

.....

¹⁵ Typ útoku DDoS (distribuované útoky) zasílá záplavu paketů s cílem zahltit informační systém (Jirásek et al., 2013).

Tabulka 17: Normování hodnoty rizika (HR)

Hodnota	Úroveň	HR	Popis
1	Nízká	<1 – 9>	Riziko je považováno za přijatelné.
2	Střední	<12 – 24>	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
3	Vysoká	<27 – 36>	Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.
4	Kritická	<48 – 64>	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění.

Zdroj: Vlastní zpracování

3 Analýza rizik ve vybrané organizaci

Forma zpracování analýzy rizik je vedena jako projekt. Prováděli jsme jej ve za použití interních zaměstnanců bez využití služeb externí firmy. Majitelé společnosti si přejí, aby zůstalo jméno jejich společnosti v anonymitě, z důvodu ochrany informací. Název společnosti je fiktivní, některé údaje o společnosti jsou v této praktické části lehce pozměněny. Informace o sesbíraná data o informačním systému IS FACILITY, který je analyzován, jsou skutečná. Rozsah výstupní dokumentace bude zkrácen z důvodu přesahu stanoveného rozsahu diplomové práce. Jedná se však o zrealizovanou analýzu a i přes zkrácené výstupní zprávy není ovlivněna kvalita realizovaného projektu.

3.1 Kontext organizace

Společnost FACILITY s.r.o. vznikla v roce 1996, se základním jměním ke konci roku 2017 je více než 7 mil Kč. Společnost se stala součástí akvizice mezinárodní mateřské společnosti a dle jejich dalších aktivit – fúze, akvizice dalších firem do své skupiny – se rozšiřuje.

Organizace je specialistou v poskytování integrovaného facility managementu¹⁶, zajišťuje technické a podpůrné služby, neustále inovuje své služby a svým klientům nabízí unikátní know-how. V současné době spravuje cca 10tis objektů s více než 6 miliony m2 podlahové plochy. Působí na českém trhu a rychle se rozrůstá, koncem roku 2017 měla 500 zaměstnanců na plný úvazek. Pro správu nemovitostí je alokováno přibližně 450 zaměstnanců. Organizace se soustředí především na komplexní správu nemovitostí a vyhledávání nových rentabilních projektů. Správa a údržba nemovitostí zahrnuje technické služby, úklidové služby, havarijní služby, energetický management, revize technických zařízení. Dále poskytuje tzv. lehké služby, podpůrné administrativní služby mezi které patří bezpečnostní služby, recepce, helpdesk, úklid. Velký důraz klade na aktivní spolupráci se zákazníky, a komplexní kvalitní službu nejvyššího stupně, profesionalitu, příznivé pracovní podmínky, společenskou odpovědnost s šetrným přístupem k životnímu prostředí, což přispívá ke konkurenční výhodě.

.....

¹⁶ Pro facility management existuje ve světě mnoho definic. Jedná se však spíše modifikace původní definice asociace IFMA: „Metoda, jak v organizacích sladit pracovní prostředí, pracovníky a pracovní činnosti. Zahrnuje v sobě principy obchodní administrativy, architektury, humanitních a technických věd (IFMA.cz, 2018).“

3.1.1 Vize

Vize společnosti spočívá v poskytování komplexních služeb spojených se správou a údržbou majetku. Zaměřuje se na kvalitu poskytovaných služeb, protože úroveň kvality umožňuje jejich zákazníkům soustředit se na výhradně na jejich podnikání a zhodnocení jejich investic. Vůči všem zaměstnancům nabízí stabilitu, hodnocení dle schopností, možnost firemního a osobního růstu na základě stanovených pravidel. Usiluje o to, aby byl pro zaměstnance prestižním zaměstnavatelem. Vůči širší společnosti zastává pravidla trvale udržitelného vývoje. Buduje neustále se rozvíjející dlouhodobé partnerství všech zainteresovaných stran.

Strategie firmy staví na 9 oblastech, jejichž rozvoj plánuje do ročních cílů. Spokojení zákazníci, odborně způsobilí a loajální zaměstnanci, kvalitní dodavatelé, soulad s právními předpisy, šetrnost k životnímu prostředí, technické prostředky a materiál, prevence v oblasti bezpečnosti a ochrany zdraví při práci, kontrolní systém a etický kodex.

Pro zachování základních myšlenek vize si majitelé společnosti FACILITY s.r.o. zakládají na zachování kontinuity své společnosti, mají zájem o eliminaci a potlačení rizika. Uvědomují si, že například ochranou důvěrných informací způsobí nižší tempo růstu či zisku vůči konkurenci. Podporují zavedení procesu řízení rizik a projekt analýzy rizik.

3.1.2 Charakteristika informačního systému

Informační systém FACILITY má společnost postaven na základě tohoto modelu firmy ManageEngine, viz Obrázek 6: CAFM model IS Facility.

3.2 Zahájení projektu

Hlavními faktory:

- Získání aktivní podpory managementu;
- Inicie projektu;
- Identifikace zainteresovaných stran;
- Zadávací listina projektu.

Vedení společnosti si uvědomuje, že pro požadovaný růst je třeba provést kroky, které pomohou k udržení se v přední linii před konkurencí. Obchodní příležitosti jsou v některých případech limitovány požadavky plynoucí ze zákona o veřejných zakázkách. Informační systém FACILITY, ve kterém společnost spravuje své nemovitosti, závazky, příležitosti a služby s nimi spojené, je na vysoké úrovni, nebyl

však proveden audit a společnost nemá certifikaci dle standardu ISO/EIC 2700x. Zároveň není známo zda IS splňuje požadavky ZKB a jeho prováděcích předpisů.

Obrázek 6: CAFM model IS Facility



Zdroj: (Zoho Corporation, 2013).

Od realizace projektu organizace očekává zavedení procesu ISMS. Vedoucí pracovníci si uvědomují, že při procesu analýzy rizik dojde k ověření skutečného stavu jejich IS a veškeré hrozby budou posouzeny v souladu s legislativními požadavky kladené na jejich společnost. Výstupem projektu je návrh opatření a odstartování nikdy nekončícího procesu zlepšování. Dalším efektem projektu očekávají zvýšení důvěryhodnosti a otevření dalších obchodních příležitostí. Společnost se tak stane lépe připravenou, méně zranitelnou v oblasti kybernetické kriminality. Tabulka 20 obsahuje zadávací listinu projektu.

3.2.1 Iniciace projektu

Před samotným zahájením projektu bývá zvykem definovat:

- rozsah, čas, náklady projektu;
- identifikovat sponzora projektu;
- zvolit projektového manažera;
- setkání týmu, případná revize procesu a očekávání, které souvisí s projektem.

Základem pro spuštění projektu je rozhodnutí vedení společnosti o realizaci. Projekt získal vysokou prioritu a jeho garantem se stal Jan Novák, jeden z vlastníků. Před finálním rozhodnutím o spuštění projektu byl zpracován předběžný rozsah, náklady a harmonogram projektu. Projektovým manažerem byl zvolen projektový manažer firmy.

Analýza zahrnuje pouze vybrané kritické části systému. Do této skupiny jsou zahrnuty data o majetku. Analyzovány jsou software, hardware, data, lidé, dokumentace, a aplikační programové vybavení, které souvisí s vymezenou oblastí. Na projektu se podíleli interní zaměstnanci, konkrétně v počtu 5 osob z různých oddělení. Do projektu budou zapojeni i ostatní vybraní zaměstnanci, v roli respondentů. Tabulka 18: Inicie projektu obsahuje základní informace o projektu před jeho zahájením.

3.2.2 Identifikace zainteresovaných stran

Pro splnění klíčových předpokladů projektu si vlastník projektu uvědomuje, že je třeba sestavit silný projektový tým. Projektový manažer je vlastníkem projektu považován za schopného člověka vést takový tým. V roli specialisty kybernetické bezpečnosti byl nominován konzultant z IT oddělení. Technologickým architektem byl nominován analytik z IT oddělení. Člen týmu pro potřeby projektového manažera byl nominován koordinátor helpdesku z IT oddělení. Vedoucí IT oddělení jako poradce a garant aktiv. Seznam zainteresovaných stran, viz Tabulka 19: Zainteresované strany.

3.3 Plánování projektu

V rámci plánování analýzy byly provedeny následující činnosti. Byl(a):

- stanoven cíl analýzy rizik;
- dojednána metodika, hranice a hloubka analýzy;
- zainteresované strany se dohodly na pojmech;
- stanoven rozsah, harmonogram, rozpočet a délka trvání projektu;
- Připraven rozpad, WBS, viz Tabulka 21;
- Sestaven analytický tým a dohodnuta pravidla komunikace;
- Dohodnut způsob přenosu dat.

Tabulka 18: Iniciace projektu

Projektový manažer	Anna Bílá
Cíle	Získat audit dle zákona 205/2017. Mezi strategické cíle společnosti FACILITY s.r.o. trvalý růst, ziskovost a udržení kvality poskytovaných služeb. Projekt přispěje k realizaci těchto cílů tím, že zvýší úroveň zabezpečení svého IS pro interní i externí účely. Výstupy projektu slouží ke zvládnutí rizik a k zavedení systému řízení bezpečnosti informací.
Současná situace a popis problému/potřeby	Společnost disponuje ve svém informačním systému FACILITY citlivými daty – interními a i třetích stran. Společnost do bezpečnosti IS sice investuje, ale ISMS nemá vytvořený. Potřeba vznikla také z legislativních požadavků GDPR, ZKB. Některé obchodní případy byly ztraceny pro nesplnění požadavků ze zadávací dokumentace výběrového řízení. Dalším důvodem je potřeba řídit ve firmě bezpečnostní rizika, pro který není vypracován plán zvládnutí rizik. Zaměstnanci nejsou v oblasti kybernetické bezpečnosti pravidelně školeni.
Klíčové předpoklady	Zájem vedení zavést opatření pro řízení rizik. Spolupráce a součinnost v rámci firmy. Podpora TOP managementu. Plnění harmonogramu. Projekt musí vést zkušený projektový manažer a součástí projektového týmu musí být zástupci z dotčených oddělení. Musí být podpořen top managementem.
Předběžné požadavky	Získat audit dle zákona 205/2017. Zavést ISMS.
Odhad rozpočtu	Předběžný odhad nákladů činí 3.720 tis Kč. Pracnost projektu je odhadována 280 MD17, průměrná cena činí 12000 Kč. Jednorázové náklady za nákup nového SW se nepředpokládají. Pro udržitelnost projektu během 2 let se předpokládají náklady 360.000 Kč/rok na aktualizaci a koordinaci informací vytvořené dokumentace.
Návrh harmonogramu	Přáním sponzora – vlastníka projektu je dokončit projekt do 3 měsíců, existuje však předpoklad, že bude vypracovaný projekt bude užitečný po dobu 2 let. Za předpokladu, že se nezmění ZKB nebo jiné předpisy.
Možná rizika	Zajištění finančních prostředků, odbornost týmu. Zajištění spolupráce stávajících dodavatelů. Zajištění spolupráce v rámci firmy. Zaměstnanci jsou ochotni se účastnit projektu a podporovat využívání navržených opatření. Projektový tým pracuje efektivně, a je stabilní. Během realizace jsou k dispozici očekávané kapacity týmů. Tým plní harmonogram. Nehrozí nedostatek finančních prostředků.

Zdroj: Vlastní zpracování

Analytický tým byl sestaven. Zkratka pro projektového manažera – PM. Pravidla komunikace byly stanoveny v tomto rozsahu. Jako projektový tým budeme pracovat proaktivně, snažit se předcházet potenciálním problémům. Budeme se:

- vzájemně informovat o všem, co je důležité k projektu;
- vést diskuzi ve stejnou dobu;

- PM včas a s předstihem informovat, pokud hrozí nedodržení termínu k předem určenému úkolu;
- Rozhodovat jako tým;
- používat e-mail, sdílené adresáře (např. ftp) a další technologie k usnadnění komunikace;
- spolupracovat při tvorbě harmonogramu, aktuální data vkládat do předem určeného místa vždy do pátku do 16h.

Tabulka 19: Zainteresované strany

Jméno	Pozice	Interní/Externí	Role v projektu
Jan Novák	Vlastník firmy	interní	Sponzor projektu
Oto Veselý	Vedoucí IT oddělení	interní	Garant aktiv, poradce.
Anna Bílá	Projektový manažer	interní	Řídí projekt.
Josef Rozsah	Konzultant	interní	Specialista kybernetické bezpečnosti
Pavel Starý	Koordinátor helpdesk	interní	Specialista kybernetické bezpečnosti
Jan Pilný	Analytik IT	interní	Technologický architekt

Zdroj: Vlastní zpracování

3.4 Realizace projektu

Je provedena v tomto rozsahu:

- Identifikace respondentů.
- Rozdílová analýza.
- Identifikace, dekompozice aktiv a hodnocení aktiv.
- Identifikace a hodnocení hrozeb a zranitelností.
- Hodnocení rizik.
- Výběr vhodných opatření.

.....

¹⁷ Jedná o anglický výraz pro vyjádření ceny práce za 1 den (8hodin) používaný zejména v IT projektech. Manday = člověkodenní.

- Výběr vhodných opatření
- Plán zvládnutí rizik, Prohlášení o aplikovatelnosti realizace jednotlivých opatření, kontrola realizace, zpráva o zvládnutí rizik.

Tabulka 20: Zadávací listina projektu

Název projektu	Analýza rizik IS FACILITY
Termín zahájení projektu	1.1.2018
Termín ukončení projektu	31.3.2018
Rozpočet	Společnost alokovala 3 720 000 Kč. Většinu nákladů budou tvořit interní náklady na mzdy.
Manažer projektu	Projektový manažer firmy Anna Bílá
Projektové cíle	Audit dle ZKB č. 205/2017. Zvýšení úrovně zabezpečení IS FACILITY. Návrh opatření ke zvládnutí rizik.
Hlavní kritérium projektu	Projekt bude realizován ve schválených nákladech do 3 měsíců.
Role a odpovědnosti	Majitel společnosti - sponzor projektu Vedoucí IT oddělení – garant aktiv Specialista kybernetické bezpečnosti – člen týmu Projektový manažer – manažer projektu Garant aktiv – člen týmu Majitel společnosti - sponzor projektu Technologický architekt – člen týmu
Rizika projektu	Nedostatek nebo nízká kvalita informací od interních garantů. Ne všechny náklady byly identifikovány a zahrnuty do plánu. Dodržení časového harmonogramu.

Zdroj: Vlastní zpracování

3.4.1 Rozdílová analýza dokumentace

Před zahájením analýzy rizik byla provedena rozdílová analýza dle požadavků vyplývajících z prováděcího předpisu VKB, v rozsahu organizačních i technických opatření.

Je realizována v tomto rozsahu:

- Identifikace současného stavu,
- Identifikace bezpečnostních opatření (organizační a technická) organizace,
- Identifikace shody opatření s povinnostmi ZKB.

Výstupem rozdílové analýzy jsou chybějící části základny pro ISMS, organizační a technická opatření. Tabulka 22 znázorňuje organizační opatření, Tabulka 23 technická opatření.

Tabulka 21: WBS projektu

Fáze projektu	WBS – jednotlivé činnosti projektu
Zahájení	Identifikace respondentů – zainteresovaných stran Zahajovací schůzka Zadávací listina projektu
Plánování	Plánovací schůzka týmu Deklarace rozsahu projektu WBS Harmonogram a přehled nákladů Určení zdrojů k úkolům Určení trvání úkolu Určení závislosti mezi úkoly Ganttův diagram
Realizace	Informace od respondentů, rozdílová analýza Šablony a nástroje Identifikace, dekompozice aktiv Ohodnocení aktiv Identifikace a hodnocení hrozeb Identifikace a hodnocení zranitelností Vyhodnocení rizik Výběr vhodných opatření
Monitorování a kontrola	Zprávy o postupu
Uzavření	Rozhodnutí o způsobu zvládnutí rizik Plán zvládnutí rizik Návrh opatření Plán zvládnutí rizik Prohlášení o aplikovatelnosti

Zdroj: Vlastní zpracování

V rámci realizovaného projektu byly provedeny všechny úkoly. Pro stanovený cíl této práce rozepíši pouze ty výsledky, které jsou podstatné pro jeho splnění. Např. v práci nebudu uvádět Ganttův diagram apod.

Tabulka 22: Organizační opatření

Odkazy na VKB	Požadavky dle VKB	Návrh vypořádání
§ 3 Systém řízení bezpečnosti informací	NE	Vytvořit Směrnici ISMS
§ 4 Řízení rizik	NE	Stanovit Plán zvládání rizik.
§ 5 Bezpečnostní politika	Částečně	Vytvořit ke Směrnici ISMS
§ 6 Organizační bezpečnost	Částečně	Sestavit výbor kybernetické bezpečnosti
§ 7 Požadavky na dodavatele	Částečně	Dopracovat Politiku pro řízení vztahu s dodavateli
§ 8 Řízení aktiv	Částečně	Aktualizovat Směrnici klasifikaci aktiv
§ 9 Bezpečnost lidských zdrojů	Částečně	Evidence realizovaných školení. Pravidla a plán pro bezpečnost lidských zdrojů.
§ 10 Řízení provozu a komunikací	Částečně	Aktualizovat Směrnici o Řízení provozu určí pravidla pro řízení komunikací.
§ 11 Řízení přístupu osob k IS	Částečně	Do stávající dokumentace zpracovat politiku pro řízení přístupu osob k IS.
§ 12 Akvizice, vývoj a údržba	ANO	Splňuje
§ 13 Zvládání KBU a KBI	NE	Nákup outsourcing služeb
§ 14 Řízení kontinuity činností	NE	Stanovit politiku dle VKB
§ 15 Kontrola a audit IS	NE	Provést po realizaci analýzy rizik

Zdroj: Vlastní zpracování

3.4.1 Výsledky identifikace a dekompozice aktiv

Otázky byly předloženy 42 respondentům formou Dotazníku, viz Příloha č. 1. v elektronické podobě včetně pokynů a popisu. Nejprve respondenti odpovídali na Otázky č. 1 a 2, poté v druhém kole na Otázku č. 3.

Projektový tým provedl hodnocení aktiv podle schválené Metodiky. Ke každému aktivu je přidělen vlastník (garant).

Garanty aktiv a PM byla předdefinována aktiva, viz Tabulka 24, a provedena dekompozice IS.

Kvalitativní hodnota aktiva je dána na základě hodnocení daného aktiva z pohledu jednotlivých bezpečnostních atributů DDI. Dle předpokladů použité metody vycházíme při určení důležitosti (hodnoty) aktiv z dopadů na hlavní činnost IS FACILITY, se zohledněním dopadů z pohledu určení kritických míst IS.

Dotazníkového šetření se účastnilo celkem 42 respondentů, návratnost dotazníků byla 100 %. Nově definované Aktivum (informace) – osobní údaje třetích stran bylo stanoveno vzhledem k důležitosti nového Ustanovení EU o ochraně osobních údajů EU – GDPR.

Tabulka 23: Technická opatření

§	Požadavky dle VKB	Požadavky ZKB
§ 17	Fyzická bezpečnost	Analýza rizik
§ 18	Nástroj pro ochranu integrity v komunikační síti	Splňuje
§ 19	Nástroj pro ověřování identity uživatelů	Analýza rizik
§ 20	Nástroj pro ochranu před škodlivým kódem	Splňuje
§ 21	Nástroj pro zaznamenávání činnosti IS a jejich uživatelů a administrátorů	Analýza rizik
§ 22	Nástroj pro detekci KBI	Nesplňuje
§ 23	Nástroj pro sběr a vyhodnocování KBU	Nesplňuje
§ 24	Aplikační bezpečnost	Analýza rizik
§ 25	Kryptografické prostředky	Analýza rizik
§ 26	Nástroj pro zajišťování úrovně dostupnosti	Splňuje
§ 27	Bezpečnost průmyslových a řídicích systémů	Nezkoumáno

Zdroj: Vlastní zpracování

Tabulka 24: Identifikace a dekompozice IS

Katalog ID	Název aktiva	Garant aktiva	Skupina aktiv
A1	LAN switch	Administrátor	NET
A2	GW router		
A3	WAN router		
A4	DNS server		
A5	NTP server		
A6	Firewall		
A7	Wmware	Vedoucí IT oddělení	SW
A8	Windows 2003		
A9	MS SQL		
A10	Vmax appliance		
A11	SAN appliance		
A12	Windows 2008		
A13	Windows 7, Vista		
A14	.net Framework 4.0		
A15	FACILITY tlustý klient		
A16	Zálohovací zařízení	Vedoucí IT oddělení	HW
A17	Server IS360		
A18	Pracovní stanice (NB,DT)		
A19	SAN switch		
A20	Server DB45		
A21	Serveroví a síťoví správci	Vedoucí IT oddělení	Lidé
A22	Správci zabezpečovacího zařízení		
A23	Uživatel IS FACILITY		
A24	Admin IS FACILITY		
A25	Dodavatele	Vedoucí IT oddělení	Dodavatele
A26	Dokumentace	Vedoucí IT oddělení	Dokumentace
A27	Osobní údaje třetích stran	Vedoucí IT oddělení	Data

Zdroj: Vlastní zpracování.

Tabulka 25: Hodnocení aktiv

Katalog	Důležitost	Důvěrnost	Integrita	Dostupnost	UDU	UIN	UDO
ID	Kd	DU	IN	DO	Kd*DU	Kd*IN	Kd*DO
A1	4	1	4	1	1	4	1
A2	4	1	4	1	1	4	1
A3	4	1	4	1	1	4	1
A4	4	1	4	1	1	4	1
A5	3	1	2	1	1	2	1
A6	4	1	4	1	1	4	1
A7	4	4	4	4	4	4	4
A8	3	1	2	1	1	2	1
A9	4	4	4	4	4	4	4
A10	3	1	2	1	1	2	1
A11	2	1	3	1	1	2	1
A12	3	1	2	1	1	2	1
A13	3	1	1	1	1	1	1
A14	2	1	1	1	1	1	1
A15	4	1	1	1	1	1	1
A16	4	1	2	1	1	2	1
A17	4	1	2	1	1	2	1
A18	4	1	1	1	1	1	1
A19	4	4	4	4	4	4	4
A20	4	4	4	4	4	4	4
A21	4	4	4	4	4	4	4
A22	4	4	4	4	4	4	4
A23	2	1	1	1	1	1	1
A24	2	1	1	1	1	1	1
A25	3	1	1	2	1	1	2
A26	2	1	1	1	1	1	1
A27	4	3	3	3	3	3	3

Zdroj: Vlastní zpracování.

Tabulka 25 ukazuje výsledné hodnoty aktiv na základě provedeného výpočtu dle schválené metodiky hodnoty aktiv.

Výsledná hodnota důvěrnosti, integrity a důležitosti aktiva byla vypočtena jako vážený průměr zjištěných hodnot zaokrouhlený na celé číslo nahoru. Váhou pro výpočet váženého průměru byla četnost určité hodnoty aktiva v odpovědích.

Výsledná hodnota důležitosti aktiva z pohledu práce respondenta a práce IS FACILITY byla vypočtena jako vážený průměr zjištěných hodnot zaokrouhlený na celé číslo nahoru. Váhou pro výpočet váženého průměru byla četnost určité hodnoty důležitosti aktiva v odpovědích.

3.4.1 Identifikace a hodnocení rizik

Hrozby vychází z katalogu hrozeb a zranitelností, které jsou obsaženy ve VKB, a jsou doplněné o hrozby specificky identifikované. Tabulka 26 představuje hrozby, které jsou seřazeny dle hodnoty. Obrázek 7: Ukázka hodnocení rizik znázorňuje záznam z prováděného hodnocení v nástroji MS Excel.

Obrázek 7: Ukázka hodnocení rizik

Pravděpodobnost hrozby		Hodnota zděděná z dopadu na primární aktivum	LAN_switch	GW_router	WAN_router	DNS_server	NTP_server	Firewall	Vmware	SAN_switch	Vmax appliance	SAN appliance	Windows 2003	Server HP380	Windows 2008	Server / a
Klikněte na souhrn 1			NET	NET	NET	NET	NET	NET	SW	HW	SW	SW	SW	HW	SW	ST
Hrozba	Na jaký atribut bezpečnosti působí?	1	2	4	5	6	7	9	10	12	13	14	15	18	20	
porušení bezpečnostní politiky	CIA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
zneužití vnitřních prostředků	CIA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
zneužití identity fyzické osoby	CIA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
porušení licenčního ujednání	A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
selhání technického vybavení	CIA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
selhání softwarového vybavení	CIA	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1
hacking	CIA	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1
DDoS	A	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1
škodlivý kód	CIA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
nedostatek klíčových zaměstnanců	A	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1
přerušení dodávky elektřiny	IA	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
přerušení konektivity do internetu	A	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
selhání počítačové sítě	A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
zhoršení provozních podmínek	A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
poškození softwarového vybavení	CIA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
poškození technického vybavení	IA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
úmyslné smazání informací	A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
úmyslné pozměnění informací	I	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
krádež informací	C	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
krádež hmotného aktiva	A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
narušení fyzické bezpečnosti	CIA	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
únik informací z nedbalosti	C	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
pozměnění informací z nedbalosti	I	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
smazání informací z nedbalosti	A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
bombový teroristický útok	A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
požár	A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Zdroj: Vlastní zpracování dle nástroje po analýzu rizik MS Excel.

Tabulka 26: Hodnocení hrozeb

Hrozba	Hodnota hrozby
Přerušení konektivity do internetu	3
Záplava	2
Škodlivý kód	2
Poškození nebo selhání technického a sw vybavení	2
Přerušení dodávky elektřiny	2
Hacking	2
DDos	2
Zneužití identity fyzické osoby	1
Porušení licenčního ujednání	1
Demonstrace v okolí	1
Porušení bezpečnostní politiky	1
Zneužití vnitřních prostředků	1
Úmyslné smazání informací	1
Narušení fyzické bezpečnosti	1
Krádež informací	1
Požár	1
Blesk/přepětí	1
Odcizení/poškození aktiva	1
Záplava	1
Zemětřesení	1

Zdroj: Vlastní zpracování.

Tabulka 27: Hodnocení zranitelností a opatření

Zranitelnost	Ovlivněné hrozby	Opatření	Hodnota zranitelností
Nedostatečná ochrana před škodlivým kódem	Škodlivý kód	Antimalware řešení	4
Nedostatečná ochrana před škodlivým kódem	Hacking, DDoS	WAF	4
Nedostatečná autentizace	Zneužití vnitřních prostředků, zneužití identity fyzické osoby, úmyslné smazání informací, krádež informací	Autentizace	4
Nedostatečná kontrola změn	Škodlivý kód	Configuration review	4
Nedostatečné postupy pro případ útoků a incidentů	Hacking, DDoS, škodlivý kód	CSIRT	4
Nedostatečná ochrana před únikem informací	Únik informací z nedbalosti, krádež informací	DLP	4
Nedostatečné postupy pro případ útoků a incidentů	Hacking, DDoS, škodlivý kód	CSIRT	4
Nedostatečné plány kontinuity	Požár, záplava, demonstrace v okolí, zemětřesení	Plán kontinuity činností	4
Nedostatečná údržba IS	Selhání a poškození technického a sw vybavení, hacking, DDoS, škodlivý kód, přerušení dodávky elektřiny, přerušení konektivity do NET, úmyslné smazání informací, úmyslné pozměnění informací, krádež hmotného aktiva, požár, záplava, blesk/přepětí, zemětřesení	DRP	4
Nedostatečný monitoring činností uživatelů	Zneužití identity fyzické osoby, poškození sw vybavení, poškození technického vybavení, úmyslné smazání informací, krádež informací, únik informací, porušení bezpečnostní politiky, hacking, škodlivý kód	Monitoring	4
Nedostatečné testování	Hacking, selhání sw vybavení, únik informací z nedbalosti	Testování	3
Nedostatečné řízení lidských zdrojů	Krádež informací, poškození technického vybavení, úmyslné smazání informací, krádež hmotného aktiva	Řízení lidských zdrojů	2

Zdroj: Vlastní zpracování

3.5 Stanovení úrovně rizika

Hodnota úrovně rizika byla stanovena na základě výpočtu, který je uveden v Metodice. Úroveň rizika se nachází v nástroji pro analýzu rizik mezi hodnotami 0 až 64, z důvodu přesnějších výsledků. Přepočet výsledků na normovanou hodnotu 1 až 4, viz Tabulka 28: Normalizace hodnoty rizika úrovně rizika.

Tabulka 28: Normalizace hodnoty rizika úrovně rizika

Hodnota	Úroveň	HR – hodnota rizika	Popis
1	Nízká	<1 - 9>	Riziko je považováno za přijatelné
2	Střední	<12 -24>	Riziko může být sníženo méně náročnými opatřeními
3	Vysoká	<27- 36>	Riziko je dlouhodobě nepřijatelné a musí být zahájeny kroky k jeho odstranění
4	Kritická	<48 – 64>	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění

Zdroj: Vlastní zpracování

3.5.1 Porovnání úrovní rizik s kritérii pro přijatelnost rizik

V následujícím seznamu rizik je srovnání závažnosti vůči kritériím pro přijatelnost rizik, hodnoty normalizují, viz Tabulka 28. Níže se soustředím pouze na rizika, které mají normovanou hodnotu <2 – 4>. V této fázi je třeba porovnat a stanovit úroveň a kritéria pro přijatelnost rizik. Výstup je velmi rozsáhlý a diplomovou práci by o cca 10 stran zvýšil. Proto vkládám ukázkou hodnocených rizik pro vybrané hrozby, viz Tabulka 30, Tabulka 31, Tabulka 32. Rizika jsou seřazena podle hodnoty rizika, a podle hrozeb. Každé jednotlivé riziko je označeno vlastním číslem (ID). Tabulka 29 je ukázkou Katalogu rizik, který obsahuje seznam rizik dle ID. Katalog rizik je Přílohou č. 2 této práce.

3.5.1 Základní přístup k určení přijatelných rizik

Při zpracování analýzy rizik byl stanoven a schválen přístup pro určení přijatelných rizik. Rizika úrovně 1 budou považována za akceptovatelná, v případě že budou nadále monitorována, viz Tabulka 33.

Tabulka 29: Ukázka z Katalogu rizik

ID rizika	Hrozba	Zranitelnost	Opatření
R1	Porušení bezpečnostní politiky	Nedostatečná bezpečnostní osvěta	Osvěta
R2	Porušení bezpečnostní politiky	Nesynchronizovaný čas	Synchronizace času
R24	Zneužití identity fyzické osoby	Nedostatečná identifikace zaměstnanců	Visačka

Zdroj: Vlastní zpracování

Tabulka 30: Hodnota rizika pro Přerušení konektivity do internetu

ID rizika	Zranitelnost	Opatření	Hodnota rizika	Dotčená aktiva
R86	Nedostatečný DRP	DRP	4	Server IS360, Server DB45, MS SQL
R86	Nedostatečný DRP	DRP	3	LAN switch, WAN router, DNS server, Vmware, SAN switch, Serverové a síťové správci, správci zabezpečovacích zařízení, Server IS360
R86	Nedostatečný DRP	DRP	2	Firewall, Pracovní stanice (NB, DT), Windows 7, Vista, .net framework 4.0, IS tlustý klient, uživatel IS, admin IS
R87 R88 R89	Nedostatečný monitoring, Závislost na jednom ISP Jeden bod selhání.	Monitoring 2 ISP Autorekonfigurace	2	LAN switch, WAN router, DNS server, Firewall, Vmware, Serverové a síťové správci, Správci zabezpečovacích zařízení, Server IS360, Server DB45, MS SQL, Dokumentace, Dodavatelé

Zdroj: Vlastní zpracování.

Tabulka 31: Hodnota rizika pro Selhání softwarového vybavení

ID rizika	Zranitelnost	Opatření	Hodnota rizika	Dotčená aktiva
R33	Nedostatečné řízení zdrojů ICT	Řízení zdrojů ICT	3	DNS server
R34	Nedostatečný DRP	DRP	3	Server IS360
R34	Nedostatečný DRP	DRP	2	LAN switch, WAN router, DNS server, Vmware, SAN switch, Serverové a síťové správci, správci zabezpečovacích zařízení, Server IS360, Server DB45, MS SQL

Zdroj: Vlastní zpracování.

Tabulka 32: Hodnota rizika pro Hacking

ID rizika	Zranitelnost	Opatření	Hodnota rizika	Dotčená aktiva
R42 R44 R48 R49	Nedostatečné postupy pro případ útoku a incidentů Nedostatečné řízení technických zranitelností Nedostatečný monitoring Nedostatečné testování	CSIRT Skenování zranitelností Monitoring Bezpečnostní testy	3	GW router, Firewall, Server IS360
R43 R52	Nedostatečný DRP Nedostatečná ochrana před škodlivým kódem	DRP, WAF	3	Server IS360
R42, R43 R44 R48 R49	Nedostatečné postupy pro případ útoku a incidentů Nedostatečný DRP Nedostatečné řízení technických zranitelností Nedostatečný monitoring Nedostatečné testování	CSIRT DRP skenování zranitelností monitoring bezpečnostní testy	2	Firewall, Pracovní stanice (NB, DT), Windows 7, Vista, .net framework 4.0, IS tlustý klient, uživatel IS, admin IS
R49	Nedostatečné testování	testování	2	Vmware, Serveroví a síťoví správci, Správci zabezpečovacích zařízení, Server IS360, Server DB45, MS SQL
R52 R54	Nedostatečná ochrana před škodlivým kódem Nedostatečná kontrola připojení necertifikovaných zařízení	Hardening NAC	2	GW router
R53	Nedostatečná ochrana před škodlivým kódem	WAF	2	Server IS360, Server DB45, MS SQL

Zdroj: Vlastní zpracování

3.5.2 Posouzení dopadu na aktiva

Na základě hodnocení aktiv a rizik, které bylo provedeno v předchozích podkapitolách lze konstatovat, že největším rizikem pro aktiva je přerušení konektivity do internetu. Ta by v nejvyšší možné kritické hodnotě <4> mohla ovlivnit aktiva Server IS360, Server DB45, MS SQL. Způsob, jak řešit rizika je uveden v následující kapitole.

Tabulka 33: Hodnota rizika pro Porušení licenčního ujednání

ID rizika	Zranitelnost	Opatření	Hodnota rizika	Dotčená aktiva
R26	Porušení licenčního ujednání	Nedostatečná kontrola licencí	1	Všechna aktiva

Zdroj: Vlastní zpracování

3.6 Ukončení projektu

Pro komplementaci podkladů pro finální výstupy a prezentaci výsledků analýzy rizik sloužili následující dokumenty, Prohlášení o aplikovatelnosti, Plán zvládání rizik. VKB předepisuje jejich minimální obsah, resp. Osnovu. Pro sestavení těchto zpráv bylo nezbytné kromě dat shromážděných v průběhu jednotlivých fází projektu analýzy rizik učinit další kroky. Sestavit katalog opatření, sestavit registr rizik, sestavit a schválit seznam možných přístupů pro zvládání rizik a stanovit a schválit základní přístup organizace pro určení přijatelných rizik.

3.6.1 Registr rizik

Jde o nástroj jehož pomocí byla zpracována analýza rizik. Jedná se o databázi, která svoji strukturou umožňuje efektivně zpracovávat data během analýzy do finálních výstupů.

3.6.2 Přístupy pro zvládání rizik

U identifikovaných rizik je nutné analyzovat možnosti jejich ošetření a zvolit vhodnou metodu pro zvládání rizika. Při výběru nejvhodnější metody je klíčové zvážit náklady a přínosy jednotlivých možností pro zvládání rizika (Fenz et al., 2014). Organizace schválila následující přístupy pro zvládání rizik.

Akceptace rizika. Doporučuje se u rizik nízké úrovně a zbytkových rizik. Případně je riziko akceptovat u těch případů, kdy náklady na implementaci opatření či přenos rizika neúměrně převyšují dopad rizika.

Přenos rizika na jinou stranu. Doporučuje se u rizik s vážným dopadem, ale nízkou pravděpodobností hrozby. Přenos rizik může být realizován např. formou pojištění nebo outsourcingu.

Redukce rizika na přijatelnou úroveň prostřednictvím zavedení bezpečnostních opatření. Doporučuje se u všech rizik s vysokou pravděpodobností hrozby.

Vyhnutí se riziku, chápáno jako rozhodnutí organizace upustit od plánované činnosti nebo změnit podmínky provozu některých činností. Doporučuje se u rizik s kritickou úrovní a tam, kde není možné využít výše zmíněné přístupy.

3.6.3 Návrh způsobu zvládání rizik pro vybranou společnost

Příloha č. 4 obsahuje Návrh způsobu zvládání rizik. Přehled identifikuje opatření v návaznosti na existující rizika, rizika jsou zastoupena pouze svými ID. V tomto seznamu jsou uvedena rizika všechna, včetně těch, na která nemusí být uplatněno žádné opatření. V posledním sloupci je zdůvodnění navrženého opatření vyplývajícího z VKB.

3.6.4 Návrh a realizace opatření

VKB striktně předepisuje implementaci některých opatření, nebo předepisuje jejich parametry (například sílu hesla). Tato opatření jsou uvedena v katalogu opatření. Z tohoto katalogu jsou vybírána bezpečnostní opatření k redukci rizik, která by měla být nasazena do míst identifikovaných při analýze rizik.

Konkrétní opatření se provádí na základě odborného posouzení a doporučení projektového týmu. Postup při hodnocení v nástroji pro analýzu rizik je následující. U každého opatření se ptáme, zda je dokumentováno, kontrolována jeho účinnost. Pokud opatření není, zadáváme 4. Pokud opatření je, tak se dále ptáme, zda je účinné a zda nás před danou hrozbou ochrání. Pokud nás ochrání vždy, tak uvedeme 1, pokud ve většině případů, tak uvedeme 2, pokud jen někdy, tak uvedeme 3 a pokud vůbec, uvedeme 4. Katalog opatření uvádím v Příloze č. 3.

Pro účely zvládání rizik jsou navržena opatření, odůvodněná příslušným paragrafem § ZKB viz Příloha č. 5.

3.6.5 Plán zvládání rizik

V rámci Plánu zvládání rizik jsem stanovila k jednotlivým opatřením priority.

1. Opatření priority 1

Vytvoření DRP a BCP¹⁸ (O11 a O62). Jako největší riziko se na základě analýzy rizik ukázalo to, že nejsou vytvořeny DRP a BCP plány, který je nezbytným předpokladem k tomu, aby organizace byla schopna obnovit činnost systému a poskytovat své

.....

¹⁸ Business continuity plan

služby i poté, co došlo k havárii, živelní pohromě, nebo útoku. Z tohoto důvodu se jedná o prioritu č. 1 pro další zvládání rizik. Vytvořeným DRP a BCP dojde k významnému snížení rizika a to:

- formou naplánování činností pro případ, že dojde ke krizové situaci;
- pravidelným testováním DRP a BCP postupů, a tím ke školení pověřených zaměstnanců k činnostem s tím souvisejícím.

2. Opatření priority 2

Začít provádět bezpečnostní testy (O29). Zajistit provádění bezpečnostních testů v rámci celého životního cyklu, především pak při aktualizaci stávajícího řešení. Při pravidelném testování může dojít k odhalení případných zranitelností, jejich včasnému odstranění, a tím ke zvýšení bezpečnosti.

CSIRT (O07). Vytvoření bezpečnostního týmu na bázi CSIRT, který by zabezpečil postupy a procesy pro případ kybernetického ohrožení výrazně zvýší bezpečnost napříč informačním systémem. V rámci vytvoření týmu dojde k nastavení komunikace, která se projeví v rámci samotného kybernetického ohrožení.

Řešit DDoS protection (O39). Za pomoci nástroje a zapojení do projektu CLAUDIA zabezpečit IS FACILITY před útoky DDoS typu a zajistit dostupnost systému alespoň pro uživatele v ČR. Díky tomu dojde ke snížení dopadu těchto útoků na cílové uživatele.

Zavést monitoring (O25). Musí být pořizovány, uchovávány a pravidelně vyhodnocovány záznamy událostí formou logů zaznamenávající aktivity uživatelů, výjimky, selhání a událostí či incidentů. Lze řešit implementováním služby.

Zajistit přesun do jiné lokality (O63). Za účelem zvýšení bezpečnosti by mělo dojít k přemístění některých prvků IS, nacházejících se v zátopové oblasti, do jiné lokality, případně do datového centra.

Zajistit lepší řízení lidských zdrojů (O08). Pro snížení rizika na minimum je zapotřebí najmout více zaměstnanců, rozdělit pravomoci, vytvořit dokumentace pracovních postupů pro zvýšení efektivity práce a možnosti zástupu při nemoci, dovolené, ukončení pracovního poměru pracovníka atd.

Zajistit lepší řízení zdrojů ICT (O09). Zpracovat plán pro lepší řízení zdrojů ICT, především capacity planning a posléze jeho realizace. Na základě tohoto plánu dojde k lepšímu řízení zdrojů ICT, a tak ke snížení hodnoty zranitelností.

Zavést skenování zranitelností (O18). Za pomoci automatizovaného nástroje skenovat zranitelnosti nad IS FACILITY. Doporučujeme provádět tyto skeny v týdenních intervalech. Pravidelně tak dojde k vystavení výstupů o zranitelnostech.

3. Opatření priority 3

Nasazení antimalware řešení (033). Zvážit nasazení AV řešení na serverech, případně zdůvodnit, proč toto řešení není možné nebo nedává smysl.

Zavedení bezpečnějších pravidel autentizace (03). Je nutné zvýšit úroveň autentizace. K naplnění požadavků dojde k 1.8.2018 při plánovaném upgradu IS FACILITY.

Zajistit bezpečné umístění síťových prvků (055). Zajistit přemístění všech síťových prvků IS FACILITY tak, aby byly umístěny v zabezpečených místnostech, pro to určených. Například v serverovnách, anebo alespoň zajistit, že budou pod stálým kamerovým dohledem.

Provést configuration review (019). Provedení kontroly nastavení a konfigurace systémů IS proti bezpečnostní politice (aktualizované) a zavedení pravidelných kontrol těchto systémů (kontrola dle VKB).

Zavést DLP (037). Zavést pro IS FACILITY systém Data Leakage Prevention, tak aby nedocházelo k nežádoucímu úniku informací.

Provést hardening (034). Provedením hardeningu nad systémy a koncovými stanicemi docílíme zvýšení bezpečnosti, a zároveň ochrany před narušením systémů a koncových stanic před ovlivněním/ovládnutím od útočníka.

Zavést IDS/IPS (035). Zavedení systému pro detekci a prevenci průniku a omezení šíření škodlivého kódu nám zajistí přehled nad nežádoucími událostmi v IS FACILITY.

Zajistit zlepšení kamerových systémů (048). Instalace kamerových systémů, za účelem plného pokrytí fyzického monitoringu nad prvky IS FACILITY.

Lanko (056). Zajistit možnost připnutí/upnutí mobilních zařízení (notebooků) při opuštění pracoviště, aby nemohlo dojít k jeho odcizení. Toto ustanovit i v bezpečnostní politice a zajistit dodržování.

Zajistit používání mechanických zábranných prostředků (045). Zajistit mechanické zábranné prostředky, aby nedocházelo k poškození nebo krádeži či ztrátě hmotných aktiv.

Zavést NAC (042). Zavést zvýšenou kontrolu přístupu do sítě, aby nebylo možné do sítě připojit necertifikované zařízení.

Zavést NBA (036). Zajistit monitoring/detekci anomálií nad IS FACILITY, aby došlo k včasnému odhalení probíhajícího útoku.

Dohlížet na omezení přístupu do internetu (05). Uživatelům by měl být poskytován přístup pouze k těm sítím a službám, jejichž užívání souvisí s pracovním

zařazením daného uživatele. Navrhujeme stanovit v bezpečnostní politice možnosti přístupu do internetu, a potenciálně nebezpečné internetové stránky centrálně blokovat pomocí řešení nabízejícího filtrování obsahu. Tuto činnost kontrolovat, a navíc evidovat jednotlivé přístupy v síti jednotlivých uživatelů.

Dohlížet na omezení přístupu na vyjímatelná média (O6). Uživatelům by měl být poskytován přístup k vyjímatelným médiím pouze pro pracovní účely, a měly by být v bezpečnostní politice striktně stanoven proces, kdy k nim může uživatel přistupovat. Stejně tak stanovit zákaz používání soukromých zařízení, a ty povolená firemní držet jen po nezbytně nutnou dobu, a po jejím uplynutí je uložit bezpečně do trezoru. Vyměnitelná média by měla být chráněna způsobem přiměřeným jeho obsahu.

Skartace médií a dokumentů (O14). Mělo by být zpracován skartační plán, který ustanoví, jakým způsobem a po jaké době nepotřebnosti dat a informací má dojít ke zničení a smazání médií a dokumentů. Vše musí být provedeno v souladu s příslušnými zákonnými normami a interními předpisy.

Zavést testování (O28). Vytvoření testů IS FACILITY, tyto testy provádět v pravidelných intervalech a jejich provedení evidovat.

Trezor (O57). Zajistit používání trezoru, který by sloužil k uložení hmotných aktiv. Především by tak došlo ke snížení zranitelnosti krádeži hmotného aktiva anebo použití aktiva v případě havarijního plánu.

Visačka (O49). Bezpečnostní politika by měla být upravena tak, aby každý zaměstnanec nosil viditelně svou visačku. Toto ustanovení by mělo být podloženo kontrolami a postihy, aby to dotýčný zaměstnanec opravdu dodržoval.

2 ISP (O51). Zajistit využívání 2 ISP (konektivita více poskytovateli internetové konektivity), zajistí se tím redundance pro připojení a navýšení dostupnosti IS FACILITY.

Vlastníci aktiv na základě navržených priorit nasazení jednotlivých opatření musí identifikované opatření vypořádat a akceptovat podle schváleného přístupu pro zvládání rizik, dle kapitoly 3.6.2. Způsob a formulář k akceptaci navrhovaných opatření je Přílohou č. 4 této práce.

3.6.6 Prohlášení o aplikovatelnosti

Účelem tohoto Prohlášení je vést přehled o aplikovaných opatřeních vycházejících z návrhů opatření ve VKB a o stanovení náležitostí v oblasti kybernetické bezpečnosti, a které slouží k minimalizaci rizik spojených se správou informačního systému, viz Příloha č. 7.

Prohlášení o aplikovatelnosti obsahuje:

- Přehled vybraných bezpečnostních opatření včetně zdůvodnění jejich výběru a jejich vazby na identifikovaná rizika.
- Přehled zavedených bezpečnostních opatření.
- Zdůvodnění proč jsou implementována/neimplementována, případně je uvedeno zdůvodnění, proč je potřebné je implementovat.
- Odkazy na dokumentaci, kde jsou jednotlivá opatření řešena.

Použitá metodika sestavení Prohlášení o aplikovatelnosti vychází z požadavků ZKB a VKB. Jednotlivá bezpečnostní opatření jsou výstupem procesu identifikace a hodnocení rizik, pro jejíž zpracování byly využity výsledky z rozdílové analýzy technických opatření implementovaných v rámci informačního systému. Výstupy z analýzy rizik jsou uvedeny v praktické části a v Přílohách č. 1 - 7.

4 Závěr

Cílem této práce bylo upozornit na význam řízení bezpečnostních rizik a ochrany informačních systémů. V práci uvádím pádné argumenty proč bezpečnost informací v organizacích neopomíjet a proč je důležité zavést potřebná opatření v rámci jednotlivých interních podnikových směrnic. V teoretické části jsem vymezila systém řízení bezpečnosti informací z hlediska mezinárodních standardů i české legislativy.

Provedla jsem rešerši autorů o tom, jak by se bezpečnostní rizika měla v organizacích řídit. Existuje mnoho kvalitních odborných článků i literatury, které se tomuto tématu věnuje. Zajímavý pohled mají zejména citovaní autoři, kteří problematiku posuzují na základě svých praktických zkušeností. Z tohoto důvodu jsem zvolila knihu, Řízení informačních rizik v praxi, primárním zdrojem. Uvědomuji si, že se mnohdy opírám právě jen o tento zdroj literatury, zejména pokud přecházím do kapitoly o procesu řízení rizik. Ne zvolila jsem špatně ani knihu od autorů Tony Merna, Faisal F. Al-thani, Risk management. Čerpala jsem z ní zejména pro orientaci v problematice řízení rizik a pomohla mi při stanovení metodiky pro praktickou část práce.

Elektronické zdroje, zejména normy a standardy mi pomohly k orientaci a mohla jsem tak vymezit systém řízení bezpečnosti informací. V rámci jedné z kapitol jsem provedla srovnání různých metod vhodných pro analýzu rizik a stanovila jsem metodiku pro analýzu rizik. Uvádím důvody proč kybernetickou bezpečnost ve společnostech neopomíjet a proč jsou zvolené konkrétní metody v praktické části.

Dalším stanoveným cílem práce bylo praktické vyřešení zadaného projektu analýzy rizik IS vybrané organizace. I přes omezení identifikace organizace jsou uvedené informace a získaná data postavena na skutečnosti.

Před zahájením procesu analýzy rizik jsem provedla rozdílovou analýzu, na základě které vznikl záznam o aktuálním stavu organizačních a technických opatření v rámci VKB. V procesu analýzy rizik jsem identifikovala aktiva, ohodnotila je a vytvořila základnu pro další fázi hodnocení rizik. Identifikovaná rizika jsem seřadila dle závažnosti, každému z rizik bylo přiděleno konkrétní číslo (ID). Na základě zjištění hodnot jednotlivých jsem navrhla opatření tak, aby došlo k minimalizaci nebo redukci identifikovaných rizik a byly naplněny požadavky ZKB a VKB. Vedení organizace bylo informováno o předpokladu, že identifikovaným rizikům je možno se vyhnout, pokud upustí od dané činnosti, která je s daným rizikem spjata, nebo změni podmínky provozu.

Výstupem provedené analýzy rizik je praktická část a jednotlivé Přílohy č. 1-7. V Plánu zvládání rizik jsou navržena opatření seřazená dle priorit k vyhodnoceným rizikům. Vlastníci aktiv v této fázi volí způsob zvládání navržených opatření včetně termínu. Rizika mohou být přenesena na jinou stranu, která může dané riziko účinněji zvládnout. Je potřeba si však uvědomit, že lze přenést odpovědnost za zvládnutí rizika, nikoli však odpovědnost za dopad. Dokumentem Prohlášení o aplikovatelnosti plním jeden z vytyčených cílů, realizovat analýzu rizik dle ZKB a VKB.

Potýkala jsem se s některými problémy. Například zpracování samotné analýzy bylo velmi pracné pro neexistenci poloautomatického nebo automatického nástroje. I přes dostupnost trial verzí některých nástrojů (např. u metody CRAMM), jsem zvolila pro výpočty tabulkový procesor MS Excel. Důvodem mého rozhodnutí byla obtížnost práce se software. Pro práci s nástroji pro analýzu rizik je třeba znalosti a zkušenosti. Nástroj MS Excel obsahuje mnoho matematických výpočtů a transformací a slouží i pro registr rizik. Je výtvorem třetí osoby a nemohu jej poskytnout k dispozici. Zejména z tohoto důvodu jsem připravila Přílohy v rozsahu v jakém jsou, aby byly výsledky dostačující pro zhodnocení výstupu mé práce.

Přínos práce shledávám v provedení literární rešerše koncepčních rámců v praxi. V aplikační části tkví přínos v použití vybrané metodiky. Realizace projektu byla vlastníkem projektu akceptována. Vzhledem k turbulentnímu prostředí a rychle se měnícím požadavkům se podmínky v rámci organizace mohou měnit. Tyto změny ovlivňují všechny faktory působící na výslednou míru rizika, a tím i na náklady. Přístupy pro zvládání rizik se tedy mohou v čase měnit a z těchto důvodů je nutné identifikovaná rizika dále monitorovat a pravidelně zkoumat. Projekt na analýzu rizik startuje ve společnosti proces řízení bezpečnosti informací. V oblasti bezpečnosti informací je třeba se neustále vzdělávat a reagovat na rychle měnící požadavky nejen legislativní ale i kybernetické útoky. Úspěch přeje připraveným a je třeba kontinuálně řídit rizika, provádět pravidelné kontroly a monitorovat změny.

Seznam literatury

- AMSP.CZ, 2017. *Asociace malých a středních podniků a živnostníků ČR / Výsledky vyhledávání gdpr* [online]. [cit. 3. 4. 2018]. Dostupné z: <http://amsp.cz/page/2/?s=gdpr>
- ANDERSON, J. Ross, 2008. *Security engineering : a guide to building dependable distributed systems*. 2. vydání. Indianapolis: Wiley Publishing. ISBN 978-0-470-06852-6.
- AVERIA, 2018. *ICT Network News* [online]. 2018. [cit. 18. 3. 2018]. Dostupné z: <http://ict-nn.com/cs/bezpecnost/4957-jak-v-souladu-s-gdpr-zajistit-povinnost-ohlaseni-incidentu-do-72-hodin-od-zjisti>
- BRENNER, Joel, 2007. *Iso 27001: Risk Management and Compliance. Risk Management; New York*. 1., roč. 54, č. 1, s. 24-26,28-29. ISSN 00355593.
- CZ.NIC, 2017. *Malá novela Zákona o kybernetické bezpečnosti - CSIRT* [online]. 2017. [cit. 18. 1. 2018]. Dostupné z: <https://www.csirt.cz/page/3581/mala-novela-zakona-o-kyberneticke-bezpecnosti/>
- ČERMÁK, Miroslav, 2009. *Řízení informačních rizik v praxi*. Brno: Tribun EU. ISBN 978-80-7399-731-1.
- DEMING.ORG, 2018. *The W. Edwards Deming Institute* [online]. 2018. [cit. 18. 4. 2018]. Dostupné z: <https://deming.org/deming/timeline>
- ENISA, 2018. *Inventory of Risk Management / Risk Assessment Methods — ENISA* [online]. 2018. [cit. 31. 3. 2018]. Dostupné z: <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods>
- FENZ, Stefan, Johannes HEURIX, Thomas NEUBAUER a Fabian PECHSTEIN, 2014. *Current challenges in information security risk management. Information Management & Computer Security; Bradford*. roč. 22, č. 5, s. 410–430. ISSN 09685227.
- GDPR BEZ OBAV, 2018. *GDPR bez obav. GDPR bez obav* [online]. 2018. [cit. 8. 4. 2018]. Dostupné z: <http://www.gdprbezobav.cz/>
- GDPR.CZ, 2018. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky. GDPR.cz* [online]. 2018. [cit. 18. 11. 2017]. Dostupné z: <https://www.gdpr.cz/>
- GOVCERT.CZ, 2018. *GovCERT.CZ* [online]. 2018. [cit. 18. 1. 2018]. Dostupné z: <https://www.govcert.cz/cs/vladni-cert/govcert-cz/>

IFMA.CZ, 2018. *IFMA - The Czech Republic Chapter of IFMA* [online]. 2018. [cit. 18. 3. 2018]. Dostupné z: <http://www.ifma.cz/index.php/facility-management/co-je-facility-management/166-facility-management>

IPMA.CZ, Řízení, 2013. *Doporučená praxe pro řízení rizik*. 2013.

ISO.ORG, 2017. *ISO/IEC 27001 Information security management* [online]. 2017. [cit. 18. 1. 2018]. Dostupné z: <https://www.iso.org/isoiec-27001-information-security.html>

ISO.ORG, 2018a. *ISO 31000:2018(en), Risk management — Guidelines* [online]. 2018. [cit. 31. 3. 2018]. Dostupné z: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>

ISO.ORG, 2018b. *ISO/IEC 27005:2011(en), Information technology — Security techniques — Information security risk management* [online]. 2018. [cit. 3. 4. 2018]. Dostupné z: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en>

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2013. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Praha: Policejní akademie ČR v Praze : Česká pobočka AFCEA. ISBN 978-80-7251-397-0.

MARTÍŠKOVÁ, Petra, Veronika HUMLEROVÁ a Antónia ŠTENSOVÁ, 2017. *Nový Způsob Ochrany Osobních Údajů V Podobě „Gdpr“ Očima Veřejnosti. Mladá Veda; Presov*. 11., roč. 5, č. 6, s. 1–11.

MERNA TONY a AL-THANI FAISAL F., 2007. *Risk management: řízení rizika ve firmě*. 1. vyd. Brno: Computer Press. ISBN 978-80-251-1547-3.

MVČR, 2018a. *Sbírka zákonů a Sbírka mezinárodních smluv - Ministerstvo vnitra České republiky* [online]. 2018. [cit. 18. 3. 2018]. Dostupné z: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=316/2014&typeLaw=zakon&what=Cislo zakona smlouvy>

MVČR, 2018b. *Sbírka zákonů a Sbírka mezinárodních smluv - Ministerstvo vnitra České republiky. Zákon 205/2017 Sb.* [online]. 2018. [cit. 18. 3. 2018]. Dostupné z: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=205/2017&typeLaw=zakon&what=Cislo zakona smlouvy>

NORMY.CZ, 2010. *Normy.cz / Výsledky hledání* [online]. 2010. [cit. 18. 1. 2018]. Dostupné z: <http://normy.cz/Vysledky.aspx>

NOVÁK, Luděk a Josef POŽÁR, 2011. Systém řízení informační bezpečnosti. In: *Pracovní příručka bezpečnostního manažera*. 1. vyd. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, s. 104. ISBN 978-80-7251-364-2.

SCHWALBE, Kathy, 2011. *Řízení projektů v IT*. Brno: Computer Press a.s. ISBN 978-80-251-2882-4.

SMITH, J. Nigel, 2008. *Engineering Project Management*. 3. vyd. Oxford: Wiley Publishing. ISBN 978-1-4051-6802-1.

TECHTARGET, 2018. What is data loss prevention (DLP)? - Definition from WhatIs.com. *WhatIs.com* [online]. 2018. [cit. 8. 4. 2018]. Dostupné z: <https://whatis.techtarget.com/definition/data-loss-prevention-DLP>

UOOU.CZ, 2018. *GDPR (Obecné nařízení): Úřad pro ochranu osobních údajů* [online]. 2018. [cit. 18. 1. 2018]. Dostupné z: <https://www.uoou.cz/gdpr%2Dobecne%2Dnbsp%2Dnarizeni/ds-3938/p1=3938>

ZOHO CORPORATION, 2013. *CAFM Software / Web-Based Facilities Management CAFM Software* [online]. 2013. [cit. 4. 4. 2018]. Dostupné z: <https://www.manageengine.com/products//facilities-desk/cfm-software.html>

Přílohy

Příloha č. 1 – Dotazník

Příloha č. 2 – Katalog rizik

Příloha č. 3 – Katalog opatření

Příloha č. 4 – Návrh zvládnání rizik

Příloha č. 5 – Návrh opatření

Příloha č. 6 – Vypořádání navrhovaného opatření

Příloha č. 7 – Prohlášení o aplikovatelnosti

Příloha č. 1 – Dotazník

Dotazník pro identifikaci a hodnocení aktiv					
Respondent (Titul, Jméno a Příjmení):					
Datum:					
Projektový manažer:					
Otázka č. 1:		Jaká aktiva považujete za kritická pro Vaši práci?			
Číslo	Aktivum	Nedůležitá	Důležitá	Velmi důležitá	Kritická
	Informace (Data)				
1					
2					
3					
	Procesy (Služby)				
	Aplikace				
	Hardware				
	Software				
	Zaměstnanci				
	Dodavatelé				
	Dokumentace				
	Jiné (specifikujte)				

Pozn.: č. 1 Pro každé aktivum bylo v dotazníku dostatečné množství řádků. Pro úsporu místa v diplomové práci jsem Dotazník upravila pro názornou představu, viz první aktivum Informace (data).

Pozn.: č. 2 Označte vždy důležitost uvedeného aktiva podle stupnice Nedůležitá – Důležitá – Velmi důležitá – Kritická. Otázku posuzuje respondent z pohledu svého samostatného oddělení a hodnotí, jak důležité jsou pro jejich činnost. Pro konkrétní aktivum uvádí jeho důležitost podle stupnice:

- **Kritická:** Bez tohoto aktiva se zcela zastaví hlavní činnosti samostatného oddělení či výstupy z nich nebudou validní, nebo nebudou k dispozici. Hrozí nebezpečí prodlžení
- **Velmi důležitá:** Bez tohoto aktiva se velmi omezí hlavní činnosti samostatného oddělení či výstupy z nich jsou omezeny. Hrozí nebezpečí prodlžení.
- **Důležitá:** Bez tohoto aktiva se omezí hlavní činnosti samostatného oddělení či výstupy z nich jsou omezeny.
- **Nedůležitá:** Bez tohoto aktiva není omezena hlavní činnost samostatného oddělení.

Příloha č. 2 – Katalog rizik

ID Rizika	Hrozba	Zranitelnosti	Opatření
R1	porušení bezpečnostní politiky	Nedostatečná bezpečnostní osvěta	Osvěta
R2		Nesynchronizovaný čas	synchronizace času
R3		Nedostatečný auditing	auditing
R4		Nedostatečný monitoring	monitoring
R5		Nedostatečné ochrana pomocí CCTV	kamerové systémy
R6	zneužití vnitřních prostředků	Nedostatečná bezpečnostní osvěta	Osvěta
R7		Nedostatečná identifikace	Identifikace
R8		Nedostatečná autentizace	Autentizace
R9		Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R10		Nedostatečné řízení přístupu do internetu	omezení přístupu do internetu
R11		Nedostatečné řízení přístupu na vyjímatelná média	omezení přístupu na vyjímatelná média
R12		Nesynchronizovaný čas	synchronizace času
R13		Nedostatečný auditing	auditing
R14		Nedostatečný monitoring	monitoring
R15		Nedostatečné ochrana pomocí CCTV	kamerové systémy
R16	zneužití identity fyzické osoby	Nedostatečná bezpečnostní osvěta	Osvěta
R17		Nedostatečná autentizace	Autentizace
R18		Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R19		Nesynchronizovaný čas	synchronizace času
R20		Nedostatečný auditing	auditing
R21		Nedostatečný monitoring	monitoring
R22		Nedostatečné systém kontroly fyzického přístupu	systémy pro kontrolu vstupu/přístupu
R23		Nedostatečné ochrana pomocí CCTV	kamerové systémy
R24		Nedostatečná identifikace zaměstnanců	visačka
R25		Nedostatečná kontrola vstupu osob	ostraha
R26	porušení licenčního ujednání	Nedostatečná kontrola licencí	kontrola licencí
R27	selhání technického vybavení	Nedostatečné řízení zdrojů ICT	Řízení zdrojů ICT
R28		Nedostatečný DRP	DRP
R29		Nedostatečné zabezpečená síťová architektura	redundance
R30		Nesynchronizovaný čas	synchronizace času
R31		Nedostatečný auditing	auditing
R32		Nedostatečný monitoring	monitoring
R33	selhání softwarového vybavení	Nedostatečné řízení zdrojů ICT	Řízení zdrojů ICT
R34		Nedostatečný DRP	DRP
R35		Nedostatečné zálohování a archivace	zálohování a archivace
R36		Nesynchronizovaný čas	synchronizace času
R37		Nedostatečný auditing	auditing
R38		Nedostatečný monitoring	monitoring
R39		Nedostatečné testování	rollback
R40		Nedostatečné testování	testování
R41	hacking	Nedostatky ve vývoji	SSDLC
R42		Nedostatečné postupy pro případ útoků a incidentů	CSIRT
R43		Nedostatečný DRP	DRP
R44		Nedostatečné řízení technických zranitelností	patchování
R45		Nedostatečné řízení technických zranitelností	skenování zranitelností
R46		Nesynchronizovaný čas	synchronizace času
R47		Nedostatečný auditing	auditing
R48		Nedostatečný monitoring	monitoring
R49		Nedostatečné testování	testování
R50		Nedostatečné testování	bezpečnostní testy
R51		Nedostatky ve vývoji	SSDLC
R52		Nedostatečná ochrana před škodlivým kódem	hardening
R54	DDoS	Nedostatečná kontrola připojení necertifikovaných zařízení	NAC
R55		Nedostatečné postupy pro případ útoků a incidentů	CSIRT
R56		Nedostatečné zabezpečená síťová architektura	DMZ
R57		Nedostatečný DRP	DRP
R58		Nedostatečný monitoring	monitoring
R59		Nedostatečná ochrana před škodlivým kódem	hardening
R60		Nedostatečná ochrana před zahlcením	DDoS protection
R61		Nedostatečný firewall	Firewall
R62		Nedostatečná ochrana před škodlivým kódem	WAF

ID Rizika	Hrozba	Zranitelnosti	Opatření
R63	škodlivý kód	Nedostatečná bezpečnostní osvěta	Osvěta
R64		Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R65		Nedostatečné řízení přístupu do internetu	omezení přístupu do internetu
R66		Nedostatečné řízení přístupu na výjimečná média	omezení přístupu na výjimečná média
R67		Nedostatečné postupy pro případ útoků a incidentů	CSIRT
R68		Nedostatečně zabezpečená síťová architektura	DMZ
R69		Nedostatečný DRP	DRP
R70		Nedostatečné zálohování a archivace	zálohování a archivace
R71		Nedostatečné řízení technických zranitelností	patchování
R72		Nedostatečné řízení technických zranitelností	skenování zranitelností
R73		Nedostatečná kontrola změn	configuration review
R74		Nesynchronizovaný čas	synchronizace času
R75		Nedostatečný auditing	auditing
R76		Nedostatečný monitoring	monitoring
R77		Nedostatečná ochrana před škodlivým kódem	antimalware řešení
R78		Nedostatečná ochrana před škodlivým kódem	hardening
R79		Nedostatečná ochrana před škodlivým kódem	IDS/IPS
R80		Nedostatečné opatření proti spuštění necertif. aplikací	Opatření proti spuštění necertif. aplikací
R82	přerušení dodávky elektřiny	Nedostatečný DRP	DRP
R83		Nedostatečný monitoring	monitoring
R84		Závislost na jednom zdroji el.	2 nezávislé příklady el. Energie
R85	přerušení konektivity do internetu	Závislost na jednom zdroji el.	alternativní zdroj napájení
R86		Nedostatečný DRP	DRP
R87		Nedostatečný monitoring	monitoring
R88		Závislost na jednom ISP	2 ISP
R89	selhání počítačové sítě	Jeden bod selhání	autorekonfigurace
R90		Nedostatečný DRP	DRP
R91		Nedostatečně zabezpečená síťová architektura	redundance
R92		Nedostatečný monitoring	monitoring
R93	poškození softwarového vybavení	Jeden bod selhání	autorekonfigurace
R94		Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R95		Nedostatečné řízení lidských zdrojů	Řízení lidských zdrojů
R96		Nedostatečný DRP	DRP
R97		Nedostatečné zálohování a archivace	zálohování a archivace
R98		Nesynchronizovaný čas	synchronizace času
R99		Nedostatečný auditing	auditing
R100		Nedostatečný monitoring	monitoring
R101	poškození technického vybavení	Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R102		Nedostatečné řízení lidských zdrojů	Řízení lidských zdrojů
R103		Nedostatečný DRP	DRP
R104		Nedostatečně zabezpečená síťová architektura	redundance
R105		Nedostatečný monitoring	monitoring
R106		Nedostatečné mechanické zábranné prostředky	mechanické zábranné prostředky
R107		Nedostatečné ochrana pomocí CCTV	kamerové systémy
R108		Nedostatečná kontrola vstupu osob	ostraha
R109	úmyslné smazání informací	Nechráněné síťové prvky	bezpečné umístění síťových prvků
R110		Nedostatečná identifikace	Identifikace
R111		Nedostatečná autentizace	Autentizace
R112		Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R113		Nedostatečné řízení lidských zdrojů	Řízení lidských zdrojů
R114		Nedostatečný DRP	DRP
R115		Nedostatečné zálohování a archivace	zálohování a archivace
R116		Nesynchronizovaný čas	synchronizace času
R117	úmyslné pozměnění informací	Nedostatečný auditing	auditing
R118		Nedostatečný monitoring	monitoring
R119		Nedostatečná identifikace	Identifikace
R120		Nedostatečná autentizace	Autentizace
R121		Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R122		Nedostatečné řízení lidských zdrojů	Řízení lidských zdrojů
R123		Nedostatečný DRP	DRP
R124		Nedostatečné zálohování a archivace	zálohování a archivace
R125		Nedostatečné zajištění integrity	kontrolní součty
R126		Nesynchronizovaný čas	synchronizace času
R127		Nedostatečný auditing	auditing
R128		Nedostatečný monitoring	monitoring
R129		Nedostatečné řízení změn	řízení změn

ID Rizika	Hrozba	Zranitelnosti	Opatření
R130	krádež informací	Nedostatečná identifikace	Identifikace
R131		Nedostatečná autentizace	Autentizace
R132		Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R133		Nedostatečné řízení přístupu do internetu	omezení přístupu do internetu
R134		Nedostatečné řízení přístupu na vyjímátná média	omezení přístupu na vyjímátná média
R135		Nedostatečné řízení lidských zdrojů	Řízení lidských zdrojů
R136		Nedostatečné šifrování dat v úložišti	šifrování dat v úložišti
R137		Nesynchronizovaný čas	synchronizace času
R138		Nedostatečný auditing	auditing
R139		Nedostatečný monitoring	monitoring
R140		Nedostatečná ochrana před únikem informací	DLP
R141	krádež hmotného aktiva	Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R142		Nedostatečné řízení lidských zdrojů	Řízení lidských zdrojů
R143		Nedostatečný DRP	DRP
R144		Nedostatečné zabezpečená síťová architektura	redundance
R145		Nedostatečný monitoring	monitoring
R146		Nedostatečné mechanické zábranné prostředky	mechanické zábranné prostředky
R147		Nedostatečné ochrana pomocí CCTV	kamerové systémy
R148		Nedostatečná ochrana přenosných zařízení před zcizením	lanko
R149		Nedostatečná ochrana přenosných médií a dokumentů	trezor
R150		Nedostatečná evidence majetku	evidence majetku
R151	narušení fyzické bezpečnosti	Nedostatečné nebo chybné řízení přístupu	striktní řízení přístupu
R152		Nedostatečný monitoring	monitoring
R153		Nedostatečné mechanické zábranné prostředky	mechanické zábranné prostředky
R154		Nedostatečná kontrola pohybu osob v chráněných prostorách	čidla detekující průnik
R155		Nedostatečné systém kontroly fyzického přístupu	systémy pro kontrolu vstupu/přístupu
R156		Nedostatečné ochrana pomocí CCTV	kamerové systémy
R157		Nedostatečná identifikace zaměstnanců	visačka
R158		Nedostatečná kontrola vstupu osob	ostraha
R159	požár	Nedostatečná bezpečnostní osvětla	Osvětla
R160		Nedostatečný DRP	DRP
R161		Nedostatečný monitoring	monitoring
R162		Nedostatečné prostředky pro detekci a omezení působení požáru	prostředky omezující působení požárů
R163		Nedostatečné ochrana pomocí CCTV	kamerové systémy
R164		Nedostatečné plány kontinuity	plán kontinuity činností
R165	záplava	Nedostatečný DRP	DRP
R166		Nedostatečný monitoring	monitoring
R167		Nedostatečná odolnost budovy	odolnost budovy
R168		Nedostatečné plány kontinuity	plán kontinuity činností
R169	zemětřesení	Nedostatečný DRP	DRP
R170		Nedostatečná odolnost budovy	odolnost budovy
R171		Nedostatečné plány kontinuity	plán kontinuity činností
R172	blesk/přepětí	Nedostatečný DRP	DRP
R173		Nedostatečný monitoring	monitoring
R174		Nestabilní el. síť	přepěťová ochrana
R175	demonstrace v okolí	Nedostatečná odolnost budovy	odolnost budovy
R176		Nedostatečné plány kontinuity	plán kontinuity činností
R177		Nevhodné umístění budovy	přesun do jiné lokality
R178	přerušování konektivity do internetu	Závislost na jednom ISP	2 ISP
R179	krádež hmotného aktiva	Nedostatečná ochrana přenosných zařízení před zcizením	lanko

Příloha č. 3 – Katalog opatření

ID opatření	Opatření	Zranitelnost	Poznámka	Paragraf
O1	Osvěta	Nedostatečná bezpečnostní osvěta	Proběhla osvěta jak se chovat na sociálních sítích, na internetu, jak pracovat s e-mailem, vyjímatelnými médii, mobilními zařízeními, a co je to (spear) phishing, vishing, watering holes, bezpečnostní incidenty a nestandardní stavy a komu je hlásit? Jsou k dispozici pracovní postupy nebo prezentace? Byly s nimi zaměstnanci seznámeni? Byli přezkoušeni? Nejsou materiály=4, jsou materiály=3, proběhlo seznámení=2, proběhlo přezkoušení=1 (Pouze pokud je možné to doložit.)	§ 9 Bezpečnost lidských zdrojů
O10	DMZ	Nedostatečně zabezpečená síťová architektura	Jsou jednotlivá aktiva, která spolu nemusí komunikovat od sebe oddělena? Na fyzické vrstvě=1, na linkové=2 na síťové=3, nejsou vůbec oddělena je tam IP konektivita=4	§ 17 Nástroj pro ochranu integrity komunikačních sítí
O11	DRP	Nedostatečný DRP	Je se selháním daného assetu počítáno v DRP? ANO=1, ANO, ale ne testováno=3, NE=4. V případě pohrom je zpracován a testován DRP, který umožní rozjet daný systém v jiné lokalitě? ANO=1, ANO, ale jen ve stejné lokalitě=2, nebyl netestován=3, NE není žádný plán=4	§ 14 Řízení kontinuity činnosti
O12	zálohování a archivace	Nedostatečné zálohování a archivace	Je dokumentováno, co se má zálohovat, jak, kdy, kde, kam, kým? Je popsáno, jak se má kontrolovat záloha? Zálohuje se, je záloha k dispozici, nachází se mimo hodnocené aktivum a ověřuje se použitelnost záloh? Jedná se nejen o zálohu dat, ale i programového vybavení. ANO=1, Záloha není mimo systém=2, NE, záloha se nekontroluje a test obnovy neprobíhá=3, záloha není vůbec=4	§ 10 Řízení provozu a komunikací
O13	redundance	Nedostatečně zabezpečená síťová architektura	Je daný asset provozován v režimu cluster, primary/secondary, aby v případě jeho selhání byl rychle obnoven provoz? ANO=1, na skladě=2, lze rychle dodat=3, NE=4	§ 26 Nástroj pro zajišťování úrovně dostupnosti
O14	Skartace médií a dokumentů	Nedostatečné postupy likvidace médií a dokumentů	Je popsán způsob skartace dat a postupuje se podle něj? Papír i média se šrotují na místě=1, probíhá svoz a likvidaci zajišťuje externí firma=2, neprobíhá vůbec=4	§ 16 Fyzická bezpečnost
O15	klimatizace	Nedostatečná klimatizace	Jaký typ chlazení klimatizace využívá? A jaká je závislost na médiu?	§ 16 Fyzická bezpečnost
O16	kontrola licencí	Nedostatečná kontrola licencí	Kontroluje se nějakým nástrojem, zda počet instalací odpovídá počtu licencí, a že se na hodnoceném aktivu nenachází nějaký nelicencovaný SW? Můžete doložit, kdy poslední kontrola proběhla? Je možné vidět onen výstup? ANO, automaticky a prohledávají se i seznamy nainstalovaných programů na daném zařízení=1, kontrola probíhá jen proti seznamu zakoupených licencí=2, NE neprobíhá žádná kontrola=4	
O17	patchování	Nedostatečné řízení technických zranitelností	Sleduje správce daného assetu, security bulletinů a ví, o zranitelnostech, vyhodnocuje je a stanovuje plán nasazení příslušného patche nebo workarroundu? ANO, patche nebo workarroundy jsou nasazovány téměř ihned=1, jsou nasazovány do několika dnů=2, do několika týdnů=3, jsou nasazovány až po několika měsících=4	
O18	skenování zranitelností	Nedostatečné řízení technických zranitelností	Probíhá pravidelný vulnerability sken assetů pomocí nějakého nástroje jako je Qualys? ANO, denně=1, týdně=2, měsíčně=3, jedenkrát ročně nebo vůbec=4	
O19	configuration review	Nedostatečná kontrola změn	Probíhá configuration review daného assetu za účelem ověření, že je nakonfigurován v souladu s bezpečnostní politikou a to pomocí nějakého automatického nástroje? denně=1, týdně=2, měsíčně=3, ročně=4	
O2	Identifikace	Nedostatečná identifikace	Každá osoba má přidělen jedinečný identifikátor, který nevyrazuje jeho účel a tento identifikátor není sdílen mezi více osobami. Nesdílí se a nevyrazuje účel=1, vyrazuje účel použití=2, sdílený identifikátor=4. V případě, že je používána visačka, je nosena viditelně a je na ní fotografie.	§ 11 Řízení přístupu a bezpečné chování uživatelů
O20	kontrolní součty	Nedostatečné zajištění integrity	Proti pozměnění a přehrání jsou informace chráněny pořadovým číslem + kontrolním součtem=4, Hashem=3, HMAC=2, el. podpisem=1	§ 25 Kryptografické prostředky
O21	šifrování dat v úložišti	Nedostatečné šifrování dat v úložišti	Jsou tam, kde je to vyžadováno, použity kryptografické prostředky v souladu s požadavky vyhlášky 316, příloha 3? Šifrují se data v úložišti, tam kde je to vyžadováno? ANO=1, slabá šifra=2, prolomená šifra=3, NE=4	§ 25 Kryptografické prostředky
O22	šifrování při přenosu	Nedostatečné šifrování při přenosu	Jsou tam, kde je to vyžadováno použity kryptografické prostředky v souladu s požadavky vyhlášky 316, příloha 3? Šifrují se data při přenosu, tam kde je to vyžadováno? ANO=1, slabá šifra=2, prolomená šifra=3, NE=4	§ 25 Kryptografické prostředky
O23	synchronizace času	Nesynchronizovaný čas	Je u sledovaného aktiva zajištěna synchronizace času minimálně 1x za 24 hodin? ANO=1, NE=4	§ 21
O24	auditing	Nedostatečný auditing	Zaznamenává se, přihlášení, odhlášení, změna práv, činnosti adminů, neúspěšné činnosti uživatelů, zahájení a ukončení činnosti technických aktiv, varovná hlášení, přístupu k záznamům, změny přihlašovacích údajů, u transakčních systémů pak i stav a změna hodnot a tyto logy uchovává minimálně po dobu 3 měsíců. Neprobíhá=4, záznamy se ukládají na auditovaném systému=3, na jiný než sledovaný systém=2, do centrálního logu=1	§ 21 Nástroj pro zaznamenávání činností KII a VIS, jejich uživatelů a administrátorů
O25	monitoring	Nedostatečný monitoring	Probíhá monitoring, události z daného aktiva jsou zasílány do SIEM=1, nejsou zasílány do SIEM=4	§ 22 a § 23
O26	řízení změn	Nedostatečné řízení změn	Podléhá změna nějakému schválení nebo kontrole, probíhá verzování? ANO=1, změna je kontrolována v rámci workflow, NE=4	§ 12 Akvizice, vývoj a údržba

ID opatření	Opatření	Zranitelnost	Poznámka	Paragraf
027	rollback	Nedostatečné testování	probíhá testování na možnost vrácení se na předchozí verzi? ANO=1, výrobce možnost deklaruje=2, výrobce tuto možnost negarantuje, ale mělo by to být možné=3, není to možné=4	§ 12 Akvizice, vývoj a údržba
028	testování	Nedostatečné testování	Jsou prováděny testy assetů podle nějaké mezinárodně uznávané metodiky? Akceptační, stress, load, performance testy	§ 12 Akvizice, vývoj a údržba
029	Bezpečnostní testy	Nedostatečné testování	Probíhají penetrační testy, bezpečnostní audity, audity zdrojového kódu	§ 24 Aplikační bezpečnost
03	Autentizace	Nedostatečná autentizace	Subjekt se autentizuje komplexním heslem, které splňuje 3 z následujících požadavků: obsahuje nejméně jedno velké písmeno, malé písmeno, číslici, nebo speciální znak. Maximální doba platnosti je 100 dnů. Je zamezeno opětovnému použití již dříve použitých hesel a nemumožňuje uživateli změnit heslo dříve než za 24 hodin od poslední změny. Minimální délka hesla: 8 znaků u uživatele, 15 znaků u admina. Případně se subjekt může autentizovat prostředkem, který zajišťuje minimálně stejnou úroveň bezpečnosti. Pokud není použito komplexní heslo nebo je délka menší jak 8 znaků, tak=4, při délce 8 znaků je zranitelnost=3, při délce 9 je zranitelnost=2 a při 10 a více je zranitelnost=1.	§ 18 Nástroj pro ověřování identity uživatelů
030	SSDLC	Nedostatky ve vývoji	probíhá vývoj podle nějaké SSDLC metodiky? (Tím by mělo být zajištěno, že systém neobsahuje známé chyby uvedené např. v OWASP top 10) ANO=1, NE=4	§ 12 Akvizice, vývoj a údržba
031	UX	Složitě uživatelské rozhraní	Respektují se požadavky na přístupnost a UX (Tím by mělo být zajištěno, že systém je uživatelsky přívětivý a odolný vůči chybám, vyžaduje potvrzení u kritických operací.) ANO=1, NE=4	§ 12 Akvizice, vývoj a údržba
032	bezpečná komunikace mezi systémy	Nedostatečné zabezpečení síťové architektura	Je komunikace mezi systémy navazována bezpečným způsobem? mutual SSL=1, heslo + TCP/IP wrapper=2, jen heslo=3	§ 17 Nástroj pro ochranu integrity komunikačních sítí
033	antimalware řešení	Nedostatečná ochrana před škodlivým kódem	Je na zařízení nainstalován nějaký antimalware, který reportuje do SIEM? Pokud tam není žádný AV, tak=4, pokud nějaký bez HIPS, tak=3, pokud obsahuje technologii HIPS=2 (1 není, protože AV obecně selhávají v prvních 48 hodinách)	§ 20 Nástroj pro ochranu před škodlivým kódem
034	hardening	Nedostatečná ochrana před škodlivým kódem	Byl proveden hardening systému podle best practice např. CIS nebo se asset nachází ve výchozí konfiguraci? Hardening byl proveden=1, účty přejmenovány, hesla změněna, služby zastaveny=2, jen hesla byla změněna=3, nachází se ve výchozí konfiguraci=4 (default password, weak protocols, common string, known accounts)	
035	IDS/IPS	Nedostatečná ochrana před škodlivým kódem	Jsou nasazeny IDS/IPS zařízení a jsou jeho signatury aktualizovány? ANO=1, nasazeno, ale neaktualizováno=3, NE není nic=4	§ 20 Nástroj pro ochranu před škodlivým kódem
035	IDS/IPS	Nedostatečná ochrana před škodlivým kódem	Jsou nasazeny IDS/IPS zařízení a jsou jeho signatury aktualizovány? ANO=1, nasazeno, ale neaktualizováno=3, NE není nic=4	§ 20 Nástroj pro ochranu před škodlivým kódem
036	NBA	Nedostatečná ochrana před škodlivým kódem	Je nasazeno nějaké NBA řešení, které detekuje anomálie na síti? ANO=1, NE=4	§ 20 Nástroj pro ochranu před škodlivým kódem
037	DLP	Nedostatečná ochrana před únikem informací	Bylo nasazeno nějaké DLP řešení? Host based+network based=1, host based=2, network based=3, NE=4	§ 24 Aplikační bezpečnost
038	Persistent workstation	Nedostatečná ochrana před škodlivým kódem	Je nasazeno nějaké řešení např. VDE, které zajišťuje, že se stanice vrací do své výchozí konfigurace a do roaming profilů neukládá spustitelné soubory, tj. je zajištěna persistence? Jeden den=1, týdnů=2 měsíčně=3, ročně=4	§ 20 Nástroj pro ochranu před škodlivým kódem
039	DDoS protection	Nedostatečná ochrana před zahlcením	Je nasazen nějaký systém proti DDoS útokům? Organizace je součástí projektu Fénix=1, DDoS protector je nasazen u ISP=2, DDoS protector je nasazen on premise=3, DDoS protector není=4	§ 26 Nástroj pro zajišťování úrovně dostupnosti
04	striktní řízení přístupu	Nedostatečné nebo chybné řízení přístupu	Přístup k objektu (datům, službám, assetům, prostorám) je řízen na principu need to know a least privilege, to znamená, že přístup k datům nebo službě je umožněn jen takovému subjektu (člověk nebo stroj) v rozsahu, který daný subjekt nezbytně nutně potřebuje k výkonu své funkce. Správce assetu vydefinoval seznam rolí a přidělil jim jen potřebná oprávnění. Veškeré přístupy jsou přidělovány/odebírány v případě nástupu, odchodu nebo změny prac. zařazení na základě požadavku nadřízeného pracovníka a existuje o tom záznam mimo zkoumaný systém. Toto opatření by mělo být implementováno u všech aktiv. jemnoznámé řízení přístupu=1, hruboznamé řízení přístupu např. jen R/W=2, žádné řízení přístupu=4	§ 19 Nástroj pro řízení přístupových oprávnění
040	Firewall	Nedostatečný firewall	Je nasazen firewall a jsou aktualizována pravidla? ANO=1, neaktualizována=3, NE=4	§ 17 Nástroj pro ochranu integrity komunikačních sítí
041	WAF	Nedostatečná ochrana před škodlivým kódem	Jedná se o legacy aplikaci, u které neproběhly penetrační testy nebo se ví, že obsahuje zranitelnosti, které nelze odstranit? Je nasazen Webový aplikační Firewall, který by aplikaci ochránil? ANO=1, NE=4	§ 20 Nástroj pro ochranu před škodlivým kódem
042	NAC	Nedostatečná kontrola připojení necertifikovaných zařízení	Bylo nasazeno nějaké opatření proti připojení necertifikovaných zařízení do vnitřní sítě 802.1x=1, MAC filtering=3, nic=4	§ 27 Bezpečnost průmyslových a řídicích systémů
043	Opatření proti spouštění necertifikovaných aplikací	Nedostatečné opatření proti spouštění necertifikovaných aplikací	Je použita technologie AppLocker a veškerý kód včetně maker musí být podepsán, jinak nejde spustit a nastaveno reportování do SIEM? ANO=1, ANO, ale nereportuje do SIEM=2, jen jedno z výše uvedeného=3, NE=4	
044	prostředky omezující působení požárů	Nedostatečné prostředky pro detekci a omezení působení požáru	Jsou nainstalovány a kontrolovány čidla detekující vznik požáru a funkční hasicí prostředky (ověřuje se jejich funkčnost) čidlo a sprinkler=1, hasicí přístroj=2, NE=4?	§ 16 Fyzická bezpečnost

ID opatření	Opatření	Zranitelnost	Poznámka	Paragraf
045	mechanické zábranné prostředky	Nedostatečné mechanické zábranné prostředky	Jsou chráněné prostory zabezpečeny mechanickými prostředky? Silné stěny, okna nad úroveň terénu, mříže, fólie na skle, zámky? ANO, vše ýše uvedené=1, NE nic z toho=4, něco tam je, ale ne moc účnné=2, spíš selže=3	§ 16 Fyzická bezpečnost
046	čidla detekující průnik	Nedostatečná kontrola pohybu osob v chráněných prostorách	Jsou nainstalovány systémy detekce pohybu např. PIR čidla, glass break sensory, otevření oken a dveří po pracovní době apod., a napojeny na PCO? ANO=1, NE=4	§ 16 Fyzická bezpečnost
047	systémy pro kontrolu vstupu/přístupu	Nedostatečné systém kontroly fyzického přístupu	Je použit nějaký systém pro kontrolu vstupu? Fingervein/palm/retina=1, PIN=2, karta=3, nic=4	§ 16 Fyzická bezpečnost
048	kamerové systémy	Nedostatečné ochrana pomocí CCTV	Je zkoumané aktivum chráněno pomocí kamerového systému, jsou záznamy ukládány, sleduje kamery někdo? NE nejsou kamery=4, Jen nahráváno=3, je nahráváno a sleduje to i ostraha na monitorech=1	§ 16 Fyzická bezpečnost
049	visačka	Nedostatečná identifikace zaměstnanců	Nosí zaměstnanci organizace visačky, aby bylo zřejmé, kdo je kdo? ANO=3, NE=4 (tato opatření nejsou v praxi moc účinná)	§ 16 Fyzická bezpečnost
05	omezení přístupu do internetu	Nedostatečné řízení přístupu do internetu	Je přístup do internetu nějak omezen? Žádná konektivita=1, content filtering=2, URL/IP filtering=3, no filtering=4	§ 19 Nástroj pro řízení přístupových oprávnění
050	ostraha	Nedostatečná kontrola vstupu osob	Provádí ostraha identifikaci osob na vstupu? Požaduje občanku a návštěvu si vyzvedává zaměstnanec=1, pouze kontrola občanky a pak volný pohyb po budově=2, žádná kontrola občanky=4	§ 16 Fyzická bezpečnost
051	2 ISP	Závislost na jednom ISP	Je konektivita do internetu zajištěna od 2 různých poskytovatelů? ANO a nebo není potřeba=1, NE=4	§ 26 Nástroj pro zajišťování úrovně dostupnosti
052	2 nezávislé přívody el. Energie	Závislost na jednom zdroji el.	Jsou k dispozici 2 přívody elektrické energie, každý z jedné strany budovy? ANO=1, NE=4	§ 16 Fyzická bezpečnost
053	alternativní zdroj napájení	Závislost na jednom zdroji el.	Je k dispozici alternativní zdroj napájení? UPS a dieselagregát=1, UPS=2, nic=4	§ 16 Fyzická bezpečnost
054	autorekonfigurace	Jeden bod selhání	Jsou zařízení nastavena tak, aby se sama rekonfigurovala a využila záložních tras? ANO=1, NE=4	§ 26 Nástroj pro zajišťování úrovně dostupnosti
055	bepečné umístění síťových prvků	Nechráněné síťové prvky	Jsou kabeláž a aktivní prvky umístěny tak, aby s nimi nemohlo být manipulováno a jsou pod dohledem kamer? ANO=1, nejsou snadno dosažitelné=3, NE=4	§ 16 Fyzická bezpečnost
056	lanko	Nedostatečná ochrana přenosných zařízení před zcizením	Jsou přenosná zařízení uzamykána při krátkodobém opuštění pracoviště? ANO=1, NE=4	§ 16 Fyzická bezpečnost
057	trezor	Nedostatečná ochrana přenosných médií a dokumentů	Jsou média, dokumenty a mobilní zařízení zavírána do trezoru při dlouhodobé nepřítomnosti? ANO=1, NE=4	§ 16 Fyzická bezpečnost
058	evidence majetku	Nedostatečná evidence majetku	Probíhá důsledná evidence majetku a je majetek vrácen v případě ukončení pracovního poměru? ANO=1, NE=4	§ 9 Bezpečnost lidských zdrojů
059	přepěťová ochrana	Nestabilní el. síť	Je nainstalována přepěťová ochrana? ANO=1, NE=4	§ 16 Fyzická bezpečnost
06	omezení přístupu na vyjímatelyná média	Nedostatečné řízení přístupu na vyjímatelyná média	Může uživatel připojovat vyjímatelyná zařízení? NE=1, je omezen zápis/čtení=2, bez omezení=4	§ 19 Nástroj pro řízení přístupových oprávnění
060	parkoviště mimo budovu	Nedostatečná ochrana podzemních prostor	Nachází se v budově podzemní parkoviště? ANO=4, NE=1	§ 16 Fyzická bezpečnost
061	odolnost budovy	Nedostatečná odolnost budovy	Byla budova projektována jako DC, tzn. Zdi, voda, klimatizace, elektroinstalace byla navržena a provedena dle best practice, byla instalována čidla? ANO=1, ne byly provedeny dodatečné úpravy=2, NE a nebyly provedeny žádné úpravy pro zvýšení odolnosti=4	
062	plán kontinuity činností	Nedostatečné plány kontinuity	Je vypracován a otestován business continuity plán, je možno pracovat i z jiné lokality ANO=1, NE=4	
063	přesun do jiné lokality	Nevhodné umístění budovy	nachází se v nejbližším okolí budovy jiná organizace, která by mohla být cílem útoku nebo zdrojem nebezpečí nebo problému? Vezměte i v úvahu, že by kolem budovy mohly probíhat demonstrace, oblast bude uzavřena a zaměstnanci nebudou mít možnost se dostat do práce. ANO=4, NE=1	
064	vlastnictví	Absence vlastnictví	Musí být stanoven garant aktiva a ten musí definovat pravidla a alokovat prostředky na správu a zabezpečení aktiv, protože bez toho může dojít k realizaci úmyslných hrozeb a nedbalosti při správě a následně pak k poškození, zničení, krádeži aktiv, která nebudou odpovídajícím způsobem chráněna.	§ 8 Řízení aktiv
065	auditovat	neefektivní řízení bezpečnosti informací	Zavedení tohoto opatření navrhuji hodnotit nikoliv u každého typového aktiva zvlášť ale u organizační jednotky jako celku neboť zásadním způsobem ovlivňuje úroveň bezpečnosti v organizaci.	§ 15 Kontrola a audit KII a VIS
066	Bezpečnostní dokumentace	Nedostatečná dokumentace		§ 28 Bezpečnostní dokumentace
067	Implementovat SRBI	neefektivní řízení bezpečnosti informací	Zavedení tohoto opatření navrhuji hodnotit nikoliv u každého typového aktiva zvlášť ale u organizační jednotky jako celku neboť zásadním způsobem ovlivňuje úroveň bezpečnosti v organizaci.	§ 3 Systém řízení bezpečnosti informací
068	Řídit rizika	Nevědomé přijetí neakceptovatelných rizik	Zavedení tohoto opatření navrhuji hodnotit nikoliv u každého typového aktiva zvlášť ale u organizační jednotky jako celku, neboť zásadním způsobem ovlivňuje vnímání rizik v organizaci.	§ 4 Řízení rizik

ID opatření	Opatření	Zranitelnost	Poznámka	Paragraf
069	Zavést bezpečnostní politiku	Absence pravidel	Zavedení tohoto opatření navrhuji hodnotit nikoliv u každého typového aktiva zvlášť ale u organizační jednotky jako celku neboť zásadním způsobem ovlivňuje implementaci dalších opatření.	§ 5 Bezpečnostní politika
07	CSIRT	Nedostatečné postupy pro případ útoků a incidentů	Jsou definovány postupy jak reagovat na jednotlivé typy incidentů, odpovídající proces byl implementován, tj. proběhlo školení a jednotlivé role v procesu byly obsazeny konkrétními lidmi a tito lidé byli vybaveni odpovídajícími pravomocemi a nástroji a funkčnost procesu byla ověřena=1, NE=4, funguje neformálně=3	§ 13 Zvládání kybernetických bezpečnostních událostí a incidentů
070	Ustanovit bezpečnostní role	Absence rolí	Zavedení tohoto opatření navrhuji hodnotit nikoliv u každého typového aktiva zvlášť ale u organizační jednotky jako celku neboť ovlivňuje efektivnost zavedení ŠŘBI.	§ 6 Organizační bezpečnost
071	Stanovit bezpečnostní požadavky	Slabina u dodavatele	Zavedení tohoto opatření navrhuji hodnotit nikoliv u každého typového aktiva zvlášť ale u organizační jednotky jako celku, ale dovedu si představit, že u každého aktiva bude položena otázka, kdo je dodavatel a zda je s ním smlouva a obashuje ty požadavky.	§ 7 Stanovení bezpečnostních požadavků pro dodavatele
08	Řízení lidských zdrojů	Nedostatečné řízení lidských zdrojů	Byly identifikovány kritické pozice, tj. takové pozice, kde je vyžadována speciální znalost, která se nedá na trhu snadno koupit. Je sledována nemocnost, zdravotní stav těchto osob, psychická a fyzická zátěž, vyhodnocují se incidenty, porušení zákoníku práce, vyhodnocuje se, zda zaměstnanec nevykonává soustavně se opakující rutinní činnost, je zpracován plán pro případ epidemie, neblíží se jeho odchod do důchodu, a je vypracován plán následnictví? Výběru, hodnocení, vzdělávání a uvolňování pracovníků je věnována odpovídající pozornost. ANO=1 (Pouze pokud je možné to doložit.), NE=4	§ 10 Řízení provozu a komunikací
09	Řízení zdrojů ICT	Nedostatečné řízení zdrojů ICT	Probíhá provozní monitoring, vyhodnocuje se trend v počtu incidentů daného typu, sleduje se životnost aktiva (končící záruka nebo podpora u OS) a plánuje se jeho obnova v rámci capacity planningu, a je takový plán k dispozici? Je věnována dostatečná pozornost výběru kvalitních HW a SW prostředků, kdy nerozhoduje jen cena? (Pouze pokud je možné to doložit.) ANO=1, rozhoduje především cena=3, NE=4	§ 10 Řízení provozu a komunikací

Příloha č. 4 – Návrh zvládání rizik

Návrh zvládání rizik		
ID rizika	Návrh zvládání rizika	Odůvodnění
R77	Antimalware řešení	§ 20 Nástroj pro ochranu před škodlivým kódem
R8, R17, R111, R120, R131	Autentizace	§ 18 Nástroj pro ověřování identity uživatelů
R109	Bezpečné umístění síťových prvků	§ 16 Fyzická bezpečnost
R50	Bezpečnostní testy	§ 24 Aplikační bezpečnost
R73	Configuration review	§ 27 Bezpečnost průmyslových a řídicích systémů
R42, R55, R67	CSIRT	§ 13 Zvládání kybernetických bezpečnostních událostí a incidentů
R60	DDoS protection	§ 26 Nástroj pro zajišťování úrovně dostupnosti
R140	DLP	§ 24 Aplikační bezpečnost
R28, R34, R43, R57, R69, R82, R86, R90, R96, R103, R114, R123, R143, R160, R165, R169, R172	DRP	§ 14 Řízení kontinuity činností
R5, R15, R23, R107, R147, R156, R163	Kamerové systémy	§ 16 Fyzická bezpečnost
R179	Lanko	§ 16 Fyzická bezpečnost
R106, R146, R153	Mechanické zábranné prostředky	§ 16 Fyzická bezpečnost
R4, R14, R21, R32, R38, R48, R58, R76, R83, R87, R92, R100, R105, R118, R128, R139, R145, R152, R161, R166, R173	Monitoring	§ 22 Nástroj pro detekci kybernetických bezpečnostních událostí § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
R10, R65, R133	Omezení přístupu do internetu	§ 19 Nástroj pro řízení přístupových oprávnění

Návrh zvládnání rizik		
R11, R66, R134	Omezení přístupu na vyjímatelná média	§ 19 Nástroj pro řízení přístupových oprávnění
R164, R168, R171, R176	plán kontinuity činností	§ 14 Řízení kontinuity činností
R177	přesun do jiné lokality	§ 16 Fyzická bezpečnost
R95, R102, R113, R122, R135, R142	Řízení lidských zdrojů	§ 10 Řízení provozu a komunikací
R136	šifrování dat v úložišti	§ 25 Kryptografické prostředky
R40, R49	testování	§ 12 Akvizice, vývoj a údržba
R149	trezor	§ 16 Fyzická bezpečnost
R24, R157	visačka	§ 16 Fyzická bezpečnost
R178	2 ISP	§ 26 Nástroj pro zajišťování úrovně dostupnosti
R2, R12, R19, R30, R36, R46, R74, R98, R116, R126, R137	synchronizace času	§ 21 Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

Příloha č. 5 – Návrh opatření

ID opatření	Popis návrhu	Důvod návrhu implementace	Návrh způsobu realizace
033	Nasazení antimalware řešení	§ 20 Nástroj pro ochranu před škodlivým kódem	Zvážit nasazení antiviru na serverech a případně zdůvodnit, proč SW na serveru nemůže být nasazen nebo nemá smysl
03	Zavedení vyšší úrovně bezpečnosti v pravidlech autentizace	§ 18 Nástroj pro ověřování identity uživatelů	Dle informací zjištěných při identifikaci aktiv a následného ověření dojde k nasazení potřebných opatření do 2 měsíců.
055	Zajistit bezpečné umístění síťových prvků	§ 16 Fyzická bezpečnost	Ochránit síť na jejím perimetru, zajistit, že všechny prvky budou pod kamerovým systémem.
029	Začít provádět bezpečnostní testy	§ 24 Aplikační bezpečnost	Stanovit si pravidla a dobu realizace penetračních testů. Penetrační testy provádět např. 1x za rok a/nebo v případě větší změny.
019	Provést configuration review	§ 27 Bezpečnost průmyslových a řídicích systémů	Provedení kontroly nastavení a konfigurace systémů v bezpečnostní politice a zavedení pravidelných kontrol těchto systémů.
07	CSIRT	§ 13 Zvládání kybernetických bezpečnostních událostí a incidentů	Vytvoření bezpečnostního týmu na bázi CSIRT, který by zabezpečil postupy a procesy pro případ kybernetického ohrožení.
039	Začít řešit DDoS protection	§ 26 Nástroj pro zajišťování úrovně dostupnosti	Za pomoci nástroje IS FACILITY zabezpečit IS před útoky DDoS typu a zajistit dostupnost systému alespoň pro uživatele v ČR.
037	Zavést DLP	§ 24 Aplikační bezpečnost	Zajistit Data loss prevention nad IS tak, aby byla zajištěna důvěrnost dat na vyšší úrovni.
011	Vytvořit DRP	§ 14 Řízení kontinuity činností	Vytvořit DRP, pravidelně ho aktualizovat a testovat (1x ročně).
048	Zajistit zlepšení kamerových systémů	§ 16 Fyzická bezpečnost	Instalace kamerových systému, aby došlo k plnému pokrytí fyzického monitoringu nad prvky IS.
056	Lanko	§ 16 Fyzická bezpečnost	Zajistit možnost připnutí/upnutí mobilních zařízení (notebooků) při opuštění pracoviště, aby nemohlo dojít k jeho odcizení.
Návrh jednotlivých opatření			

Návrh jednotlivých opatření			
045	Zajistit používání mechanických zábranných prostředků	§ 16 Fyzická bezpečnost	Zajistit mechanické zábranné prostředky, aby nedocházelo k poškození/krádeži/ztrátě hmotných aktiv.
025	Zavést monitoring	§ 22 Nástroj pro detekci KBU. § 23 Nástroj pro sběr a vyhodnocení KBU.	Implementovat Bezpečnostní monitoring. Optimálně jako službu outsourcing.
05	Dohlížet na omezení přístupu do internetu	§ 19 Nástroj pro řízení přístupových oprávnění	Nastavit a kontrolovat práva uživatelů a administrátorů, evidovat přístupy
06	Dohlížet na omezení přístupu na vyjímatelná média	§ 19 Nástroj pro řízení přístupových oprávnění	Nastavit a kontrolovat práva určeným uživatelům a administrátorům
062	Vytvořit plán kontinuity činností	§ 14 Řízení kontinuity činností	Vytvořit plán kontinuity činností a udržovat jej aktuální a pravidelně jej testovat. (1x ročně)
063	Zajistit přesun do jiné lokality	§ 16 Fyzická bezpečnost	Zajištění přesunu do jiné lokality.
08	Zajistit lepší řízení lidských zdrojů	§ 10 Řízení provozu a komunikací	Najmutí více zaměstnanců, rozdělení pravomocí, dokumentace pracovních postupů pro zvýšení efektivity práce a možnosti zástupu při nemoci, dovolené, ukončení pracovního poměru pracovníka atd.
09	Zajistit lepší řízení zdrojů ICT	§ 10 Řízení provozu a komunikací	Zpracovat plán pro lepší řízení zdrojů ICT.
018	Zavést skenování zranitelností	§ 27 Bezpečnost průmyslových a řídicích systémů	Za pomoci automatizovaného nástroje skenovat zranitelnosti nad IS (1x týdně).
021	Zvýšit úroveň šifrování dat v úložišti	§ 25 Kryptografické prostředky	Dle informací získaných v průběhu Analýzy rizik, dojde k nasazení potřebných opatření do 2 měsíců.
028	Zavést testování	§ 12 Akvizice, vývoj a údržba	Pravidelné provádění testování IS.
057	Trezor	§ 16 Fyzická bezpečnost	Pořízení trezoru pro zabránění krádeži hmotného aktiva.
049	Visačka	§ 16 Fyzická bezpečnost	Navrhnout používání visačky všech osob pohybujících se po budově
051	2 ISP	§ 26 Nástroj pro zajišťování úrovně dostupnosti	Zajistit využívání 2 ISP (konektivita více operátory)
023	Zajistit synchronizaci času	§ 21 Nástroj pro zaznamenávání činností IS	Zajistit/nastavit pravidelnou synchronizaci času dle VKB.

Příloha č. 6 – Vypořádání navrhovaného opatření

ID opatření	Priorita nasazení opatření	Způsob vypořádání opatření	Garant	Termín provedení
011	1			
062	1			
029	2			
07	2			
039	2			
025	2			
063	2			
08	2			
09	2			
018	2			
033	3			
03	3			
055	3			
019	3			
037	3			
034	3			
035	3			
048	3			
056	3			
045	3			
042	3			
036	3			
05	3			
06	3			
014	3			
021	3			
028	3			
057	3			
049	3			

051	3			
023	3			
051	3			
023	3			

Příloha č. 7 – Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti Základem pro sestavení seznamu bezpečnostních opatření byla VKB, kde jsou opatření rozdělena na organizační a technická. Každá část, byla rozdělena do podoblastí dle jednotlivých paragrafů a odstavců VKB.	
§ 6 Organizační bezpečnost Cíl: Ustanovit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci Dokumentace: Směrnice ISMS	
§6, odst. 1 Organizace řízení bezpečnosti informací Bude zaveden systém pro řízení bezpečnosti informací	neaplikováno
§6, odst. 2 Určení bezpečnostních rolí Budou určeny bezpečnostní role pro zajištění vyšší bezpečnosti aktiv	neaplikováno
§6, odst. 7 Výbor pro řízení kybernetické bezpečnosti Bude zřízen výbor pro kybernetickou bezpečnost	částečně
§6, odst. 8 Vzdělávání rolí kybernetické bezpečnosti Bude zavedeno pravidelné školení	neaplikováno
§ 7 Stanovení bezpečnostních požadavků Cíl: Udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami. Dokumentace: Směrnice Řízení dodavatelů	
§7, odst. 1 Stanovení pravidel pro dodavatele Ve schvalovacím procesu	neaplikováno
§7, odst. 2 a) Hodnocení rizik před uzavřením smlouvy Ve schvalovacím procesu	neaplikováno
§7, odst. 2 b) SLA Ve schvalovacím procesu	neaplikováno
§7, odst. 2 c) Pravidelné hodnocení rizik Ve schvalovacím procesu	neaplikováno

§ 8 Řízení aktiv Cíl: Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně. Dokumentace: Klasifikace aktiv	
§ 8, odst. 1 a) Evidence aktiv	aplikováno
§ 8, odst. 3 a) Hodnocení aktiv	aplikováno
§ 8 odst. 1 b)	aplikováno
§ 8 odst. 3 b) Určení garantů aktiv	
§ 8 odst. 4 a) Rozlišování úrovní aktiv	aplikováno
§ 8 odst. 4 a) Stanovení pravidel pro manipulaci s aktivy	aplikováno
§ 8 odst. 4 a) Přípustné způsoby používání aktiv	aplikováno
§ 8 odst. 4 b) Stanovení pravidel ochrany aktiv	aplikováno
§ 8 odst. 4 c) Smazání nebo likvidace technických nosičů dat	aplikováno
§ 9 Bezpečnost lidských zdrojů Cíl: Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a pro jednotlivé role byli vybráni vhodní kandidáti. Dokumentace: Směrnice bezpečnosti lidských zdrojů	
§ 9 odst. 1a) Plán rozvoje bezpečnostního povědomí bude zavedeno	neaplikováno
§ 9 odst. 1b) Poučení osob v bezpečnostních rolích	aplikováno
§ 9 odst. 1c) Kontrola dodržování bezpečnostní politiky Doplnit kapitolu ve Směrnici	neaplikováno
§ 9 odst. 1d) Vrácení aktiv a odebrání přístupových práv	neaplikováno
§ 9 odst. 2 Záznamy o školení Budou uchovávány záznamy.	neaplikováno
§ 9 odst. 3 a) Pravidla pro určení do bezpečnostních rolí Budou stanovena pravidla.	neaplikováno
§ 9 odst. 3 b) Hodnocení účinnosti plánu rozvoje bezpečnostního povědomí	aplikováno
§ 9 odst. 3 c) Pravidla pro řešení porušení bezpečnostních pravidel	aplikováno
§ 9 odst. 3 d) Změna přístupových práv	aplikováno

§ 10 Řízení provozu a komunikací Cíl: Cílem řízení bezpečnosti provozu IS a KS KII a VIS je zajistit spolehlivý, stabilní a bezpečný provoz Dokumentace: Směrnice ISMS, část Řízení provozu a komunikací	
§10 odst. 1 Používání technických nástrojů	aplikováno
§10 odst. 2 Pravidla pro bezpečný provoz	aplikováno
§10 odst. 3 a) Práva a povinnosti osob za stávající bezpečnostní role, administrátorů a uživatelů	neaplikováno
§10 odst. 3 b) Postupy pro spuštění a ukončení chodu systému a ošetření chybových stavů	neaplikováno
§10 odst. 3 c) Postupy pro sledování kybernetických bezpečnostních událostí a ochranu záznamů	neaplikováno
§10 odst. 3 d) Spojení na kontaktní osoby	aplikováno
§10 odst. 3 e) Změnové postupy	aplikováno
§10 odst. 3 f) Řízení kapacit	aplikováno
§10 odst. 4 Zálohování	aplikováno
§10 odst. 5 a) Oddělení vývojového, testovacího a provozního prostředí	aplikováno
§10 odst. 5 b) Řešení reaktivních opatření vydaných NBÚ	neaplikováno
§10 odst. 6 a) Bezpečnost a integrita komunikačních sítí a bezpečnost komunikačních služeb	aplikováno
§10 odst. 6 b) Pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi	neaplikováno
§10 odst. 6 c) Pravidla pro výměnu a předávání informací	aplikováno
§10 odst. 6 d) Smlouvy pro výměnu a předávání informací	aplikováno
§ 11 Řízení přístupu a bezpečné chování uživatelů Cíl: Omezit přístup k informacím a vybavení pro zpracování informací Dokumentace: Směrnice ISMS, část Řízení přístupu	
§ 11 odst. 1 Jednoznačný identifikátor	aplikováno
§ 11 odst. 2 Ochrana přihlašovacích údajů	aplikováno
§ 11 odst. 3 a) Identifikátor aplikací	aplikováno

§ 11 odst. 3 b) Omezení přidělování administrátorských oprávnění	aplikováno
§ 11 odst. 3 c) Politika řízení přístupu vytvořit dokumentaci	neaplikováno
§ 11 odst. 3 d) Přezkoumání přístupových oprávnění	aplikováno
§ 11 odst. 3 f) Používání mobilních zařízení	aplikováno
§ 12 Akvizice, vývoj a údržba Cíl: Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů v jejich celém životním cyklu. To zahrnuje i požadavky na informační systémy, které poskytují služby ve veřejných sítích. Dokumentace: Směrnice ISMS, vytvořit část k tomuto paragrafu	
§ 12 odst. 1 Požadavky na změny IS	aplikováno
§ 12 odst. 2 a) Hodnocení rizik akvizice, vývoje a údržby IS Budou zavedena opatření.	neaplikováno
§ 12 odst. 2 b) Bezpečnost vývojového prostředí a testovacích dat Budou zavedena opatření	neaplikováno
§ 12 odst. 2 c) Bezpečnostní testování změn IS Po každé změně IS bude prováděno testování.	neaplikováno
§ 13 Zvládání kybernetických bezpečnostních událostí a incidentů Cíl: Okamžitá reakce na KBU a vedení záznamů o jejich výskytu a řešení Dokumentace: Směrnice ISMS, část Zvládání KBU a KBI	
a) Oznamování KBU	neaplikováno
b) Prostor pro vyhodnocení oznámených KBU	neaplikováno
c) Klasifikace KBI, přijímání opatření, hlášení, sběr podkladů	neaplikováno
d) Prošetření KBI	aplikováno
e) Dokumentace KBI	neaplikováno
§ 14 Řízení kontinuity činností Cíl: Kontinuita bezpečnosti informací musí být součástí systémů řízení kontinuity činností organizace Dokumentace: Směrnice ISMS, Strategie řízení kontinuity činností	

§14 odst. 1 a) Práva a povinnosti bezpečnostních rolí	neaplikováno
§14 odst. 1 b) Cíle řízení kontinuity činností	neaplikováno
§14 odst. 1 c) Strategie řízení kontinuity činností	neaplikováno
§14 odst. 2 a) Dopady kybernetických bezpečnostních incidentů	neaplikováno
§14 odst. 2 b) Testování plánů kontinuity	neaplikováno
§14 odst. 2 c) Opatření pro zvýšení odolnosti IS	neaplikováno
§14 odst. 2 d) Postupy pro provedení opatření vydaných NBÚ	neaplikováno
§ 15 Kontrola a audit kybernetické bezpečnosti Cíl: Zabezpečení kontroly a souladu opatření dle ZKB Dokumentace: Směrnice ISMS, část Provádění auditů	
§15 odst. 1 a) Soulad bezpečnostních opatření	neaplikováno
§15 odst. 1 b) Kontroly dodržování bezpečnostní politiky	neaplikováno
§15 odst. 2 Audit kybernetické bezpečnosti	neaplikováno
§15 odst. 3 Kontrola zranitelností technických prostředků	aplikováno
§ 16 Fyzická bezpečnost Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace. Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace. Dokumentace: Směrnice ISMS, část Bezpečnostní politika	
§16 odst. 1 a) Zamezení neoprávněnému vstupu Nasazeno s cílem chránit aktiva.	aplikováno
§16 odst. 1 b) Zamezení poškození a zásahům do vymezených prostor Nasazeno částečně s cílem chránit aktiva. Pro zvýšení bezpečnosti bude provedena revize a nasazení kamerových systémů pro plné pokrytí IS, bezpečné umístění prvků IS do příslušných místností, přesun prvků IS mimo záplavovou oblast, dodržování při pohybu v oblastech prvků IS nošení visaček pro snadnou identifikaci osob, manipulujících s technickými aktivy.	aplikováno
§16 odst. 1 c) Prevence	neaplikováno

Pro zvýšení bezpečnosti bude zavedeno chránění hmotná přenosná aktiva upínacími prvky, mechanickými zábrannými prostředky, při nečinnosti uložení do trezoru.	
§16 odst. 2 a) Ochrana objektů	aplikováno
§16 odst. 2 b) Ochrana perimetru	aplikováno
§17 - §23 Nástroje Cíl: Řízení nástrojů pro zvýšení celkové bezpečnosti, dle příslušných paragrafů. Dokumentace: Neuvedena	
§ 17 Nástroj pro ochranu integrity vnitřní komunikační sítě	aplikováno
§ 18 Nástroj pro ověřování identity Částečně. S cílem chránit aktiva a procesy IS bude zvýšena náročnost autentizačních prostředků pro uživatele a administrátory.	aplikováno
§ 19 Nástroj pro řízení přístupových oprávnění	
§ 20 Nástroj pro ochranu před škodlivým kódem Pro zdokonalení bezpečnosti bude nasazen antimalware řešení, zaveden detekci a prevenci průniku a omezení šíření škodlivého kódu a zaveden nástroj pro detekci anomálií	aplikováno
§ 21 Nástroj pro zaznamenávání činností	aplikováno
§ 22 Nástroj pro detekci KBU	neaplikováno
§ 23 Nástroj pro sběr a vyhodnocení KBU	neaplikováno
§ 24 Aplikační bezpečnost Cíl: Zabránit neoprávněnému poškození a zneužití aplikací a informací, testovat prostředí a zjistit slabá místa systému před spuštěním do provozu Dokumentace:	
§24 odst. 1 Provádění testů zranitelností Zavést opatření pravidelného provádění bezpečnostního testování	neaplikováno
§24 odst. 2 a) Trvalá ochrana aplikací Nasadit Data Leakage Prevention, jakožto ochrana před nežádoucím únikem dat.	neaplikováno
§24 odst. 2 b) Trvalá ochrana transakcí	neaplikováno

Nasadit Data Leakage Prevention, jakožto ochrana před nežádoucím únikem dat.	
§ 25 Kryptografické prostředky Cíl: Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a / nebo integrity informací. Dokumentace: neaplikováno	
§25 odst. 1 a) Stanovení úrovně ochrany Bude vyřešeno v rámci nového upgrade IS	neaplikováno
§25 odst. 1 a) Pravidla šifrování při přenosu dat a uložení dat na mobilních zařízeních a vyměnitelných nosičích dat. Bude vyřešeno v rámci nového upgrade IS	neaplikováno
§25 odst. 1 b) Prostředky pro ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti. Bude vyřešeno v rámci nového upgrade IS	neaplikováno
§25 odst. 2 a) Systém správy klíčů Bude vyřešeno v rámci nového upgrade IS	neaplikováno
§25 odst. 2 b) Algoritmy Bude vyřešeno v rámci nového upgrade IS	neaplikováno
§ 26 Nástroj pro zajišťování úrovně dostupnosti Cíl: Zajistit dostupnost vybavení pro zpracování informací	
§26 odst. 1 Nástroj pro zajišťování úrovně dostupnosti informací Nasazení ochrana DDoS protection a zajištění redundance internetového připojení pro zajištění bezpečnosti na aktivech.	neaplikováno
§26 odst. 2 a) Dostupnost pro splnění cílů řízení kontinuity činností Nasazení ochrana DDoS protection a zajištění redundance internetového připojení pro zajištění bezpečnosti na aktivech.	neaplikováno
§26 odst. 2 b) Odolnost vůči KBI	aplikováno
§26 odst. 2 c) Zálohování důležitých technických aktiv Zavedeno zálohování	aplikováno
§ 27 Bezpečnost průmyslových a řídicích systémů	

Cíl: Zajistit bezpečnost a ochranu aktiv, zabezpečit vhodný přístup k nim a nakládání s nimi	
a) Omezení fyzického přístupu	aplikováno
b) Omezení přístupu k sítím Pro další navýšení bude prováděna zvýšená kontrola přístupu do sítě, aby se zabránilo případným připojením necertifikovaných zařízení.	aplikováno
c) Ochrana technických aktiv Bude zavedeno provádění hardeningu a pravidelná automatizovaná kontrola nastavení nad technickými aktivy pro zajištění vyšší bezpečnosti aktiv.	neaplikováno
d) Obnovení chodu Bude zpracován DRP a BCP plán dle § 14, pro zajištění bezpečnosti aktiv.	aplikováno