Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra řízení

Diplomová práce

Proces řízení rizik ve zvoleném podniku

Bc. Dana Mokrá

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Dana Mokrá

Veřejná správa a regionální rozvoj – k. s. Hradec Králové

Název práce

Proces řízení rizik ve zvoleném podniku

Název anglicky

Risk Management in Selected Company

Cíle práce

Hlavním cílem diplomové práce je na základě analýzy popsat a zhodnotit systém řízení bezpečnosti informací ve zvoleném podniku a v případě zjištěných nedostatků navrhnout vhodná opatření.

Metodika

Práce se skládá ze dvou částí – teoretické a praktické. Teoretická část je zpracována na základě studia odborné literatury za účelem tvorby teoretických východisek práce. Praktická část je zpracována na základě výstupů z kvantitativního/kvalitativního výzkumu.

Harmonogram:

Syntéza výchozí znalostní báze: 11/2019 – 08/2020

Kvantitativní/kvalitativní výzkum: 09/2020 – 11/2020

Agregace poznatků: 12/2020 – 02/2021

Odevzdání práce na katedru: 03/2021

Doporučený rozsah práce

60-80 stran

Klíčová slova

integrovaný systém řízení, informační bezpečnost, systém řízení, informační bezpečnost, riziko, proces řízení rizik, identifikace rizik, analýza rizik, hodnocení rizik

---

Doporučené zdroje informací

BAUMRUK, J., CIKRT, M., HLÁVKOVÁ, J. et al. Analýza rizik při práci: Příručka pro zaměstnavatele. Praha: Fortuna, 2001. ISBN 80-7071-183-3.

DOUCEK, P. Řízení bezpečnosti informací. 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

MERNA, T. FAISAL, F. Risk management. Brno: Computer Press, 2007. ISBN 978-80-251-1547-3.

SCHOLLEOVÁ, M. Ekonomické a finanční řízení pro neekonomy. Praha: Grada Publishing, 2008. ISBN 978-80-247-2424-9.

SMEJKAL, V. RAIS, K. Řízení rizik ve firmách a jiných organizacích. Praha: Grada, 2013. ISBN 978-80-247-4644-9.

ŠKRLA, P., ŠKRLOVÁ, M. Řízení rizik ve zdravotnických zařízeních. Praha: Grada, 2008. ISBN 978-80-247-2616-8.

TICHÝ, M. Ovládání rizika: analýza a management. Praha: C.H. Beck, 2006. ISBN 80-717-9415-5.

VÁCHAL, J., VOCHOZKA, M. Podnikové řízení. Praha: Grada Publishing, 2013. ISBN 978-80-247-4642-5.

ZUZÁK, R., KÖNIGOVÁ, M. Krizové řízení podniku. Praha: Grada Publishing, 2009. ISBN 978-80-247-3156-8.

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

doc. Ing. Martina Fejfarová, Ph.D.

Garantující pracoviště

Katedra řízení

Elektronicky schváleno dne 15. 2. 2021

prof. Ing. Ivana Tichá, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 15. 2. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 29. 03. 2021

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Proces řízení rizik ve zvoleném podniku" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29.3. 2021 _____

Poděkování

Ráda bych touto cestou poděkovala své vedoucí práce doc. Ing. Martině Fejfarové, PhD. za její odbornou pomoc a rady při zpracování diplomové práce. Dále bych ráda poděkovala odpovědným zaměstnancům vybraného podniku, za poskytnutí podkladů pro zpracování praktické části práce. Velké poděkování patří mé rodině, která mě po celou dobu studia morálně podporovala.

Proces řízení rizik ve zvoleném podniku

Abstrakt

Diplomová práce se zabývá problematikou procesu řízení rizik bezpečnosti informací, práce je konkrétně zaměřena na podnik MHK s.r.o. Hlavním cílem diplomové práce je zhodnotit systém řízení bezpečnosti informací v rámci integrovaného systému řízení ve vybraném podniku MHK s.r.o. a v případě zjištěných nedostatků navrhnout vhodná opatření. Práce je členěna do dvou částí, teoretické a praktické. Teoretická část je zpracována na základě studia odborné literatury, ISO norem a standardů řízené rizik, která obsahuje především knižní zdroje s tématikou procesu řízení informatiky a bezpečnosti informací podniku. Praktická část je zaměřena na zhodnocení týkající se současného stavu integrovaného systému podniku a procesu řízení rizik bezpečnosti informací, včetně stanovení možných postupů jeho zlepšení. Vychází ze zpracované literatury popsané v teoretické části, dále z analýzy zpřístupněných interních dokumentů podniku, osobních rozhovorů s odpovědnými pracovníky, zejména interním auditorem podniku. Pro zpracování praktické části práce byly využity interní směrnice a materiály podniku, vlastní zkušenosti s řízením rizik a data získaná v rámci konzultací s interním auditorem v rámci auditu podniku. Ke zjištění a popisu výchozí situace v řízení rizik bylo využito interních materiálů, zejména příručky integrovaného systému podniku, směrnice systému řízení bezpečnosti informací a politiky integrovaného systému. V závěru práce je uvedeno zhodnocení a návrh doporučení vycházející z předchozí analýzy řízení rizik v podniku.

Klíčová slova: integrovaný systém řízení, informační bezpečnost, systém řízení informační bezpečnosti, riziko, proces řízení rizik, identifikace rizik, analýza rizik, hodnocení rizik.

Risk Management in Selected Company

Abstract

The diploma thesis deals with the issue of informaion security risk management, the thesis is focused specifically on the MHK Ltd company. The main goal of the diploma thesis is to evaluate the information security management system within the integrated management system in the selected company MHK Ltd and if the proposed appropriate measures are not sufficient. The thesis is divided into two parts, theoretical and practical. The theoretical part is based on the study of professional literature ISO norms and standards of risk management, which contains mainly book sources on the topic of the process IT management and infomation security of the company. The practical part is focused on the evaluation of the current state of the integrated company system and the process of the information security risk management, including the determination of possible procedures for its improvement. It is based on the processed literature described in the theoretical part, as well as on the analysis of accessible internal documents of the company, personal interviews with responsible employees, especially the internal auditor of the company. For the elaboration of the practical part of the thesis the company used internal guidelines and materials, own experience with risk management and data obtained and consultation with the internal auditor within the company´s audit. Internal material was used to identify and describe the initial situation in risk management, in particular the manual of the integrated company system, the guidelines of the information security management system and the policy of the integrated system. At the end of the thesis is the evaluation and proposal of recommendation based on the previous analysis of risk management in the company.

Keywords: integrated management system, information security, information security management system, risk, risk management process, risk identification, risk analysis, risk assessment.

Obsah

1 Úvod 11

2 Cíl práce a metodika 12

2.1 Cíl práce 12

2.2 Metodika 12

3 Teoretická východiska 15

3.1 Integrovaný systém řízení 15

3.2 Normy systému řízení bezpečnosti informací 16

3.2.1 Norma ČSN ISO/IEC 27001 17

3.3 Systém řízení bezpečnosti informací 19

3.3.1 Ustanovení ISMS 24

3.3.2 Zavádění a provoz ISMS 25

3.3.3 Monitorování a přezkoumání ISMS 26

3.3.4 Údržba a zlepšování ISMS 26

3.3.5 Přínosy zavedení ISMS 27

3.3.6 Problematika informační bezpečnosti 27

3.3.7 Hrozby informační bezpečnosti 28

3.4 Řízení rizik 29

3.4.1 Stanovení kontextu 31

3.4.2 Analýza rizik 31

3.4.3 Zvládání rizik 33

3.4.4 Vyhodnocení rizik 34

4 Vlastní práce 35

4.1 Charakteristika podniku 35

4.1.1 Politika integrovaného systému 37

4.1.2 Odpovědnost a plánování managementu 38

4.1.3 Dokumentace podniku 40

4.1.4 Právní soulad s předpisy a normami v podniku 43

4.1.5 Monitorování, měření procesů a zlepšování 44

4.2 Systém řízení bezpečnosti informací v podniku 47

4.2.1 Aplikovatelnost ČSN ISO 27001 v podniku 47

4.2.2 Pozice a role v rámci ISMS v podniku 47

4.2.3 Bezpečnostní politika podniku 48

4.2.4 Informace a komunikace v podniku 49

4.2.5 Plán kontinuity podniku 50

4.2.6 Evidence aktiv 52

4.2.7 Stupnice klasifikace informací 53

4.2.8 Stávající rizika/aspekty 54

4.2.9 Identifikace rizik 56
4.2.10 Identifikace rizik plynoucích z přístupu třetích stran 64
4.2.11 Hodnocení rizik 65
4.2.12 Přehodnocení rizik 65
4.2.13 Vyhodnocení rizik 66
4.2.14 Identifikace nových rizik informační bezpečnosti 66
4.2.15 Neustálé zlepšování 66

5 Zhodnocení výsledků a návrhy opatření 67
5.1 Zhodnocení výsledků 67
5.2 Navrhovaná opatření 68

6 Závěr 71

7 Seznam použitých zdrojů 73

8 Přílohy 76

Seznam obrázků

Obrázek 1 Systém řízení bezpečnosti informací 20
Obrázek 2 Komponenty IS 22
Obrázek 3 Hrozby informační bezpečnosti 29
Obrázek 4 Fáze procesu řízení rizik 30
Obrázek 5 Analýza rizik 32
Obrázek 6 Organizační schéma podniku MHK 36

Seznam tabulek

Tabulka 1 Časový harmonogram sběru dat 13
Tabulka 2 Základní normy ISMS 17
Tabulka 3 Stupnice pro hodnocení rizik 33
Tabulka 4 SWOT analýza pro strategické plánování 39
Tabulka 5 Role ISMS v podniku MHK 48
Tabulka 6 Kvalifikační stupně podniku 53
Tabulka 7 Dopad ztráty bezpečnosti aktiva na fungování podniku 55
Tabulka 8 Ocenění hrozby/zranitelnosti 55
Tabulka 9 Identifikovaná aktiva v podniku 56
Tabulka 10 Konkrétní případ informačního aktiva podniku MHK 57
Tabulka 11 Informační aktiva podniku s nejvyšší hodnotou rizika 58
Tabulka 12 SW aktiva a HW aktiva podniku s nejvyšší hodnotou rizika 60
Tabulka 13 Konkrétní případ fyzického aktiva podniku MHK 61
Tabulka 14 Fyzická aktiva podniku s nejvyšší hodnotou rizika 62
Tabulka 15 Konkrétní příklad aktiva lidských zdrojů podniku MHK 63
Tabulka 16 Aktiva lidských zdrojů podniku s nejvyšší hodnotou rizika 64
Tabulka 17 Maximální ohodnocená aktiva 65
Tabulka 18 Informační aktiva II

Tabulka 19 Softwarová aktiva X
Tabulka 20 Fyzická aktiva XI
Tabulka 21 Lidské zdroje XV
Tabulka 22 Ostatní aktiva XVIII
Tabulka 23 Přehled skupin aktiv podniku MHK XVII

Seznam použitých zkratek

IMS	Integrovaný systém řízení
ISMS	Systém managementu bezpečnosti informací
IS	Integrovaný systém
MIS	Manažer integrovaného systému
ICT	Informační a komunikační technologie
PV	Představitel vedení
EA	Environmentální aspekt
EMS	Systém environmentálního managementu
IA	Interní audit
BOZP	Bezpečnost a ochrana zdraví při práci
MŽP ČR	Ministerstvo životního prostředí České republiky

1 Úvod

Bezpečnost informací je v prostředí firem klíčovou problematikou, jelikož informace a informační systémy jsou kritickými aktivy každého podniku. Na tato ohrožení působí celá řada faktorů, z nichž některé jsou výsledkem pokroku lidstva a v rukách extrémistů a jedinců, se obracející proti němu, působí proti hodnotám a právům na život lidí.

Informační bezpečnost zahrnuje ochranu všech informací bez rozdílu nosiče po celý jejich životní cyklus. V současné době je spojována především s informacemi komunikovanými skrze informační technologie, které zpracovávají stále více a více informací s velkou hodnotou. Pokud hovoříme v souvislosti s informačními technologiemi o zpracovávání informací, pak tím rozumíme použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezentaci informací. Protože se mnohdy jedná o informace s nezanedbatelnou hodnotou, musí být velmi dobře chráněny. Velkým problémem zranitelnosti bezpečnosti informací v praxi bývá nedokonalost organizačních zázemí, to znamená dokumentování všech informačních toků a procedur, představované celou řadou směrnic a jiných písemných dokumentů.

Informační bezpečnost lze charakterizovat jako praktický obor, který vznikl za účelem ochrany informací, kterých fyzická či právnická osoba využívá při své činnosti. Jedná se o ochranu před narušením integrity, důvěrnosti či dostupnosti informace. Mezi tyto informace se řadí nejen provozní informace komunikované v interním prostředí, ale vše od obchodních a výrobních tajemství, přes informace o vývoji, budoucích patentech, informace o účetních záležitostech, personální informace až po informace sdílené a komunikované s různými externími subjekty. Téma bezpečnosti je stále více aktuálním a současně dokladuje, že je mu stále nevěnována adekvátní pozornost a je stále více ohrožována.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je zhodnotit systém řízení bezpečnosti informací v rámci integrovaného systému řízení ve vybraném podniku MHK s.r.o. (MHK) a v případě zjištěných nedostatků navrhnout vhodná opatření.

Dílčí cíle práce:

1. Zpracování literární rešerše týkající se integrovaného systému řízení, systému řízení bezpečnosti informací a řízení rizik.
2. Definování procesu systému řízení bezpečnosti informací a řízení rizik.
3. Charakteristika a popis sledovaného podniku.
4. Popis stávajícího systému řízení bezpečnosti informací podniku.
5. Zhodnocení systému řízení bezpečnosti informací a řízení rizik v podniku.
6. Návrh doporučení na základě vypracování praktické části diplomové práce.

2.2 Metodika

Diplomová práce je zaměřena na problematiku systému řízení bezpečnosti informací v rámci integrovaného systému řízení. Systém řízení bezpečnosti informací chrání informace podniku před ztrátou či zneužitím a je velmi důležitý pro zajištění činností podniku. Je to formalizovaný systém řízení, jehož cílem je eliminovat hrozby, které mohou způsobit ztrátu nebo poškození aktiv a tím následně způsobit ohrožení vlastníka aktiv.

V teoretické části diplomové práce je provedena a zpracována rešerše v sekundárních literárních zdrojích týkající se integrovaného systému řízení a systému řízení bezpečnosti informací. Na základě takto získaných informací je v první části zpracován základní přehled o integrovaném systému řízení. Dále je zde definován proces systému řízení bezpečnosti informací, jsou zde uvedeny hlavní znaky systému, včetně normy systému řízení bezpečnosti, která je klíčovým dokumentem systému norem zkoumané řady. Součástí celého systému je řízení rizik, které je představeno v další teoretické části diplomové práce. Ta je zpracována na základě studia odborné literatury a standardů řízené rizik, která obsahuje především knižní zdroje s tématikou procesu řízení informatiky a bezpečnosti informací podniku.

Praktická část je zpracována na základě výstupů z kvantitavního a kvalitativního výzkumu. Je zaměřena na zhodnocení týkající se současného stavu integrovaného systému podniku

a systému řízení bezpečnosti informací, včetně stanovení možných postupů jeho zlepšení. Vychází ze zpracované literatury popsané v teoretické části, dále ze zpřístupněných interních dokumentů podniku a osobních rozhovorů s interním auditorem podniku. Pro zpracování byly využity interní směrnice a materiály podniku, vlastní zkušenosti s řízením rizik a data získaná v rámci konzultací s interním auditorem v rámci auditu podniku.

Sběr dat

Praktická část diplomové práce byla zpracována na základě zkoumání a pozorování nynějšího chodu celého integrovaného systému sledovaného podniku. Podnik byl zkoumán při interních auditech podniku a osobních rozhovorech s manažerem integrovaného systému. Zároveň byl pozorován chod systému řízení bezpečnosti informací v podniku. První interní audit byl zaměřen na integrovaný systém podniku, druhý interní audit byl zaměřen na systém řízení bezpečnosti informací včetně rizik bezpečnosti informací. Prvotně bylo zjištěno, zda podnik splňuje základní znaky integrovaného systému a byla provedena analýza současného stavu systému. V rámci interního auditu byly manažerovi podniku položeny otázky týkající se současného stavu integrovaného systému podniku. Položené otázky, které byly použity při osobních rozhovorech s manažerem integrovaného systému jsou součástí diplomové práce v příloze 1. Získané informace jsou použity v praktické části diplomové práce. Nejdelší fází sběru dat bylo pozorování podniku, na které byl vyčleněn 1 měsíc. Kompletní přehled časového harmonogramu je uveden v tabulce 1.

Tabulka 1 Časový harmonogram sběru dat

Činnost	10/2020	11/ 2020	12/ 2020
1. interní audit			
2. interní audit			
Pozorování podniku			

Zdroj: Vlastní zpracování (2021)

K získání dalších relevantních dat potřebných k zjištění a popisu systému řízení bezpečnosti informací v podniku, bylo využito aktuálních interních materiálů. Zejména příručky integrovaného systému podniku, směrnice systému řízení bezpečnosti informací a politiky integrovaného systému podniku. Dalším krokem, který byl nezbytný pro analýzu systému, bylo seznámení se s vnitropodnikovými dokumenty zabývajícími se řízením rizik. Pro přehodnocení rizik byla využita směrnice k zajištění bezpečnosti informací s názvem Registr aktiv a rizik bezpečnosti informací podniku.

Zhodnocení systému řízení bezpečnosti informací v rámci integrovaného systému řízení bylo provedeno zejména ze získaných informací interního auditu podniku a z předložených interních dokumentů podniku. V závěru práce jsou na základě vyhodnocení systému řízení bezpečnosti informací navržena možná opatření pro zlepšení zjištěných nedostatků.

3 Teoretická východiska

3.1 Integrovaný systém řízení

Vlastní proces řízení není a nikdy nebyl jednoduchou činností. Spolu s narůstající složitostí vztahů v podniku se zvyšuje i nutnost chápat vlastní proces řízení s větší komplexností. Řízení dle Doucka, Nováka, Nedomové a Svaté (2) přestává být individuálním problémem jednotlivých manažerů a dostává stále více multidisciplinární a interdisciplinární charakter. V této situaci se v současném globálním světě, kde stále více narůstá potřeba systematického a systémového řízení všech procesů probíhajících v podniku, zrodila nová filosofie řízení – integrovaný systém řízení (IMS Integrated Management System), která představuje komplexní a průřezový pohled na problematiku řízení v podniku a pomáhá realizovat základní vazby mezi jednotlivými odbornými oblastmi řízení.

Definice IMS dle Ondráka, Sedláka a Mazálka (4) představuje integrovaný systém jako filozofii komplexního řízení podniku. Doucek, Novák, Nedomová a Svatá (2) představuje integrovaný systém řízení jako účinný nástroj pro moderního manažera. Oblasti obsažené v tomto v integrovaném systému patří mezi kritické z pohledu hodnocení konkurenceschopnosti podniku na trhu.

Integrovaný systém řízení je tedy jediný systém určený k řízení více operací podniku v souladu s více standardy, jako jsou normy pro kvalitu, ochranu životního prostředí a ochranu zdraví a bezpečnosti (6).

Základní znaky integrovaného systému řízení:

- integrovaný systém musí zastřešovat v podniku jeden vedoucí pracovník – koordinátor integrovaného systému řízení,
- politika podniku, přidělování a čerpání zdrojů je řízeno jednotlivě na všechny komponenty,
- organizační strukturu a rozdělení odpovědnosti respektují všechny komponenty integrovaného systému řízení,
- řízení podniku a plánování mechanismy jsou harmonizované, je vytvořena jednotná dokumentace,
- informační a podpůrný systém, včetně udržování, implementace právních předpisů v podniku, jsou harmonizované s hlavními procesy v podniku,

- školení, zvyšování kvalifikace a systémy odměňování a hodnocení jsou harmonizovány,
- systém měření a monitorování, včetně komunikace a podávání zpráv, je jednoduchý a jeho procesy pro všechny oblasti pevně stanovené,
- přezkoumávání celého integrovaného systému řízení i jeho každé komponenty, včetně plánování a realizování interních auditů, projednávání nesrovnalostí, řešení neshod, vyhodnocování zjištěných výsledků, je integrováno,
- návrhy a realizace nápravných a preventivních opatření jsou prováděna v jednotě u všech komponent integrovaného systému řízení (6).

Z výše uvedených znaků vyplývá, že integrovaný systém řízení je systém určený k řízení více operací podniku v souladu s více standardy, jako jsou normy pro kvalitu, ochranu životního prostředí a ochranu zdraví a bezpečnosti. V praxi představuje integrovaný systém řízení sloučení stávajících formálních systémů a zavedení specifických osvědčených postupů v celém podniku (6). Proces řízení podniku je tedy nutné vnímat jako řešení komplexního problému, v jehož rámci je nezbytné řídit nejen podnik jako celek, ale i každý její dílčí aspekt.

Dle Palečka a kol. (5) je většina systémů řízení vysoce kompatibilní a všechny vycházejí z Demingova původního cyklu „Plánuj – proveď – kontroluj – konej“. Za komponenty IMS jsou dle Doucka, Nováka, Nedomové a Svaté (2) v dnešní době považovány zejména systém řízení kvality, systém řízení vztahu k okolí, systém řízení bezpečnosti a ochrany zdraví při práci a systém řízení bezpečnosti informací. Systému řízení bezpečnosti informací (ISMS) se více věnuji v níže uvedených kapitolách.

3.2 Normy systému řízení bezpečnosti informací

Tato mezinárodní norma podává přehled systémů řízení bezpečnosti informací a termíny a definice běžně používané v řadě norem ISMS. Norma je použitelná pro všechny typy a velikosti podniku (například pro obchodní podniky, vládní úřady, neziskové organizace). Dle Nezmara (10) je tato norma rámcovou normou pro ochranu dat a bezpečnost dat.

Skupina norem ISO/IEC 27000 pro systém managementu bezpečnosti informací se skládá dle Ondráka, Sedláka a Mazálka (4) z několika základních mezinárodních norem, které poskytují návod k vypracování a uplatnění efektivního systému managementu, kritéria pro ověřování shody s požadavky a metody systému. Na tyto základní normy pak mohou navazovat další normy, které poskytují návod nebo doporučení na uplatnění specifických požadavků. Níže jsou uvedeny v tabulce 2 základní normy řady ČSN ISO/IEC 27000.

Tabulka 2 Základní normy ISMS

Označení normy	Název normy
ČSN ISO/IEC 27000	Systémy managementu bezpečnosti informací – Přehled a slovník
ČSN ISO/IEC 27001	Systémy řízení bezpečnosti informací – Požadavky
ČSN ISO/IEC 27002	Soubor postupů pro opatření bezpečnosti informací
ČSN ISO/IEC 27003	Směrnice pro implementaci systému řízení bezpečnosti informací
ČSN ISO/IEC 27004	Řízení bezpečnosti informací – Měření
ČSN ISO/IEC 27005	Řízení rizik bezpečnosti informací
ČSN ISO/IEC 27006	Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
ČSN ISO/IEC 27007	Směrnice pro audit systémů řízení bezpečnosti informací
ČSN ISO/IEC 27008	Směrnice pro auditory opatření bezpečnosti informací
ČSN ISO/IEC 27010	Řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi
ČSN ISO/IEC 27011	Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002
ČSN ISO/IEC 27014	Správa a řízení bezpečnosti informací

Zdroj: Vlastní zpracování dle Ondráka, Sedláka a Mazálka (4)

3.2.1 Norma ČSN ISO/IEC 27001

Norma ČSN ISO/IEC 27001 je klíčovým dokumentem systému norem zkoumané řady. Zavádí základní požadavky na řízení bezpečnosti informací, vůči nimž se podnik certifikuje. Účel, za kterým byla tato mezinárodní norma sestavena, je poskytnout podniku návod a být mu rádcem při ustanovení, zavádění, provozování, monitorování, udržování a zlepšení systému ISMS. Požadavky této mezinárodní normy jsou obecně použitelné a jsou aplikovatelné ve všech podnicích bez ohledu na jejich typ, velikost a povahu činnosti (7).

V hlavní části normy jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému managementu bezpečnosti informací. Jsou zde specifikovány požadavky na výběr a zavedení bezpečnostních opatření chránících informační aktiva (4).

Vyloučení jakýchkoliv požadavků specifikovaných v kapitolách 4 - 10 je nepřijatelné, pokud chce podnik dosáhnout shody s touto normou (7).

Norma 27001 je použitelná a aplikovaná pro všechny typy organizací bez ohledu na jejich velikost a povahu činností. Je aplikovatelná na organizace s procesním řízením, respektive je postavena na faktu, že organizace, která se rozhodla implementovat ISMS a to v jakémkoliv oddělení a rozsahu upustila od funkčního řízení a přešla na procesní řízení (7).
Norma poskytuje podporu pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací. Norma prosazuje přijetí procesního přístupu při realizaci ISMS a skládá se z níže uvedených odstavců.

Kontext podniku

Podnik musí určit externí a interní aspekt, který je významný pro její záměry a který ovlivňuje její schopnost dosáhnout zamýšleného výstupu systému řízení bezpečnosti informací podniku, zároveň musí stanovit rozsah systému a neustále ho zdokonalovat a zlepšovat (7).

Vůdčí role

Vrcholové vedení podniku musí s ohledem na systém řízení bezpečnosti informací demonstrovat vůdčí roli a závazek, musí stanovit politiku bezpečnosti informací a zajistit, že odpovědnosti a pravomoci pro role relativní bezpečnosti informací jsou přiřazeny a komunikovány (7).

Plánování

Při plánování systému řízení bezpečnosti informací musí podnik zvážit kontext podniku a určit rizika a příležitosti, na které se potřebuje zaměřit, podnik musí definovat a používat proces ošetření rizik a stanovit cíle relevantní jednotlivý funkcím a úrovním rizika (7).

Podpora

Podnik musí určit a zajistit zdroje potřebné pro ustanovení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací a musí zahrnovat dokumentované informace vyžadované systémem a musí být řízeny (7).

Provozování

Podnik musí plánovat, implementovat a řídit procesy potřebné ke splnění požadavků bezpečnosti informací, musí řídit plánované změny a přezkoumávat následky neúmyslných

změn přijímáním opatření ke snížení jakýchkoliv nepříznivých dopadů, pokud je to nezbytné (7).

Hodnocení výkonnosti

Podnik musí vyhodnocovat výkonnost a efektivnost systému řízení bezpečnosti informací a musí provádět v plánovaných intervalech interní audity k získání informací o tom, zda systém řízení vyhovuje. Výzkumy z hodnocení a přezkoumání vedením podniku musí zahrnout rozhodnutí vztahující se k příležitostem neustálého zlepšování a k jakýmkoliv potřebám pro změny v systému řízení (7).

Zlepšování

Podnik musí neustále zlepšovat vhodnost, přiměřenost a efektivnost systému řízení bezpečnosti informací (7).

3.3 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací je v normě ČSN ISO/IEC 27001 definován jako část systému řízení povinné osoby založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat (7).

ISMS dle Smejkala, Sokola a Kodla (8) lze charakterizovat jako formalizovaný systém řízení a správy informačních aktiv podniku, jehož cílem je eliminovat hrozby, které mohou způsobit ztrátu nebo poškození těchto aktiv a tím následně způsobit ohrožení vlastníka aktiv. Definice ISMS dle Ondráka, Sedláka a Mazálka (4) uvádí, že se jedná o řízení bezpečnosti informací se všemi atributy, které to obnáší a že je částí celkového systému řízení podniku.

Norma ČSN ISO/IEC 27001 nám říká, že podnik musí ustavit, implementovat, udržovat a neustále zlepšovat systém řízení bezpečnosti informací v souladu s požadavky této mezinárodní normy. Rozsah systému řízení bezpečnosti informací musí být dostupný jako dokumentovaná informace (7).

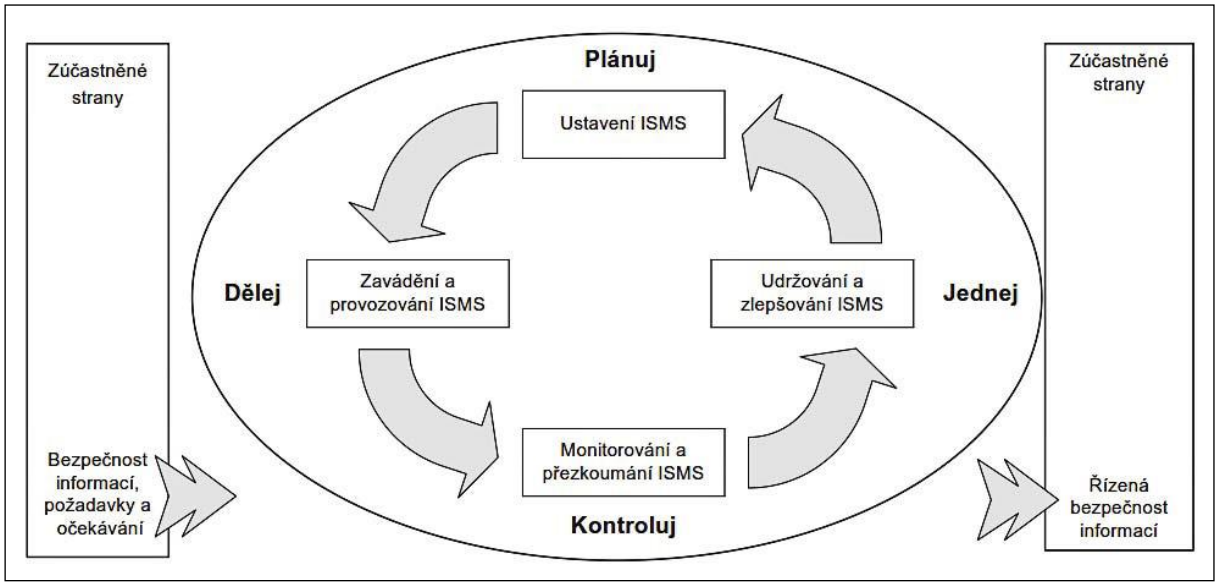
ISMS může být zaveden pro organizační složku instituce, informační systém nebo jeho část, případně může zahrnovat celý podnik. Řízení bezpečnosti informací a systém řízení bezpečnosti informací jsou v neustálé pozornosti všech manažerů, kteří během své práce přicházejí do styku s daty, zpracovávanými pomocí informačních a komunikačních technologií (16).

ISMS je systém, který nejen chrání informace podniku před ztrátou či zneužitím, ale chrání i členy vedení a zaměstnance před nechtěnými prohřešky vůči zákonům ČR. Bezpečnost informací je spojená s distribuovanou zodpovědností a je velmi důležitá pro zajištění činností každého podniku. Největším nebezpečím pro zabezpečení informací je člověk, který způsobí většinu bezpečnostních incidentů. Každý si musí být vědom toho, že se nedá bezpečnost informací zajistit stoprocentně, ale mělo by být provedeno vše, aby se bezpečnost zajistila na přijatelné úrovni za ekonomicky zdůvodnitelné náklady. A právě zde sehrává nezastupitelnou roli řízení rizik, které je nenahraditelným základem každého ISMS (16).

Z výše uvedeného vyplývá, že ISMS je systém, který chrání informace podniku před ztrátou či zneužitím a je velmi důležitý pro zajištění činností podniku. Na níže uvedeném obrázku 1 jsou uvedeny jednotlivé fáze. Dle Doucka, Nováka, Nedomové a Svaté (2) je systém řízení bezpečnosti složen ze čtyř fází celého životního cyklu systému řízení:

1. Ustanovení ISMS
2. Zavádění a provoz ISMS
3. Monitorování a přezkoumávání ISMS
4. Údržba a zlepšování ISMS

Obrázek 1 Systém řízení bezpečnosti informací



Zdroj: Vlastní zpracování dle Ondráka, Sedláka, Mazálka (4)

Fáze „Plánuj“ Plánování představuje základ budování systému řízení informační bezpečnosti. V této fázi je stanoven rozsah systému řízení bezpečnosti, definována bezpečnostní politika, navrženo řízení rizik včetně jejich vyhodnocení a jsou vybrána opatření pro snížení rizik. Fáze

„Dělej“ zahrnuje zavedení a využívání bezpečnostních opatření, procesů a postupů včetně monitorování jejich účinnosti. Její součástí je rovněž vytvoření plánu kontinuity a postupů reakce na bezpečnostní incidenty. Fáze „Kontroluj“ V této fázi je posouzena funkčnost a efektivita procesů a opatření. Jsou provedeny interní audity, přehodnocena rizika a je přezkoumán systém řízení bezpečnosti informací. Fáze „Jednej“ Na základě výsledků předchozí fáze jsou provedena nápravná a preventivní opatření (17).

Ondrák, Sedlák a Mazálek (4) doplňuje, že systém řízení bezpečnosti informací postihuje tyto základní okruhy:

- IT bezpečnost,
- Komunikační bezpečnost,
- Personální bezpečnost,
- Administrativní bezpečnost,
- Fyzická bezpečnost,
- Dokumentace, bezpečnostní funkce a mechanizmy.

Informační bezpečnost v podniku

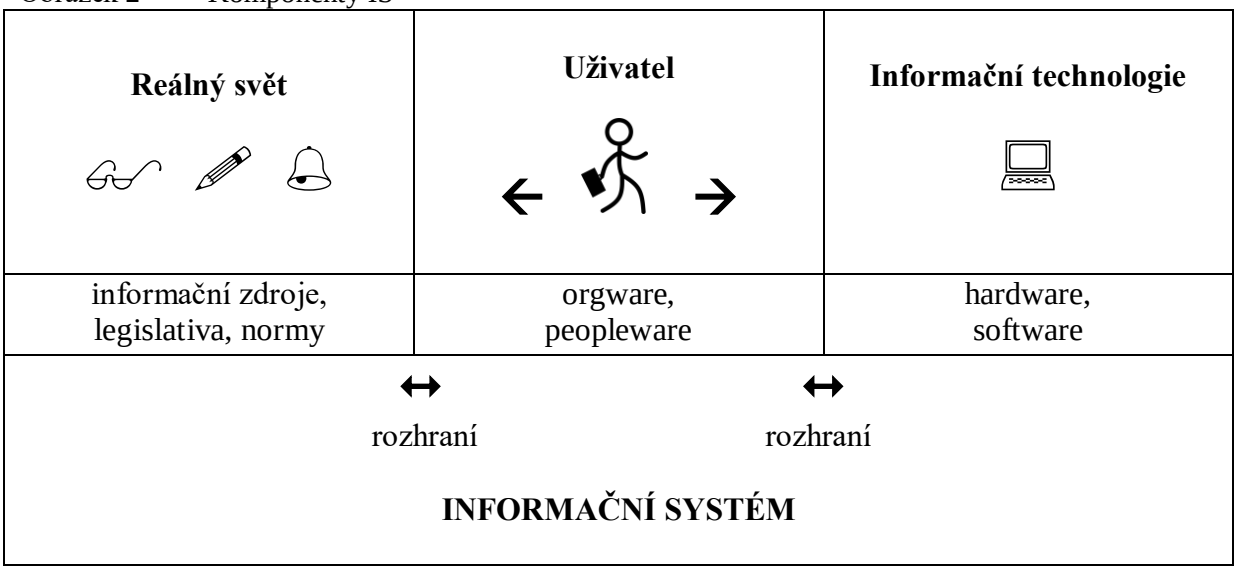
Kný a Požár (3) uvádí, že úkolem informační bezpečnosti je mimo jiné i zjištění, aby jiný subjekt nezískal citlivá data a informace, které by mu umožnily získat jakoukoliv konkurenční výhodu. Jde tedy o to, aby nedošlo k nechtěnému úniku významných a citlivých dat a aby nedošlo ke zničení či deformaci, změně dat či zhroucení, nebo dokonce zničení informačního systému. K tomuto všemu je třeba zavádět v podniku to, co se nazývá „řízení a řešení informační bezpečnosti“ s příslušným odborným personálním obsazením v podobě bezpečnostního managementu. Přístup k této problematice je v každém podniku jiný, specifický. Jsou však základní pravidla postupy a úrovně, které by měly být pro zajištění informační bezpečnosti naplněny.

Smejkal a Rais (1) doplňuje, že úroveň bezpečnosti se správně stanovuje a zabezpečuje „komplexně“, tedy v rovině administrativní, komunikační, fyzické a personální bezpečnosti.

Bezpečnost informačního systému je důležitou součástí jeho koncepce a vývoje. Je nezbytné nahlížet na bezpečnost IS komplexně a snažit se o zabezpečení IS daného podniku ve všech jeho částech a na všech jeho rozhraních. Otázka zajištění komplexní bezpečnosti informačních systémů bývá často podceňována, protože pokud nedojde v informačním

systému k žádnému bezpečnostnímu incidentu, nepřináší vložené investice žádné konkrétní výsledky. Z obrázku 2 vyplývá, že IS je tvořen nejen informačními komunikačními technologiemi, ale i jeho uživateli a okolním reálným světem, ve kterém funguje (9).

Obrázek 2 Komponenty IS



Zdroj: vlastní zpracování (2021)

Informační bezpečnost podniku se tedy dá charakterizovat jako koncepční, řídící, technologické, psychologické či právní. Dnešní manažeři jsou stavěni před úkoly, které s informační bezpečností souvisejí, a v řadě svých rozhodnutí jsou nuceni je i přímo do svých úvah zahrnovat. K tomuto dochází i přesto, že jim tato oblast přímo profesně nenáleží.

Dle Požára (23) znamená informační bezpečnost komplexní pohled, který organizaci pomáhá poznat a chránit svá cenná data a také vede praktickými opatřeními k eliminaci či výraznému snížení dopadů v případě mimořádných událostí. Informační bezpečnost znamená komplexní přístup k ochraně informací jako celku. Pro účinnou ochranu je třeba pochopit, jaká data a informace organizace má a jakou hodnotu pro ni mají. Je důležité uvědomit si cíle a reálné fungování organizace a teprve na základě toho lze navrhnout účinný a efektivní systém řízení informační bezpečnosti. Cílem však není pouhé zavedení, ale i další dlouhodobá funkčnost a rozvoj tohoto systému reagujícího na změny organizace i jejího okolí.

Řešení informační bezpečnosti

Informační bezpečnost dle Kného a Požára (3) znamená komplexní pohled, který podniku pomáhá poznat a chránit své cenné informace a také vede praktickými opatřeními k eliminaci či výraznému snížení dopadů v případě mimořádných událostí. Zavedením funkčního systému informační bezpečnosti je možné v podniku pomoci minimalizovat rizika spojená s únikem

informací. Systém řízení napomáhá snížení nákladů ICT a celkově přispívá k efektivitě procesů. Je výraznou oporou v rozhodovacích procesech na úrovni managementu ICT i na úrovni TOP managementu. Vyřešení informační bezpečnosti znamená rovněž pro podnik nemalý obchodní přínos. Nezřídka je v některých oborech zavedený systém řízení bezpečnosti přímo podmínkou pro vytváření nových obchodních vztahů.

Dle Požára (23) je zavedením funkčního systému řízení informační bezpečnosti možné v organizaci či podniku pomoci minimalizovat rizika spojená s únikem informací. Systém řízení napomáhá snížení nákladů na informační a komunikační technologie a celkově přispívá k efektivitě procesů. Je výraznou oporou v rozhodovacích procesech na úrovni managementu organizace. Účelem je zavádět systémy řízení, které přispívají ke zkvalitnění nejen interních služeb a procesů, ale i služeb či procesů určených klientům organizace či státní instituce. Vyřešení informační bezpečnosti znamená rovněž pro organizaci nemalý přínos. Nezřídka je v některých oborech zavedený systém řízení informační bezpečnosti přímo podmínkou pro vytváření nových obchodních či podnikatelských vztahů.

Ondrák, Sedlák a Mazálek (4) dodává, že cílem zavedení a provozu informační bezpečnosti je efektivní a systematické prosazení vybraných bezpečnostních opatření. Dle Požára (11) je rozhodnutí zabývat se informační bezpečností a vytvoření předpokladů jako podpora vedení, přidělení zdrojů a tvorba řešitelského týmu. Proces se skládá obvykle z 6 základních kroků:

1. Cíle a strategie řešení informační bezpečnosti.
2. Analýza rizik informačního systému.
3. Bezpečnostní politika podniku.
4. Bezpečnostní standardy.
5. Implementace informační bezpečnosti.
6. Monitoring a audit.

Fáze na sebe navazují, ale v řešení je běžné vrátit se k předchozímu kroku a zopakovat jej. Proces nekončí auditem, ale v určitých periodách se jím prochází znova, aby systém pružně reagoval na změny. Nalezené změny a řešení se formalizuje do vnitropodnikových dokumentů, zejména do bezpečnostní politiky, postupů a směrnic, určí se jejich závaznost a sankce za jejich porušení. Po implementaci zvolených opatření se stav průběžně monitoruje a periodicky ověřuje (11).

Hlavním důvodem implementace bezpečnosti podniku dle Kného a Požára (3) je:

- vzájemné prorůstání a ovlivňování ekonomik a dalších odvětví hospodářství prostřednictvím informačních a komunikačních technologií,
- digitalizace světa, kdy je neustále více dat předáváno v digitální formě, stále významnější a důležitější data z pohledu celého podniku jsou uložena v informačních systémech a v případě jejich výpadku by byla ohrožena akceschopnost infrastruktur,
- způsoby a techniky přenosu dat v sítích jsou všeobecně známé ve formách přenosových a komunikačních standardů, a proto data mohou být útočníky ohrožena.

Jelikož je problematika informační bezpečnosti disciplína, která se velice rychle rozvíjí, vznikají nové a nové programy jak v oblasti ochrany dat a informací, tak programy, které vytváří různí útočníci, jako např. hackeři, kriminální živly, teroristé a jiní. Proto je samotné zajištění a řízení bezpečnosti každého podniku jedním z průřezových profilů managementu podniku (3).

3.3.1 Ustanovení ISMS

Prvním cílem ustanovení ISMS je dle Doucka, Nováka, Nedomové a Svaté (2) upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření. Kromě definice rozsahu ISMS a odsouhlasení prohlášení o politice patří mezi kritické činnosti provedení analýzy rizik a výběr vhodných bezpečnostních opatření pro snížení vlivu existujících rizik. Tento proces prosazování by měl být ukončen souhlasem vedení se zavedením ISMS podle potřeb podniku, zjištěných při analýze a zvládání rizik ISMS.

Hlavním cílem ustanovení dle Kného a Požára (3) je provádět taková vhodná opatření, jejichž účelem je eliminovat dopad různých bezpečnostních hrozeb. S těmito hrozbami souvisí také zranitelnosti, které mohou mít negativní vliv na podnik. Tyto cíle se jsou uvedeny v úvodu projektu řešení informační bezpečnosti nebo v informační strategii.

Druhým cílem ustanovení ISMS je dle Doucka, Nováka, Nedomové a Svaté (2) definovat Prohlášení o politice, který vzniká na základě specifických potřeb daného podniku. Politika ISMS je rozsahem krátký, ale významem velmi důležitý dokument, protože prezentuje zájem vedení podniku o řízení bezpečnosti informací a definuje klíčové podmínky pro ohodnocení rizik, což je základem pro celý ISMS.

Při ustanovení ISMS podniku definuje rozsah a hranice ISMS na základě posouzení specifických rysů svých činností, svého uspořádání, struktury, umístění, aktiv a technologií, včetně důvodů pro vyjmutí z rozsahu ISMS. Z toho vyplývá, že ISMS se nutně nemusí

vztahovat na celý podnik. Zpravidla se tedy ISMS implementuje pro danou lokalitu/lokality a nebo pro daný informační systém.

Ondrák, Sedlák a Mazálek (4) také doplňuje nutnost získání souhlasu vedení podniku s nasazením a ustanovením systému. Norma tento souhlas požaduje a z hlediska praktického musí být zavádění ISMS prováděno směrem od vrchu dolů.

3.3.2 Zavádění a provoz ISMS

V rámci zavedení systému řízení informační bezpečnosti jsou zvolena vybraná opatření informační bezpečnosti do praxe. Opatření jsou popsána a jsou s nimi seznámeni všichni zaměstnanci podniku. Nedílnou součástí dle Kného a Požára (3) je vytvoření systému detekce a reakce na bezpečnostní incidenty, které mohou ohrozit důležitá a citlivá data.

Tato etapa životního cyklu se soustředí na prosazení všech bezpečnostních opatření tak, jak byla navržena v ustanovení ISMS. Důležité je především připravit dílčí plány, kde jsou upřesněny termíny a odpovědné osoby. Všechna bezpečnostní opatření by měla být zdokumentována dle Doucka, Nováka, Nedomové a Svaté (2) v příručce bezpečnosti informací a mělo by dojít k vysvětlení bezpečnostních principů všem uživatelům a manažerům.

Během této etapy zavádění ISMS je nezbytné provést následující činnosti:

- Formulovat dokument plán zvládání rizik a započít s jeho zaváděním.
- Zavést plánovaná bezpečnostní opatření a zformulovat příručku bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření v definovaných oblastech bezpečnosti informací (viz ISO/IEC 27002).
- Definovat program budování bezpečnostního povědomí a provést přípravu a zaškolení všech uživatelů, manažerů a odborných pracovníků z úseku informatiky a zejména z oblasti řízení bezpečnosti.
- Upřesnit způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele.
- Zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty.
- Řídit zdroje, dokumenty a záznamy ISMS (16).

Rámec ISMS je dán nejen velikostí, ale zejména počtem a kvalitou konkrétních procesů a aktivit podniku. To umožňuje stanovit další aspekty bezpečnostních požadavků jako právní,

regulační na dané provozní úrovni. Cílem tohoto kroku, jak uvádí Kný a Požár (3), je zavést, zdokumentovat a řídit vybraná bezpečnostní opatření a seznámit s nimi zaměstnance.

3.3.3 Monitorování a přezkoumání ISMS

Monitorování a přezkoumání ISMS je dle Ondráka, Sedláka a Mazálka (4) činnost prováděná k určení vhodnosti, přiměřenosti a efektivnosti předmětu přezkoumání k dosažení stanovených cílů. Pravidelná přezkoumávání účinnosti opatření s ohledem na výsledky bezpečnostních auditů, incidentů, výsledků měření účinnosti opatření, návrhů a podnětů všech zainteresovaných stran.

Hlavním úkolem této etapy je zajistit účinné zpětné vazby. V souvislosti s tímto požadavkem by proto mělo dojít k prověření všech aplikovaných bezpečnostních opatření a jejich důsledků na ISMS. Vlastní ověření začíná dle Doucka, Nováka, Nedomové a Svaté (2) u přímé kontroly odpovědných osob ze strany jejich nadřízených či bezpečnostním manažerem. Důležitou roli sehrává též nezávislé posouzení fungování a účinnosti ISMS pomocí interních auditů ISMS. Obecným cílem všech použitých zpětných vazeb je připravit dostatek podkladů o skutečném fungování ISMS, které budou předloženy vedení za účelem přezkoumání, zda je realizace ISMS v souladu s obecnými potřebami podniku.

Během této části zavádění ISMS je nezbytné provést následující činnosti:

- monitorovat a ověřit účinnost prosazení bezpečnostních opatření,
- provést interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS,
- připravit zprávu o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni vedení podniku, včetně revize zbytkových a akceptovaných rizik (16).

Podněty a připomínky k ISMS získané při jeho monitorování, jsou důležitými informacemi, které slouží pro objektivní a účinné přezkoumání ISMS vedením podniku. Přezkoumání by mělo probíhat pravidelně, a to nejméně jednou za rok. Není ale výjimkou, že probíhá častěji, a to hlavně u nově zavedených ISMS, kde je dle Doucka, Nováka, Nedomové a Svaté (2) potřeba přehodnocení častější.

3.3.4 Údržba a zlepšování ISMS

Cílem tohoto kroku je odstranit zjištěný nesoulad v ISMS, zavést efektivnější postupy a dále zlepšovat zavedený systém. V rámci tohoto kroku se dle Kného a Požára (3) provádí na základě provedených kontrol a auditů nápravné a preventivní činnosti v procesech informační

bezpečnosti a zavádějí se identifikované možnosti vylepšení systému řízení informační bezpečnosti.

Během této části zavádění je nezbytné dle Doucka, Nováka, Nedomové a Svaté (2) provést činnosti, které se skládají ze zavedením identifikované možnosti zlepšení ISMS a prováděním odpovídající opatření k nápravě a preventivní opatření pro odstranění nedostatků. Udržitelnost IS z hlediska bezpečnosti definuje Hanáček a Staudek (16) také jako výčet kritických činností a odpovídajících opatření pro akce typu registrace uživatele nebo instalace softwaru.

3.3.5 Přínosy zavedení ISMS

Zavedením systému řízení informační bezpečnosti může podniku pomoci řešit řadu problémů s bezpečností ICT. Je přímou cestou k dosažení úrovně bezpečnosti informačních technologií, ale také k účinnému a efektivnímu nakládání s informacemi v rámci celého podniku. ISMS představuje dokumentovaný systém řízení, který se stává nedílnou součástí všech procesů podniku. Stejně jako systémy managementu jakosti, systémy environmentálního managementu nebo systémy bezpečnosti a ochrany zdraví při práci i ISMS v sobě zahrnuje management, politiku, podnik a pravidelné přezkoumávání. Hlavním účelem zavedení ISMS je vytvoření systému, kde bude s minimálními náklady realizována optimální úroveň ochrany informačního systému a informací před možným narušením. Bezpečnost informačního systému je nutno řešit tak, aby rizika, kterým je denně vystaven, byla prostřednictvím vhodně nastavených procesů řízena. Rizika musíme identifikovat, stanovit jejich dopad, s ohledem na hodnotu příslušných aktiv, a definovat vhodná protiopatření. Taková řešení pak zajistí eliminaci významné části rizik ještě před jejich výskytem (3).

3.3.6 Problematika informační bezpečnosti

Dle Požára (23) je problematika informační bezpečnosti disciplína, která se velice rychle rozvíjí. Vznikají nové a nové programy jak v oblasti ochrany dat a informací tak programy, které vytváří různí útočníci jako např. hackeři, kriminální živly, teroristé aj. Samotné zajištění a řízení bezpečnosti organizace je jedním z průřezových profilů managementu organizace, či podniku. Všechny státní organizace i soukromé podniky musí budovat a neustále inovovat svou informační bezpečnost. Proto také nejvíce ohroženou oblastí úniku a ztrát dat a informací jsou jednak užívané informační a komunikační technologie a jednak lidské zdroje, tedy lidé, zaměstnanci organizace. Podle výzkumů problematiky informační bezpečnosti jsou právě lidí nejrizikovějším faktorem vyzrazení, kompromitace, modifikace, úniku a zničení citlivých dat a informací v organizaci. Informační bezpečnost má bezesporu zásadní význam

pro instituce, které ji prodávají jako součást své produkce. Softwarové, právnické, zpravodajské a konzultační podniky ji dokonce prodávají jako svou hlavní komoditu. Ovšem i jinde je bezpečnost informací kritickým znakem jakosti produkce. Závada v technické dokumentaci, společně s lidským selháním a technickou závadou, se řadí ke třem hlavním příčinám nežádoucích provozních událostí v jaderném průmyslu i v letectví.

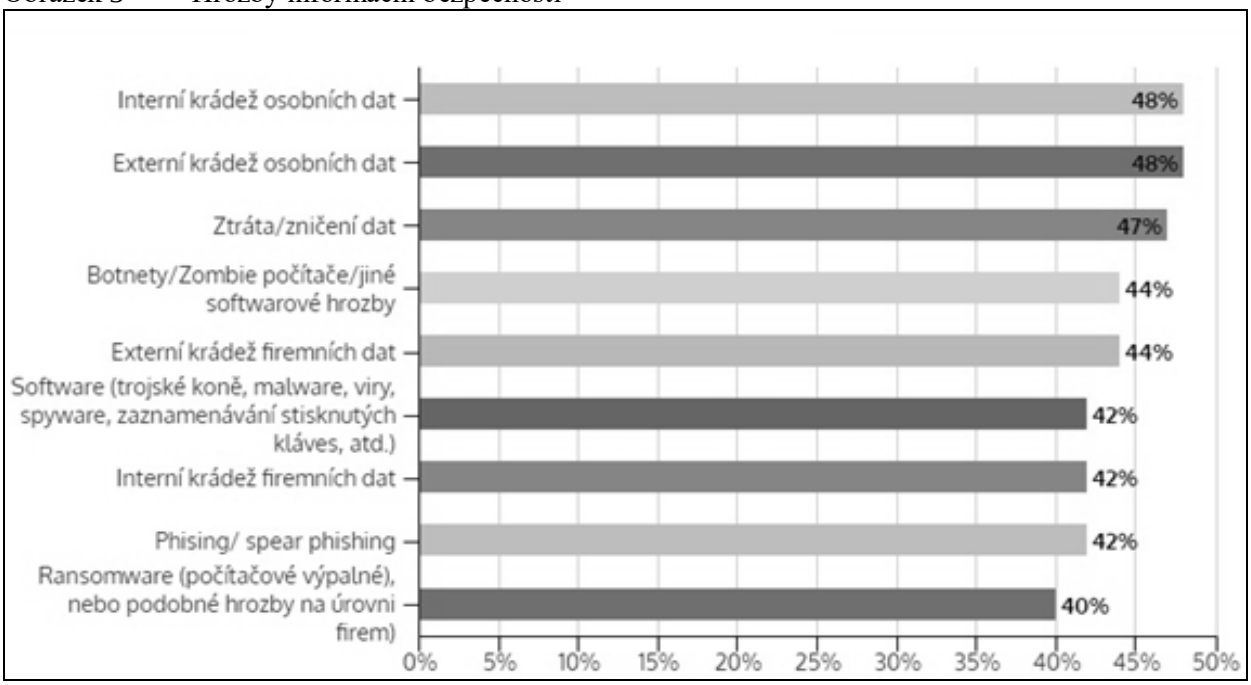
3.3.7 Hrozby informační bezpečnosti

Požár (23) uvádí, že hrozby využívají zranitelností, tj. chyb v programu nebo v jeho konfiguraci, která umožní útočníkovi získat neoprávněný přístup k datům. Část těchto chyb odhalí útočníci, kteří je neohlásí výrobcům software a ani je nezveřejní. Chyby pak využívají k útokům na inkriminovaný systém. Může se jednat jak o úmyslné využití (zneužití) nebo náhodné (například nehody, poruchy, živelné události). Hrozby se pro účely zkoumání bezpečnosti informačního systému ohodnocují. Jedná se subjektivní, relativní hodnocení, které bere v potaz četnost výskytu události u náhodných hrozeb a míru složitosti a motivace u úmyslných útoků.

Dle Geralda a Kovacicha (25) musíme pro ochranu našeho informačního systému implementovat agresivní bezpečnostní politiku. Jestliže podnik dostatečně nechrání svá informační aktiva, vystavuje se riziku ztráty trhu, zisku a obchodních příležitostí.

Níže uvedený obrázek 3 nám ukazuje nejčastější hrozby informační bezpečnosti. Stav vyplývá z provedeného průzkumu „Stav kybernetické bezpečnosti a digitální důvěry“, který byl proveden v roce 2019. Průzkumu se zúčastnilo více než 200 top manažerů na nejvyšší úrovni managementu napříč geografickými oblastmi a obory. V čele seznamu nejvážnějších hrozeb jsou krádeže firemních dat a napadení malwarem. Krádež nebo poškození dat vlastním zaměstnancem, případně pokus o ně, zažilo v posledních dvanácti měsících 69 % z oslovených respondentů. Nejčastější výskyt hlásí mediální a technologické podniky (77 %). Obavy odborníků stále narůstají – 2/3 z nich předpokládají, že je interní krádež firemních informací čeká v následujících 12-18 měsících. Průzkum také ukázal, že chybějící prostředky na najímání odborníků v oblasti kybernetické bezpečnosti a zaměstnanců s kvalitním vzděláním snižuje schopnost firem účinně se bránit před podobnými útoky (26).

Obrázek 3 Hrozby informační bezpečnosti



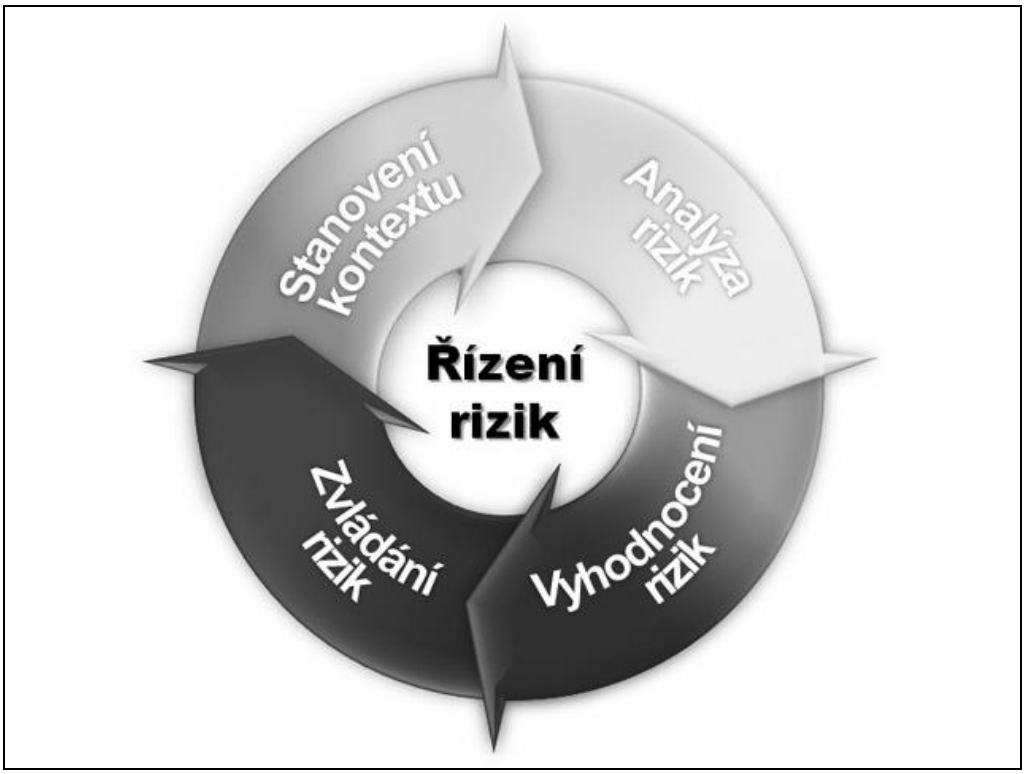
Zdroj: Vlastní zpracování dle Alexander Sophoclis Pieri (26)

3.4 Řízení rizik

Řízení rizik je integrální součástí každého řídícího procesu. Dle Smejkala, Sokola a Kodla (8) je řízení rizik proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích faktorů a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů, a naopak umožňují využít příležitosti působení pozitivních vlivů. Tvrdí, že součástí procesu řízení rizik je rozhodovací proces, vycházející z analýzy rizika. Po zvážení dalších faktorů, zejména ekonomických, technických, ale i sociálních a politických, management pro řízení vyvíjí, analyzuje a srovnává možná preventivní a regulační opatření.

Cílem řízení rizik dle Ondráka, Sedláka a Mazálka (4) je identifikace a kvalifikace rizik, kterým je třeba čelit a poté vhodným způsobem rozhodnout o zvládnutí těchto rizik. Snížení rizika je jedna z nejčastěji používaných metod. Řízení rizik je komplexní proces skládající se z několika na sebe navazujících fází a vytvářejících smyčku. Finálním výsledkem každé této etapy je rozhodnutí. Většinou je výstupem více variant řešení. Nepřijatelná úroveň rizika vyžaduje zastavení probíhajícího procesu a přijetí opatření na snížení rizika. Pro zbytková rizika, která nelze opatřeními efektivně snížit, se zpracovávají krizové plány. Níže na obrázku 4 jsou uvedeny fáze řízení rizik.

Obrázek 4 Fáze procesu řízení rizik



Zdroj: Čermák (20)

Riziko

Dle Smejkala, Sokola a Kodla (8) vyjadřuje riziko míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody. Velikost rizika je vyjádřena jeho úrovní. Riziko by nemělo být redukováno na pouhou pravděpodobnost, neboť zahrnuje jak samotnou pravděpodobnost, tak kvantitativní a kvalitativní rozsah dané události. Tomu odpovídá i vyhlášková definice, podle níž rozumíme možnost, že určitá možnost využije zranitelnosti aktiva a způsobí škodu. Úroveň rizika je určena hodnotou aktiva, resp. následkem pro jeho vlastníka či celý podnik, zranitelností aktiva a úrovní hrozby. Na růstu úrovně rizika se podílí úroveň hrozby, zranitelnost a hodnota aktiva. Provedení opatření úroveň rizika snižuje.

Požár (11) uvádí, že riziko (Risk) je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva.

Dle Smajkala a Raise (1), je riziko často chápáno jako nebezpečí vzniku určité ztráty. Finanční teorie obvykle definuje riziko jako kolísavost finanční veličiny okolo očekávané hodnoty v důsledku změn řady parametrů. Ukazuje také navazující filozofické kategorie, jakými jsou nutnost a nahodilost.

3.4.1 Stanovení kontextu

Jedná se o stanovení strategického a organizačního rámce spolu s vymezením oblastí, rizik, která mají být řízena. V této fázi jsou stanovena i kritéria, podle kterých budou rizika vyhodnocována. Stanovením kontextu se rozumí vymezení objektu, systému, u kterého se budou rizika posuzovat a o formulaci kritérií, ke kterým budeme riziko vztahovat (5).

3.4.2 Analýza rizik

Analýza rizik je dle Geralda (24) nejdůležitější etapou stanovení bezpečnostní politiky. V této fázi bude projektant pracovat s pojmy hrozba, bezpečnostní opatření, výše potencionálně způsobených škod a cena bezpečnostního opatření. Především ho bude zajímat, jaká jsou rizika plynoucí z jednotlivých hrozeb. Náplň analýzy rizik lze definovat jako proces porovnání odhadovaných rizik proti přínosu nebo ceně možných bezpečnostních opatření, stanovení implementační strategie v rámci vypracování systémové bezpečnostní politiky tak, aby byla v souladu s celkovou bezpečnostní politikou a s posláním podniku.

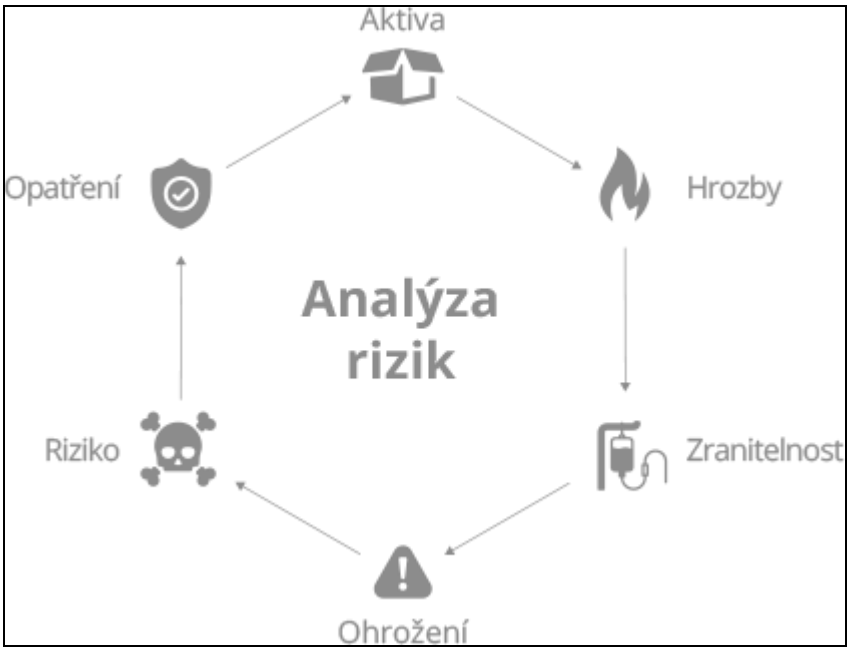
Dle Ondráka, Sedláka a Mazálka (4) je analýza rizik prováděna za účelem identifikace zranitelných míst informačního systému podniku. Zachycuje seznam hrozeb působících na IS a stanovuje rizika příslušná každému zranitelnému místu a hrozbě. Účelem takového dokumentu je snížení rizik na přijatelnou úroveň, respektive akceptaci zbytkových rizik tam, kde je jejich minimalizace neefektivní. Předpokladem úspěšné a účelné realizace analýzy rizik je přesné vymezení jejich hranic, a to z hlediska zahrnutých fyzických aktiv, aplikačních programových aktiv, datových aktiv a jejich umístění.

Analýza rizik dle Smejkala a Raise (13) je chápána jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti. Analýza rizik zpravidla zahrnuje:

1. Identifikace aktiv – vymezení posuzovaného subjektu a popis aktiv, které vlastní,
2. Stanovení hodnoty aktiv – určení hodnoty aktiv a jejich význam pro subjekt, ohodnocení možného dopadu jejich ztráty, změny či poškození,
3. Identifikace hrozeb a slabin – určení druhů událostí a akcí, které mohou ovlivnit negativně hodnotu aktiv
4. Stanovení závažnosti hrozeb a míry zranitelnosti – určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu vůči dané hrozbě.

Pod obrázkem 5, který nám popisuje analýzu rizik, jsou představeny pojmy a vysvětlení analýzy rizik

Obrázek 5 Analýza rizik



Zdroj: Vlastní zpracování (2021)

Dle Smejkala a Raise (13) je aktivum vše, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Aktiva se dělí na hmotná (např. nemovitosti, cenné papíry, peníze apod.) a nehmotná (např. informace, morálka pracovníků, kvalita personálu apod.).

Hrozba je dle Požára (11) skutečnost, událost, síla nebo osoby, jejichž působení může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost. Zranitelnost popisuje jako nedostatek nebo slabina bezpečnostního systému, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnoty aktiv.

Opatření dle Smejkala a Raise (13) je postup, proces, procedura nebo cokoliv co bylo speciálně navrženo pro zmírnění působení hrozby. Opatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.

Analýzu rizik lze chápat jako komplexní a hloubkovou analýzu současného stavu. Primárním cílem této činnosti je identifikace veškerých hardwarových, softwarových a informačních aktiv, jejich ohodnocení, výčet jejich zranitelností, výčet možných hrozeb, odhad pravděpodobnosti, že dojde k jejich naplnění, a návrh účinných a dostupných řešení

k jejich eliminaci. Jedná se o klíčový dokument pro procesy řízení bezpečnosti a řízení rizik (14).

Stupnice pro hodnocení rizik dle Ondráka, Sedláka a Mazálka (4) je uvedena v tabulce 3 na úrovních nízké – střední – vysoké a kritické.

Tabulka 3 Stupnice pro hodnocení rizik

Úroveň	**Popis**
Nízké	Riziko je považováno za akceptovatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Zdroj: Vlastní zpracování dle Ondráka, Sedláka a Mazálka (4)

3.4.3 Zvládání rizik

Fáze zvládání rizik spočívá ve volbě vhodné metody zvládání rizik. Mezi nejběžnější metody zvládání rizik patří akceptace a redukce rizika (12).

Akceptace rizika

Nejčastější metodou zvládání rizik, která spočívá v tom, že se nic nedělá, je akceptace rizika. Obecně lze tuto metodu doporučit pouze v případě nízkých a zbytkových rizik. Tento přístup má své opodstatnění, je zbytečné vynakládat prostředky na implementaci opatření proti hrozbě, která se prakticky nevyskytuje a její dopad je zanedbatelný (12).

Redukce rizika

Další nejběžnější metodou zvládání rizik je redukce rizika, jejím cílem je snížení rizika na přijatelnou úroveň. Tuto metodu lze doporučit pro všechna rizika, která se vyznačují vysokou pravděpodobností výskytu hrozby, bez ohledu na možný dopad (12).

Monitoring rizika

Rizika je vhodné monitorovat a přezkoumávat, a to nejen zbytková, za která mohou být prohlášena v podstatě jakákoliv rizika. Nepřetržitý monitoring je vhodný pro ta rizika, která se vyznačují vysokou pravděpodobností hrozby a velkým dopadem. Pravidelný monitoring je vhodný pro ta rizika, která se vyznačují nízkou pravděpodobností hrozby a malým dopadem. Pravidelné přezkoumání je vhodné pro ta rizika, která se vyznačují nízkou pravděpodobností

hrozby a velkým dopadem. Soustavné přezkoumávání je vhodné pro ta rizika, která se vyznačují vysokou pravděpodobností hrozby a velkým dopadem (12).

3.4.4 Vyhodnocení rizik

Výsledkem analýzy rizik je vyjádření a vyhodnocení velikosti rizika a jejich priorizace umožňující se dále zaměřit na rizika největší, nejzávažnější. Vlastní vyhodnocení rizik spočívá v posouzení respektive porovnání vyjádřené veličiny se stanovenými kritérii. Jestliže výsledné riziko je nižší než stanovená hodnota přijatelného rizika, není obvykle třeba další snižování rizika, ale tato rizika stále sledujeme, aby zůstala pod hranicí přijatelnosti. V případě, že hodnota rizika je nad nebo na hranici přijatelnosti, je nezbytné přijmout taková opatření, která by vedla ke snížení rizika pod mez přijatelnosti (5).

Kritéria vyhodnocení rizik dle Smejkala a Raise (8) používaná k rozhodování by měla být v souladu s definovaným vnějším a vnitřním kontextem řízení rizik bezpečnosti informací a měla by brát v úvahu cíle podniku a hlediska zainteresovaných stran atd. Rozhodnutí učiněná v rámci činnosti vyhodnocení rizik jsou založena zejména na akceptovatelné úrovni rizik. Avšak při identifikaci rizik a v analýze by měly být brány v úvahu rovněž následky, pravděpodobnost a stupeň důvěrnosti. Nahromadění většího množství nízkých nebo středních rizik může vyústit v daleko vyšší celková rizika a potřebu tuto situaci podle toho řešit.

4 Vlastní práce

4.1 Charakteristika podniku

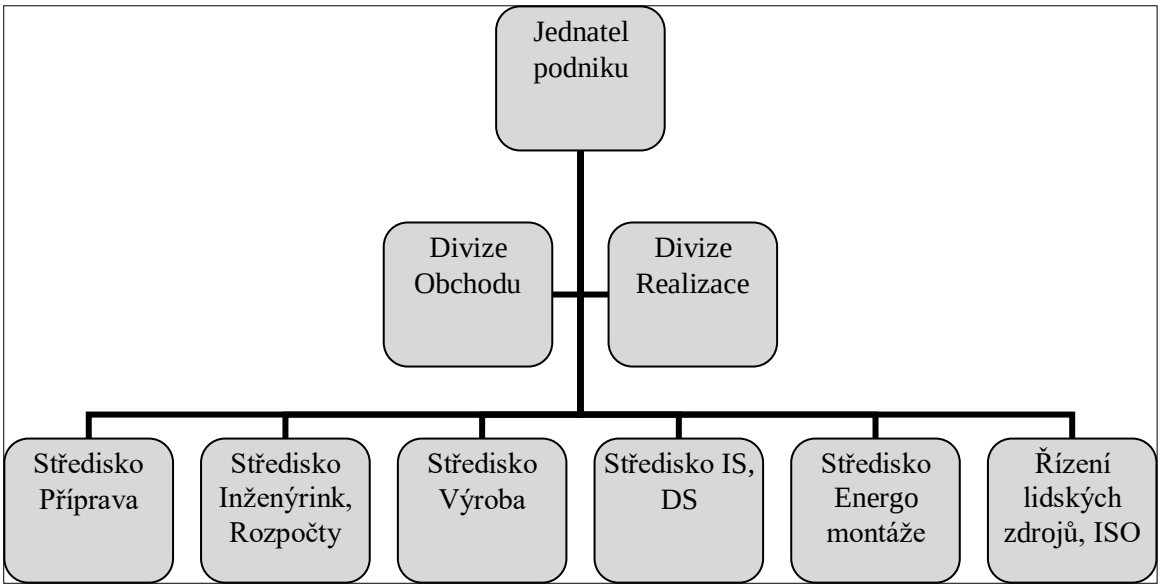
Na základě účasti interních auditů podniku a osobních rozhovorů s manažerem integrovaného systému, byly zjištěny následující informace o činnostech a poskytovaných službách, organizační struktuře a dokumentaci podniku. Interní audity se konaly v sídle podniku 1. 10. 2020 a 1. 12. 2020 za účasti představitele vedení, který celý integrovaný systém zastřešuje a za účasti manažera integrovaného systému. První interní audit byl zaměřen na celý integrovaný systém podniku, druhý interní audit byl zaměřen na rizika bezpečnosti informací. Prvotně bylo zjištěno, zda podnik splňuje základní znaky integrovaného systému a byla provedena analýza současného stavu systému. V rámci interního auditu byly manažerovi podniku položeny otázky týkající se současného stavu integrovaného systému podniku. Otázky jsou přílohou 1 této práce. První položená otázka se týká charakteristiky a struktury podniku MHK.

Podnik MHK byl založen v roce 2002 se sídlem v Hradci Králové. Hlavní realizační proces tohoto podniku je proces, kde vzniká přímá přidaná hodnota pro zákazníka a jejímž prostřednictvím dochází k realizaci zakázek. Realizační proces podniku je rozdělen do 4 procesů. Hlavním procesem jsou energomontáže a elektroinstalace včetně projekce. V oblasti energetiky podnik nabízí výstavbu veřejného osvětlení a energetického zařízení nízkého a vysokého napětí do 35 kV. Dále podnik provádí výstavbu, opravu a servis kabelových a vzdušných (vrchních) rozvodů NN a VN do 35 kV. Projektové oddělení zajišťuje kompletní zpracování projektových dokumentací energetického zařízení pro podnik ČEZ Distribuce a. s. a zpracování projektové dokumentace na VO + MR pro obce a města, včetně veřejnoprávního projednání za stavební úřad. Druhým procesem je proces průmyslové a občanské výstavby. V tomto oboru stavebních činností podnik provádí realizace a rekonstrukce nejen průmyslových, ale i bytových výstaveb a regenerace panelových domů. Zemní práce a komunikace představují třetí proces, ve kterém jsou náplní podniku dodávky inženýrských sítí, vodovodů, kanalizací, plynovodů a horkovodů, jejich výstavba a rekonstrukce včetně akutních zásahů při havarijních situacích. Středisko zabezpečuje také kompletně vlastními zdroji výstavbu zpevněných ploch a komunikací. Poslední proces tvoří Externí proces dodávek elektronických zabezpečovacích systémů, elektronických požárnických signalizací a kamerových systémů.

Organizační struktura

Organizační struktura podniku je rozdělena do dvou hlavních linií. První linii dle obrázku 6 tvoří divize Obchodu a druhou linii představuje divize Realizace. Divize Realizace kromě samotné realizace staveb zastřešuje řízení lidských zdrojů a správu interně implementovaných systémů ISO. Podnik má v současnosti zhruba 180 kmenových zaměstnanců a pouze na realizaci dodávek elektronických zabezpečovacích systémů, elektronických požárnických signalizací a kamerových systémů, si najímá externí pracovníky.

Obrázek 6 Organizační schéma podniku MHK



Zdroj: Vlastní zpracování dle ISMS (19)

Vedení podniku tvoří z hlediska celkového řízení její jednatel, který je představitelem vedení (PV). Manažerem integrovaného systému (MIS) a současně bezpečnostním manažerem je jmenována zaměstnankyně podniku. Její úlohou je především uplatňování a udržovaní definovaných procesů potřebných pro IS, předkládání zpráv vedení o dosažené výkonnosti IS a o jakékoli potřebě zlepšování a podpora povědomí závažnosti požadavků zákazníka v celém podniku. PV a MIS je odpovědný a má pravomoci zajištění vytváření, uplatňování a udržování procesů potřebných pro IS, zpracování podkladů pro přezkoumávání IS, včetně návrhů ke zlepšení, podporování vědomí závažnosti požadavků zákazníka v podniku a další práva a povinnosti. Odpovědnost za kvalitu, ochranu ŽP, BOZP a bezpečnost informací nesou všichni pracovníci. Ohledně řešení zabezpečení fungování integrovaného systému přistupuje vedení systematicky. Je si vědomo, že zajistit spokojenost našich zákazníků, tj. splnit jejich požadavky a očekávání včetně uplatnění všech legislativních požadavků na produkt, je

syntézou všech činností vstupujících do procesů. Z tohoto důvodu se všem činnostem, procesům, postupům věnuje příslušná pozornost a provádí se neustálé měření a monitorování jak produktů samotných, tak i vlastních procesů.
Správné fungování IS vyžaduje dle manažerky IS neustálou a pružnou komunikaci, která zabezpečí jeho bezproblémový chod a řízení a umožní zvyšovat jeho efektivnost. Všichni pracovníci mají pomocí e-mailu, telefonu nebo přímého kontaktu přístup k osobě odpovědné za oblast IS. Cílem interní komunikace je přenos informací na všech úrovních a funkcích za účelem posilování vnitřních vztahů vzájemné spolupráce a zapojení všech zaměstnanců do všech procesů a činností ve vztahu k EA, registrům rizik a ISŘ.
Vedení podniku provádí v pravidelných intervalech přezkoumávání IS. Cílem přezkoumávání IS je zajištění jeho přiměřenosti potřebám podniku, jeho kontinuita a efektivnost. Audit je veden manažerem integrovaného systému podniku.

Druhou otázkou pro manažerku IS bylo zjišťováno, z kterých systémů se integrovaný systém podniku MHK skládá. Bylo zjištěno, že podnik má vytvořený, dokumentovaný, uplatňovaný a udržovaný integrovaný systém, dle ISO 9001 Systém managementu kvality, ISO 14001 Systém enviromentálního managementu, ČSN ISO/IEC 27001:2014 Systém managementu bezpečnosti informací a OHSAS 18001 Systém managementu bezpečnosti a ochrany zdraví při práci. Podnik neustále zlepšuje efektivnost tohoto systému. Kontext podniku je určen interními a externími aspekty prostředí, ve kterém se podnik pohybuje, a potřebami a očekáváními zainteresovaných stran, vliv těchto aspektů a očekávání zainteresovaných stran je průběžně monitorován a na základě přezkoumání z nich plynoucích rizik či příležitostí jsou přijímána potřebná opatření. Tyto informace jsou shrnuty v registru aspektů (21) a očekávání zainteresovaných stran spravovaném manažerem integrovaného systému.

4.1.1 Politika integrovaného systému

Třetí otázka pro sledovaný podnik se týkala politiky integrovaného systému. Dle Doucka, Nováka, Nedomové a Svaté (2) je druhým cílem ustanovení ISMS definovat Prohlášení o politice, který vzniká na základě specifických potřeb daného podniku. Politika ISMS je rozsahem krátký, ale významem velmi důležitý dokument, protože prezentuje zájem vedení podniku o řízení bezpečnosti informací a definuje klíčové podmínky pro ohodnocení rizik, což je základem pro celý ISMS.
Podnik MHK má zavedenou příručku integrovaného systému, kterou vyhlašuje jednatel podniku. Tato politika IS, odpovídá záměrům podniku, zahrnuje osobní angažovanost

a aktivitu při plnění požadavků a neustálé zlepšování efektivnosti IS, poskytuje rámec stanovení a přezkoumání cílů IS a je v podniku sdělována a pochopena. Politika IS je dokumentována samostatně a je vhodným způsobem zveřejněna v prostorách podniku a na www stránkách. Aktuálnost a vhodnost politiky kvality je přezkoumávána v rámci zprávy PV o stavu IS minimálně v intervalu 1x ročně. Pracovníci jsou s Politikou IS seznamování v rámci školení, popř. v rámci pokynů pro dodavatele.

Vedení podniku si uvědomuje, že stanovená politika IS může splnit uplatňováním efektivního IS zaměřeného na zákazníka. Proto je každému zákazníkovi věnována maximální pozornost s cílem splnit v největší možné míře jeho oprávněné požadavky, a to i ty, které lze předpokládat. Vedení provádí sběr a vyhodnocování informací o spokojenosti zákazníků, které je prováděno formou předávacích protokolů, referenčních listů a zavazuje se k dalšímu rozvoji podniku, neustálému zlepšování úrovně kvality výrobků a služeb k všestrannému uspokojování očekávaných i předpokládaných potřeb zákazníků a naplňování požadavků právních předpisů. Zároveň přijímá odpovědnost za ochranu životního prostředí v souvislosti se svou podnikatelskou činností v oblasti stavebních prací. Uznává potřebu zlepšování environmentálního managementu jako jednu z nejvyšších priorit podniku. K posílení ochrany životního prostředí, zlepšení kvality, BOZP, prevenci úrazů a nemocí z povolání se vedení podniku rozhodlo kontrolovat a minimalizovat možná rizika. K prioritám podniku trvale patří ochrana životního prostředí a vytváření bezpečných pracovních podmínek pro zaměstnance.

4.1.2 Odpovědnost a plánování managementu

Základním znakem integrovaného řízení je odpovědnost a plánování. Zdali tyto znaky podnik splňuje, bylo zjišťováno otázkou čtvrtou „Jakým způsobem plánujete, udržujete a zlepšujete integrovaný systém?“. Vedení podniku zajišťuje plánování, udržování, zlepšování a schopnost reagovat na změny požadavků na IS jeho pravidelným přezkoumáváním. V případě změn vedení podniku tyto změny identifikuje, posoudí účel změn a jejich následky, nutné zdroje a potřebu rozdělení či přerozdělení odpovědností a pravomocí, a následně zajistí zapracování do dokumentace IS a zajistí jeho integritu.

Podnik plánuje tak, aby i v případě realizace organizačních či jiných změn v IS byla zachována jeho integrita. Pokud by podnik v budoucnu přistoupil k realizaci cíle, který se týká vývoje nebo pozměněné činnosti, pak před zahájením akcí budou určeny a vyhodnoceny ty environmentální aspekty, které mohou mít významné environmentální dopady. PV musí zajistit, aby při plánování nové činnosti byly e-aspekty vzaty v úvahu při stanovení environmentálních cílů. Smyslem plánování IS je zajištění fungování procesů a dalších

činností tak, aby byly splněny cíle IS a aby bylo dosaženo politiky IS. Podnik plánuje především prostřednictvím plánu školení, plánu interních auditů, plánu údržby strojů a firemních vozů.

Tabulka 4 SWOT analýza pro strategické plánování

Silné stránky
✓ síť spolehlivých dodavatelů a subdodavatelů, z nichž někteří mají unikátní charakter,
✓ kvalifikovanost pracovníků řemeslných profesí, schopných samostatného rozhodování a improvizace
✓ odborné schopnosti a zkušenosti manažera a technického ředitele z různorodých stavebních projektů,
✓ vysoká efektivita činnosti s ohledem na počet interních zaměstnanců a dobu působení na trhu,
✓ plná vytíženost výrobních kapacit, soustavná péče o lidské zdroje a odhodlání managementu zpracovat a realizovat strategickou koncepci rozvoje,
✓ využívání manažerských znalostí a dovedností v podnikové praxi
Slabé stránky
✓ marketing činnosti;
✓ nedostatečná odbornost zaměstnanců v oblasti vyspělých technologií stavění energetická a surovinová náročnost realizovaných stavebních děl;
✓ nedostatečná jazyková vybavenost a odbornost zaměstnanců v IT,
✓ úzká odborná profilace zaměstnanců,
Příležitosti
✓ včasné přizpůsobení činnosti novým trendům v oboru a získání konkurenční výhody,
✓ integrace moderních prvků do stavebního procesu,
✓ schopnost přizpůsobit se požadavkům investora i koncového zákazníka uzpůsobením díla novým požadavkům (nové technologie),
✓ požadavky na radikální snižování energetické náročnosti stávajících budov,
✓ schopnost zabezpečit kvalitní, spolehlivé, rentabilní řešení s přidanou hodnotou, zavedení nových technologií (aplikace výrobků s nanovlákny apod.),
✓ vysoce poddimenzovaný segment dřevěného stavění v ČR,
Hrozby
✓ nepřizpůsobení prodejní, marketingové a vzdělávací strategie vývoji trhu,
✓ pomalá realizace opatření směřujících k odbornému posunu podniku,
✓ spokojení se se současnými technologiemi pod vlivem dostatku zakázek a plného využití kapacit,
✓ nedostatek kvalifikovaných pracovníků a vysoké náklady na pracovní sílu,
✓ podcenění opatření proti vzniku chyb při montážích pokročilých zařízení,
✓ značné náklady na vyřizování reklamací, rychlejší přizpůsobení konkurence novým podmínkám,
✓ akcelerující ekonomická stagnace a další pokles investic do stavebnictví

Zdroj: ISMS (19)

Strategické plánování podniku je postaveno na SWOT analýze, která je znázorněna ve výše uvedené tabulce 4 a kterou nám předložil manažer IS podniku.

Infrastruktura

Vedení je odpovědné za to, že je k disposici potřebná infrastruktura v potřebném rozsahu a na potřebné technické úrovni. Infrastruktura zahrnuje budovy, pracovní prostory a technické vybavení, zařízení pro hlavní proces, podpůrné služby. Podnik má stanovenou infrastrukturu samostatně. Při pořizování investic podnik posuzuje jejich vliv na životní prostředí a pokud možno volí investice s menším negativním environmentálním dopadem. Při údržbě zařízení zvažuje potřebu údržby i z hlediska předcházení znečištění životního prostředí, vlivu na BOZP, snižování hluku, možnosti havarijních úniků, závadných látek a následné kontaminace ŽP. Důvodem k provádění údržby může být zlepšení dopadu zařízení na ŽP či BOZP nebo předcházení poruch v provozu. Při údržbě jsou vždy dodržovány podmínky a postupy, které jsou šetrné k ŽP a odpovídají podmínkám BOZP.

Pracovní prostředí

Vedení podniku MHK se zavazuje organizovat pracovní proces tak, aby prostředí bylo bezpečné, čisté, estetické a motivující. Odpovědnost za zajištění požadovaných parametrů prostředí z pohledu produktu má vedení. Za plánování a zajištění vhodného pracovního prostředí a pracovních prostředků je v souladu se strategií rozvoje podniku odpovědné vedení. Za dodržování stanovených podmínek na pracovní prostředí odpovídá stavbyvedoucí, kontrolu provádí dle obecně platných přepisů. Při prováděných činnostech, které mají stanovené technologické podmínky, jsou tyto podmínky monitorovány způsobilým měřicím zařízením, tak aby podmínky byly vhodné pro vykonávanou činnost. Každý vedoucí zaměstnanec, v rámci svých kompetencí, odpovídá a je povinen průběžně prověřovat a přispívat k zajištění vhodného pracovního prostředí jako kombinaci fyzikálních a lidských faktorů, které umožňují a přispívají k potřebné motivaci zaměstnanců při dodržení zásad BOZP a PO. Řízení pracovního prostředí je zajištěno dokumenty, jejichž seznam je uveden v Související dokumentaci.

4.1.3 Dokumentace podniku

Ondrák, Sedlák a Mazálek (4) uvádí, že jedním z okruhů systému řízení bezpečnosti informací je jednotná dokumentace, která musí být dostatečně ochráněna proti zneužití. Způsob ochrany dokumentů a dat k řízení podniku a integrovaného systému podniku MHK, byl pátou otázkou pro manažera podniku.

Dokumentace podniku MHK je souborem všech interních a externích dokumentů a záznamů, nezbytných k řízení podniku. Základním interním řízeným dokumentem je příručka IS a dále

pak další navazující záznamy a dokumenty. Dokumentace je v podniku rozdělena na interní (tj. dokumenty, které si sami vytváří) a na externí (tj. dokumenty, které si nevytváří, ale kterými jsou povinni se řídit).

Interní dokumenty

Zpracovatelem každého interního řízeného dokumentu je MIS, nebo jiný pracovník, kterého se zpracovávaná problematika týká. Při zpracovávání dokumentu se zaměřuje především na jednoduchost a srozumitelnost textu, a dále na návaznost na ostatní zpracované dokumenty tak, aby si navzájem neodporovaly. Přezkoumání zpracovaného interního řízeného dokumentu provádí buď jeho zpracovatel, nebo jiný jím zvolený pracovník dle povahy zpracovaného dokumentu. Každý interní řízený dokument schvaluje PV nebo minimálně rozhodne o jeho vydání. Každý vydávaný interní řízený dokument musí být identifikován minimálně názvem podniku, názvem dokumentu, datem zpracování, datem schválení, číslem verze, číslem paré, počtem stran a v případě tištěné verze i podpisem zpracovatele a schvalovatele. Všem pracovníkům jsou interní řízené dokumenty, které potřebují pro vykonávání práce, k dispozici na firemním serveru. Pokud kterýkoliv pracovník zachází s tištěnou verzí dokumentace, je povinen ji zachovávat čistou a nepoškozenou i pro další uživatele. S novými dokumenty nebo se zrevidovanými dokumenty jsou pracovníci seznamováni buď na poradách, nebo školeních.

Dokument v tištěné verzi musí být opatřen evidencí prováděných revizí nebo změn. Změny tištěných dokumentů IS se provádí opravou v původním dokumentu (přeškrtnutím starého údaje a uvedením nového) nebo vydáním nového listu nebo vydáním dodatku dokumentu nebo vydáním nového dokumentu IS. Provádět změny v dokumentech IS (provádět opravy, vydávat nové listy a dodatky) je oprávněn pouze MIS na základě provedené revize a na základě schválení PV. Změny zapisuje v soupisu revizí a změn na druhé straně dokumentu IS, tzn. původní stránku MIS přeškrtne a zařadí ji na konec dokumentu. Při schvalování, vydávání a distribuci dodatku příslušného dokumentu IS musí být zachován stejný postup jako při vydávání nového dokumentu IS. Dodatky se ke každému dokumentu IS číslují vzestupně. Na základě revize nebo po překročení únosného počtu dodatků, rozhodne PV o vydání nového dokumentu. Každý dokument IS reviduje MIS minimálně 1x za rok; revizí se prověřuje správnost, aktuálnost a přehlednost dokumentů.

Všechny dokumenty v elektronické verzi, které jsou umístěny na firemním serveru, jsou řízené; výjimku tvoří dokumenty označené jako neplatné; odpovědnost za uspořádání interních dokumentů, vedených v elektronické podobě mají všichni pracovníci administrativy;

v případě vydávání elektronické verze musí být tento dokument uložen na určené místo vždy v aktuální podobě.

Externí dokumenty

Dokumenty vzniklé mimo podnik (např. legislativní předpisy, normy…) musí být označeny názvem, u legislativy a norem navíc číslem a datem vydání. Pokud by bylo od jednoho vydání více výtisků, budou tyto očíslovány a rozdělovník uveden v Registru právních a jiných požadavků. MIS zajišťuje aktualizaci předpisů prostřednictví internetu – vede aktuální seznam (Registr právních a jiných požadavků) těch, které se nejvíce týkají činnosti podniku a všichni pracovníci jsou povinni se informovat o aktuálním znění vztahující se k jejich pracovní činnosti.

Řízení záznamů

Záznamy v podniku objektivně vypovídají o realizaci požadavků IS v podniku. Záznam má trvalou podobu, tj. není přípustná jeho aktualizace. Každý záznam musí obsahovat minimálně název podniku, název záznamu, datum zpracování, počet stran a v případě tištěné verze i podpis zpracovatele. Veškeré formuláře pro vedení záznamů, které jsou v podniku používány, mohou mít různou úpravu, ale musí mít zachovány zásady, co který záznam musí obsahovat. Základní vytváření záznamů vyplývá z popisu pracovní činnosti každého pracovníka, případně daného pracovníka pověřuje zpracováním jiného nestandardního záznamu MIS. Představitel vedení a MIS odpovídá za seznámení pracovníků, kterých se daný záznam týká, s jeho zpracováváním a ukládáním. Všichni pracovníci jsou povinni uchovávat na svém pracovišti pouze platné, čisté, čitelné a nepoškozené záznamy a chránit je před zneužitím, tj. záznamy mohou být vedeny v tištěné i v elektronické podobě. U záznamů vedených v tištěné podobě musí být vedeny minimálně propisovací tužkou, při chybě se nesmí nesprávný záznam přemazávat či přelepovat, ale vždy pouze přeškrtnout a vedle zapsat záznam správný včetně parafování upravitele. Požadavky na environmentální záznamy jsou dány požadavky právních předpisů v oblasti ochrany ŽP a rozhodnutími státní správy včetně doby uchovávání a archivace těchto záznamů. K environmentálním záznamům patří i záznamy týkající se měření environmentálního profilu podniku. Požadavky na záznamy BOZP jsou dány normou a požadavky právních předpisů v oblasti BOZP a rozhodnutími státní správy včetně doby uchovávání a archivace těchto záznamů.

Data v elektronické podobě představují dokumenty IS (interní i externí), záznamy a písemnosti vzniklé z činnosti podniku, které jsou uloženy v elektronické podobě na počítačích podniku. Veškeré dokumenty IS a záznamy jsou uloženy na počítači MIS

v příslušných adresářích. Ochrana před viry a před nežádoucím napadením zvenku je zajištěna pomocí antivirového řešení, a to jak softwarovým řešením, tak hardwarovým řešením. Softwarová antivirová ochrana je nainstalována na PC, na notebooku a na serveru; aktualizace antivirového softwaru probíhá zcela automaticky pravidelným stahováním updatů z internetu; za nastavení režimu aktualizace odpovídá jednatel podniku a správce sítě podniku.

Požadavky na environmentální záznamy jsou dány požadavky právních předpisů v oblasti ochrany ŽP a rozhodnutími státní správy včetně doby uchovávání a archivace těchto záznamů. K environmentálním záznamům patří i záznamy týkající se měření environmentálního profilu podniku. Požadavky na záznamy BOZP jsou dány normou a požadavky právních předpisů v oblasti BOZP a rozhodnutími státní správy včetně doby uchovávání a archivace těchto záznamů.

4.1.4 Právní soulad s předpisy a normami v podniku

Základním požadavkem IS je soulad veškerých činností s právními a jinými požadavky, kterým podnik podléhá. Jakým způsobem udržuje soulad s normami a předpisy MHK, byl šestou otázkou pro manažera podniku. MHK stanovil postup pro zjišťování, dostupnost a udržování všech právních i jiných požadavků pro ni platných, které se přímo dotýkají EA, BOZP a jejich procesů, činností, produktů a služeb. Pro sledování aktuálních právních požadavků má podnik vytvořen Registr právních a jiných požadavků, který je tvořen zákony, vyhláškami, nařízeními a dalšími legislativními předpisy z oblasti ochrany ŽP a BOZP. Tyto požadavky jsou důsledně sledovány přes internet. Registr právních a jiných požadavků je aktualizován dle potřeb, minimálně 1x ročně. Informace z těchto předpisů jsou ostatním pracovníkům podniku předávány ve formě zpracovaných aktualizovaných dokumentů EMS a BOZP a dále formou pravidelných i účelových jednorázových školení. Pro potřeby podniku se do registru zahrnují veškeré zákony a vyhlášky v platném znění z jednotlivých oblastí ŽP a BOZP.

Za aktualizaci právního registru odpovídá MIS. Externě zajištěný interní auditor zasílá MIS průběžně přehled o zákonech a vyhláškách, které vycházejí ve Sbírce zákonů, informuje ho o veškerých změnách v oblasti ochrany ŽP, BOZP a bezpečnosti informací, které se týkají činnosti podniku. Všechny právní předpisy jsou dle číselné identifikace dohledatelné na www.mvcr.cz, kde je možnost si je stáhnout, uložit, vytisknout. Dalšími zdroji pro doplňování právního registru je Věstník MŽP ČR, Zpravodaj MŽP ČR, státní normy, které jsou citovány v zákoně, rozhodnutí státní správy atd.

Při zveřejnění nové právní normy týkající se ochrany ŽP, BOZP a bezpečnosti informací zajistí PV první posouzení, zda se tato norma týká činností podniku. V kladném případě rozhodne, jakým způsobem budou povinnosti vyplývající z nového předpisu promítnuty do dokumentace podniku.

Požadavky mimo rámec legislativních požadavků, ke kterým se podnik zavázal, jsou zařazovány do registru právních a jiných požadavků. Jsou to např. dohody se státní správou, směrnice jiné než zákonné povahy, smlouvy apod.

4.1.5 Monitorování, měření procesů a zlepšování

Dle Doucka, Nováka, Nedomové a Svaté (2) je nezbytné provést v podniku činnosti, které se skládají z identifikovaných možností monitorování a zlepšení ISMS a prováděním odpovídající ch opatření k nápravě a preventivních opatření pro odstranění nedostatků. Jakým způsobem jsou v podniku MHK monitorovány a zlepšovány procesy integrovaného systému bylo zjišťováno u interní auditorky podniku otázkou sedmou.

Kontrola, zkoušení a měření jsou neoddělitelnou součástí výrobních procesů v tomto podniku a jsou podkladem pro vyhodnocování IS. Její závěry se využívají pro plánování kontrolních operací, s cílem zabezpečení shody a neustálého zlepšování činností souvisejících s produktem, procesem a ochranou ŽP. Přehled o spokojenosti zákazníků s kvalitou staveb, o zkušenostech z jejich užívání a o spokojenosti s poskytnutými službami jsou základními informacemi nezbytnými pro další zlepšování výroby podniku. Všichni pracovníci jsou povinni se aktivně zapojit do sběru informací o spokojenosti zákazníků s činností podniku. Každý pracovník je povinen neprodleně informovat jednatele nebo vedoucího pracovníka o jakýchkoliv negativních signálech od zákazníků nebo jiných stran na činnost podniku. PV tyto informace analyzuje a v závislosti na objektivitě těchto informací přijímá nezbytná opatření k nápravě. Monitorování a měření procesů se provádí systematicky, aby bylo možné ověřit, zda činnosti týkající se IS a dosažené výsledky jsou v souladu se specifikovanými požadavky (politikou a cíli IS). Výsledky měření a monitorování procesů jsou zásadním podkladem pro neustálé zlepšování. Podnik má stanoveny kritéria pro měření procesů.

Interní audit

Pravidelné interní audity jsou v podniku prováděny z toho důvodu, aby se ověřilo, že IS vyhovuje požadavkům systémových norem a je efektivně uplatněn a udržován. Zajištění interních auditů je na základě smlouvy s externím podnikem, který má interní auditory vyškolené dle stanovených kritérií. Vedení podniku odpovídá za to, že interní audity jsou plánovány a prováděny podle tohoto postupu. Interní audity jsou plánovány dle složitosti

procesů a významnosti environmentálního významu jednotlivých činností. Interní audity jsou plánované, mimořádné a následné.

Plánovaný IA: jedná se o interní audit realizovaný podle ročního plánu.

Mimořádný IA: jedná se o interní audit prováděný z konkrétních důvodů, například při zjištění určitých neshod, poruch nebo odchylek; dále se provádí při podstatných změnách IS

Následný IA: jedná se o interní audit prováděný za účelem ověřit odstranění neshod a účinnost nápravných opatření vzešlých z předchozích interních auditů.

Vlastní interní audit podniku MHK spočívá ve shromažďování informací o efektivnosti a účinnosti IS prostřednictvím pohovorů, zkoumáním dokumentů, monitorováním činností a podmínek v daných oblastech zájmu. Je třeba zaznamenávat i náznaky neshod, jestliže se jeví jako významné. Informace získané při pohovorech ověřuje vedoucí auditor získáním relevantních informací z jiných nezávislých zdrojů jako je fyzické zjišťování, měření a záznamy. Je-li to nezbytné k zajištění optimálního dosažení cílů auditu. Součástí auditu EMS je místní šetření zaměřené na identifikaci a řízení EA hodnocení souladu s legislativou, povědomí zaměstnanců o zavedeném IS. Auditorem oslovení pracovníci jsou povinni pravdivě zodpovědět všechny otázky auditora a předložit požadované podklady. Před závěrečným projednáním provedeného IA s vedoucím prověřované oblasti interní auditor přezkoumá jednotlivé neshody po věcné i formální stránce a protokolární záznamy o nich autorizuje. Auditor seznámí prověřovaného se zjištěními s důrazem na jednotlivé neshody. Spolu s auditorem zodpoví dotazy a řeší případné výhrady prověřovaných zaměstnanců. Vedoucí prověřovaného pracoviště potvrdí svým podpisem v příslušné kolonce, že identifikované neshody pochopil a souhlasí s nimi. Jestliže jsou zjištěny neshody v takovém rozsahu, že interní auditor shledá nutnost prověření dané oblasti znovu, navrhne provedení dalšího auditu na tuto oblast. Společně s MIS stanoví termín následného auditu a MIS ho zapracuje do ročního plánu/programu interních auditů.
Po ukončení interního auditu, interní auditor vypracuje zprávu z interního auditu. Tuto zprávu včetně všech souvisejících protokolů o neshodách předá interní auditor MIS, a to nejpozději do pěti pracovních dnů od ukončení interního auditu.

Zlepšování

Podnik MHK neustále zlepšuje efektivnost zavedeného IS, a to využíváním politiky IS, cílů a cílových hodnot, výsledků auditů, analýzy údajů, opatření k nápravě, preventivních opatření

a přezkoumání managementu. Zlepšování v oblasti EMS a BOZP znamená zlepšování profilu podniku (environmentálního a z pohledu BOZP).

Opatření k nápravě

Opatření k nápravě jsou podnikem přijímána buď okamžitě po výskytu neshody, kdy za jejich přijetí zpravidla odpovídá jednatel, nebo jako pravidelná systematická činnost zaměřená na odhalování příčin vzniklých neshod. Jedná se o činnosti zaměřené na odstranění příčiny vzniklé neshody s cílem zabránit jejímu opakovanému výskytu. Za tuto činnost je odpovědný PV a MIS. V pravidelných intervalech (na poradě 1x za rok) nebo v případě potřeby provádí analýzy a přezkoumání zaznamenaných neshod s cílem odhalit závažné neshody nebo neshody, které se vyskytují příliš často a podnik finančně i časově zatěžují. Na základě odhalení příčin těchto neshod přijímá PV taková opatření, která odstraní tyto příčiny a zamezí opakovanému vzniku neshod. Za realizaci opatření k nápravě určí odpovědného zaměstnance. MIS dále provádí kontrolu, zda bylo opatření realizováno. Přezkoumání efektivity a účinnosti se týká veškerých opatření k nápravě přijatých v podniku, a záznam je součástí zprávy z přezkoumání IS. Odpovědnost za obsah tohoto dokumentovaného postupu má MIS. Nápravná opatření musí být úměrná dopadu na životní prostředí.

Preventivní opatření

Preventivní opatření jsou podnikem přijímána za účelem vyloučení příčin potencionálních neshod. Tato opatření jsou přijímána přiměřeně závažnosti problému a míře rizik, aby se zabránilo jejich výskytu. V rámci neustálého zlepšování činnosti podniku vedoucí k vysoké kvalitě poskytovaných služeb, provádí podnik systematické odhalování a odstraňování potenciálních rizik. Za přijímání preventivních opatření odpovídá PV. Vyhledávání potenciálních neshod a určení jejich příčin je součástí každodenní náplně práce všech zaměstnanců, pravidelně je potom tato činnost prováděna 1x ročně v souvislosti s analýzou nápravných a preventivních opatření ve zprávě z přezkoumání IS. Preventivní opatření jsou přijímána s ohledem na závažnost důsledků potenciální neshody a organizační a finanční možnosti podniku. PV určí zaměstnance odpovědného za provedení opatření a provede kontrolu realizace tohoto opatření. Efektivitu opatření přezkoumá MIS zpravidla za 6 měsíců nebo při nejbližším přezkoumání vedením. Účinnost provedených opatření je vyhodnocována ve zprávě pro přezkoumání IS vedením.

4.2 Systém řízení bezpečnosti informací v podniku

Dle Hanáčka a Staudka (16) je systém řízení bezpečnosti informací v podniku systémem, který nejen chrání informace podniku před ztrátou či zneužitím, ale chrání i členy vedení a zaměstnance před nechtěnými prohřešky vůči zákonům ČR. ISMS je systém, který je velmi důležitý pro zajištění činností podniku. Bezpečnost informací a jejich rizika v podniku byla hlavním tématem na druhém interním auditu, který se konal 1.12. 2020.

Systém řízení bezpečnosti informací se v MHK vztahuje na následující aktivity podniku:

- projekce, montáže, opravy a rekonstrukce elektrických zařízení NN, VO a VN do 35 kV
- provádění staveb, jejich změn a odstraňování
- zemní práce a terénní úpravy, protlaky pod komunikacemi
- dodávky elektronických zabezpečovacích systémů, elektronických požárnických signalizací a kamerových systémů (externí proces)

Integrovaný systém řízení podniku MHK zahrnuje data poskytovaná klienty k realizaci činnosti, osobní informace vztahující se k zaměstnancům podniku, informace o smluvních partnerech podniku, komunikaci účastníků a IT infrastrukturu podniku (servery, síť, notebooky, stanice).

Všichni zaměstnanci podniku a smluvně vázaní spolupracovníci, kteří jsou v interakci s informačními aktivy definovanými v rozsahu systému řízení bezpečnosti informací (ISMS), jsou odpovědni za dodržování této bezpečnostní politiky. Tato politika je plně podporována a schválena vedením podniku.

4.2.1 Aplikovatelnost ČSN ISO 27001 v podniku

Prohlášení o aplikovatelnosti je seznam bezpečnostních opatření navrhovaných normou ČSN ISO/IEC 27001:2014. Pro jednotlivá opatření je v prohlášení o aplikovatelnosti zaznamenáno, zda a jak jsou v podniku implementována, případně je uvedeno zdůvodnění, proč implementována nejsou. Aplikovatelnost této bezpečnostní normy na podnik MHK je uvedeno v příručce prohlášení o aplikovatelnosti ČSN ISO 27001 v podniku.

4.2.2 Pozice a role v rámci ISMS v podniku

Bezpečnostní informační manažer

V podniku MHK odpovídá za bezpečnost informací bezpečnostní manažer, jehož jmenování nám vedení podniku předložilo. Bezpečnostní manažer bere své jmenování na vědomí

podpisem na titulní straně příručky ISMS. V podniku prosazuje bezpečnostní politiku a koordinuje školení zaměstnanců v oblasti informační bezpečnosti. Zároveň sleduje dodržování bezpečnostních opatření ve všech oblastech informační bezpečnosti a navrhuje změny politiky, směrnic a navazujících dokumentů. Bezpečnostní manažer dohlíží na provádění změn a řeší bezpečnostní události.

Bezpečnostní správce

Bezpečnostní správce podniku MHK připomínkuje aplikaci opatření z hlediska použitých technologií, řeší bezpečnostní události a zajišťuje informační bezpečnost z technického hlediska. V rámci své účasti v profesních sdruženích a dalších specializovaných bezpečnostních fórech získává aktuální informace o nejlepších praktikách a nejnovějších trendech v oblasti bezpečnosti informací.

Vedoucí bezpečnostní auditor

Vedoucí bezpečnostní auditor koordinuje školení interních bezpečnostních auditorů, plánuje a provádí nezávislé revize bezpečnosti informací. Tabulka 5 nám představuje role a zabezpečení integrovaného systému řízení bezpečnosti informací v podniku MHK.

Tabulka 5 Role ISMS v podniku MHK

Role integrovaného systému řízení bezpečnosti informací	Zabezpečení
Bezpečnostní informační manažer	Zaměstnanec podniku
Bezpečnostní správce	Externí IT podnik
Vedoucí bezpečnostní auditor	Externí IT podnik

Zdroj: Vlastní zpracování (2021)

4.2.3 Bezpečnostní politika podniku

Podnik MHK má zavedenou bezpečnostní politiku, kterou nám bezpečnostní manažer předložil. Bezpečnostní politika je základním řídícím dokumentem, který vyjadřuje postoj vedení podniku k zajištění bezpečnosti informací. Předmětem bezpečnostní politiky je stanovení cílů a odpovědností pro zajištění ochrany informačních aktiv z hlediska důvěrnosti, integrity, dostupnosti. Podnik se zavazuje zajistit zpracování, řízení a uchování informací adekvátními bezpečnostními postupy. Tato politika je tvořena a posuzována vedením podniku. Bezpečnostní manažer odpovídá za uplatnění této politiky prostřednictvím příslušných standardů a procedur. Všichni zaměstnanci a smluvně vázaní dodavatelé se řídí postupy v souladu s touto politikou. Všichni zaměstnanci jsou odpovědni za hlášení bezpečnostních incidentů a jakýchkoliv identifikovaných slabin. Všechny úmyslné činy

vedoucí k ohrožení bezpečnosti informací podniku nebo jejích zákazníků či dodavatelů budou předmětem disciplinárního nebo soudního řízení.

4.2.4 Informace a komunikace v podniku

V podniku MHK je vymezena komunikace písemná, elektronická, osobní ústní a vzdálená ústní komunikace. Písemnou komunikací se rozumí předávání informací formou papírového dokumentu nebo pomocí faxu. Elektronickou komunikací se rozumí předávání informací v elektronické podobě (vč. elektronické pošty). Osobní ústní komunikací se rozumí předávání informací formou hovoru s jinou osobou na stejném místě a vzdálenou ústní komunikací se rozumí předávání informací formou hovoru s jinou osobou na jiném místě vedenou pomocí technických prostředků (např. telefonický rozhovor). Specifika písemné komunikace a pravidla pro zacházení s těmito informacemi jsou uvedeny ve směrnici ISMS (19).

Písemná komunikace

Interní informace podniku nesmějí být vystaveny na prostranstvích, do kterých mají nekontrolovaný přístup osoby, které nejsou oprávněnými příjemci informace (např. nástěnky na chodbách, kde je nekontrolovaný přístup cizích osob). Tisk neveřejných dokumentů je vždy prováděn na lokálních tiskárnách nebo na tiskárnách, kde je zamezeno přístupu k dokumentům neoprávněnými osobami. Předávání neveřejných informací cizímu subjektu přes zprostředkovatele (např. poštovní služba) je povoleno pouze v případě, že jde o zprostředkovatele, se kterým má podnik uzavřenu smlouvu o mlčenlivosti a informace jsou při převozu uloženy v neprůhledné a zapečetěné obálce. Písemná dokumentace je uchovávána v zamykatelných schránách, případně v místnostech s výlučným přístupem autorizovaných osob. V případě, že je informace předávána adresátovi přes zprostředkovatele (např. poštovní služba) jsou informace předávány v obálce se zřetelně vyznačeným adresátem ev. okruhem adresátů.

Elektronická komunikace

Při předávání informací formou elektronické pošty pracovník podniku MHK vždy ověří, zda adresa elektronické pošty příjemce informace je platná a příjemce informace je jediným uživatelem adresy elektronické pošty. Při odesílání tajných informací musí být použito silné heslo. Při předávání informací formou elektronického souboru uloženém na nosiči dat pracovník zajistí, aby nosič dat obsahoval pouze informace, které jsou relevantní pro danou situaci a zároveň pouze data, se kterými je oprávněn příjemce se seznámit. Nosič dat musí být ochráněn proti zneužití informací neoprávněnými osobami silným heslem. Předávání tajných

informací formou elektronického souboru uloženého na nosiči dat cizímu subjektu přes zprostředkovatele (např. poštovní služba) je povoleno pouze v případě, že jde o zprostředkovatele, se kterým má podnik uzavřenu smlouvu o mlčenlivosti a informace jsou při převozu uloženy na datovém nosiči v neprůhledné a zapečetěné obálce, nosič dat musí být ochráněn proti zneužití informací neoprávněnými osobami silným heslem. On-line elektronická písemná komunikace (chat apod.) nesmí být pro předávání neveřejných informací používána. Neveřejné informace prostřednictvím emailu jsou předávány pouze určenému adresátovi.

Osobní ústní komunikace

Ústní komunikace je v MHK vedena pracovníkem podniku s příjemcem informace tak, aby byla minimalizována možnost odposlechu komunikace osobou, která není oprávněna seznamovat se s informacemi. Hovory musejí být vedeny tak, aby nebyly hlasité, a nesmí být vedeny v nekontrolovaných prostorách.

Vzdálená ústní komunikace

Při vzdálené ústní komunikaci vedené formou technických prostředků bez přenosu obrazu se pracovník podniku vždy ujistí, že osoba, se kterou hovoří, je osoba, se kterou zamýšlel hovořit. Pracovník podniku je zároveň povinen zajistit, aby nemohla do komunikace mezi ním a příjemcem informace vstoupit třetí osoba. Vzdálená ústní komunikace neveřejných informací formou technických prostředků není dovolena.

4.2.5 Plán kontinuity podniku

Plán kontinuity má podnik MHK zpracovaný formou směrnice. Cílem plánů kontinuity je především obnovení činností podniku v případě nastání závažných chyb a katastrof. Proces kontinuity zajišťuje, aby výpadky způsobené pohromami a selháním bezpečnosti (např. přírodní pohromy, nehody, chyby zařízení, úmyslné poškození) byly eliminovány na přijatelnou úroveň. Využívá se k tomu preventivních opatření a speciálních postupů obnovy. Bezpečnostní manažer je odpovědný za vytvoření plánů kontinuity pro středně a vysoce rizikové hrozby, dle analýzy rizik. Vedle vytvoření plánů kontinuity je bezpečnostní manažer zodpovědný také za jejich vhodné zveřejnění (např.: školení, vyvěšení na nástěnce), pravidelné přezkoumávání a zajištění jejich testování. Součástí každého plánu kontinuity je popis situací, které jsou impulsem pro spuštění daného plánu, popis způsobu hlášení krizové/ havarijní situace a popis činností osob při řešení krizové / havarijní situace. Plány kontinuity jsou dále udržovány prostřednictvím pravidelných přezkoumání, prováděných nejméně 1x

ročně. Za provádění pravidelných přezkoumání plánů kontinuity je zodpovědný bezpečnostní manažer a o provedení přezkoumání je povinen vyhotovit záznam. Plány kontinuity mohou selhat z důvodů nesprávných předpokladů, přehlédnutí nebo změn zařízení nebo personálu. Proto musí být ve shodě s obchodními potřebami podniku testovány, aby se zajistila jejich aktuálnost a efektivita. Testování zajišťuje bezpečnostní manažer. Před provedením testu je povinen vyhotovit plán testu, který musí být schválen vedením podniku. Po provedení testu zajistí bezpečnostní manažer vytvoření záznamu z provedeného testu. Pro zaznamenání obou kroků je možné využít jednotný záznam, test plánu kontinuity. Takové testy rovněž zajišťují, že všichni členové havarijního týmu i ostatní zaměstnanci, kteří plní nějaké úkoly stanovené plánem, jsou řádně připraveni a s plánem seznámeni.

Po nahlédnutí do plánu kontinuity podniku MHK bylo zjištěno, že podnik má tento plán rozdělen na dvě hlavní části, na havárii serveru a havárii objektu. V případě kompletní havárie serveru podniku MHK použije administrátor v danou chvíli nejméně vytížené PC, popř. jiný osobní počítač. Vzhledem ke stejnému operačnímu systému serveru, který je rovněž na jakékoliv jiné stanici v síti. Následně do 60 minut obnoví zálohovaná data do alternativního počítače. V případě funkčnosti alespoň jednoho pevného disku, připojí administrátor tento disk na náhradní PC. Následně v případě funkčnosti alespoň jednoho pevného disku, připojí administrátor tento disk na náhradní PC. Do dalších 60 minut na jednotlivých stanicích překonfiguruje sdílený adresář. Vzhledem k tomu, že na alternativním počítači bude stejná IP adresa, totožná s tou, která byla na serveru, budou všechny služby poskytované serverem plně zastoupeny alternativním PC. Maximální čas reakce administrátora do zahájení obnovy má podnik stanovený na 120 minut v pracovní den při využití vzdáleného přístupu, nebo 180 minut v pracovní den při zásahu na místě. Celkový čas potřebný k realizaci obnovy má podnik stanovený do 5,5 hodin. Havárie administrátorského PC nemůže v podniku nastat, protože na pracovišti podniku žádný takový PC není. Veškeré počítače v síti jsou vesměs vzájemně nahraditelné. V případě nutnosti použití poštovního klienta vytvoří a nakonfiguruje administrátor daný účet.

V případě, že dojde k poškození objektu s následkem nemožnosti dalšího využívání, potřebuje podnik k minimální nouzové činnosti 2 počítače, které plní funkci zpracování dat, serveru a sdílení internetu, a funkci elektronickou poštu a administrativní činnost. Pokud nastane havárie, počítač zabezpečující funkci serveru, zpracování dat a sdílení internetu musí administrátor nahradit v případě možnosti administrátorovým PC (firemním), kde je nainstalován všechen originální potřebný software, případně bude proveden okamžitý nákup

náhradního PC. Při obnově se postupuje dle předchozí havárie serveru, obnova probíhá ze zálohy. Čas potřebný k realizaci obnovy v případě použití existujícího PC má podnik stanovený do 5,5 hodiny. Čas potřebný k realizaci obnovy v případě nákupu PC je stanoven na + 1 den. Pro elektronickou poštu a administrativní činnost dostačuje instalovaný kancelářský SW MS Office. Čas potřebný k realizaci obnovy v případě použití existujícího PC je stanoven na 3,5 hodiny/PC. Čas potřebný k realizaci obnovy v případě nákupu PC je stanoven na + 1 den.

Přezkoumání systému managementu

Vedení podniku MHK provádí v pravidelných intervalech přezkoumávání integrovaného systému. Cílem přezkoumávání IS je zajištění jeho přiměřenosti potřebám podniku, jeho kontinuita a efektivnost.

Vstup pro přezkoumání vedením zahrnuje informace o výsledcích auditů, zpětné vazbě od zákazníka, výkonnosti procesů a shodě produktu (stavební výroba), hodnocení souladu s právními požadavky, komunikace s externími stranami, environmentální profil podniku, stavu preventivních opatření a nápravných opatření, následných opatřeních z předchozích přezkoumání managementu, o změnách, které by mohly ovlivnit IS, o doporučeních pro zlepšování, přezkoumání aktuálnosti Politiky IS, cílů a cílových hodnot, vyhodnocení spoluúčasti a konzultace, výkonnost v oblasti BOZP, stav vyšetřovaných incidentů a informace o technikách, produktech nebo postupech vedoucích ke zlepšení ISMS. Tyto vstupy vyhodnocuje 1x ročně PV a MIS ve vstupní zprávě pro přezkoumání vedením. Podklady získává od pracovníků odpovědných za zpracování dílčích podkladů.

Přezkoumání vedením se účastní jednatelé, manažer integrovaného systému MIS a interní auditor. V rámci přezkoumání IS je přečtena zpráva PV o stavu IS za daný rok a jsou formulovány závěry a opatření, zejména rozhodnutí a opatření ke zlepšování efektivnosti IS a jeho procesů, ke zlepšování produktu ve vztahu k požadavkům zákazníka, opatření k potřebám zdrojů a vyjádření se ke změně Politiky IS, cílů a cílových hodnot a dalším prvkům EMS a SMS vzhledem k závazku k neustálému zlepšování. Výsledky přezkoumání IS jsou zaznamenány v zápisu z porady, odpovědnost za zpracování zápisu má MIS.

4.2.6 Evidence aktiv

Podnik MHK má stanovená pravidla pro evidenci aktiv. Jedná se o aktiva, která se v rámci systému řízení bezpečnosti informací systematicky evidují. Tento postup je závazný pro všechny pracovníky podniku, kteří jsou z výkonu své funkce povinni provádět evidenci aktiv.

V pravidelném intervalu stanoveném bezpečnostním manažerem je sestavován a aktualizován přehled aktiv, který obsahuje název aktiva, a jeho zatřídění do skupin v souladu s postupem „Rozsah aktiv“. Vlastníci aktiv jsou uvedeni v Analýze rizik. Sestavení přehledu aktiv provádí pověřený zaměstnanec. Přístup k aktivům se řídí na logické i fyzické úrovni. Popis logického řízení přístupu je předmětem postupu logického zabezpečení, řízení fyzického přístupu je předmětem postupu Popis fyzického zabezpečení. Tento postup pokrývá oblasti přístupu k aplikacím, operačním systémům počítačů, mobilním prostředkům a k počítačové síti.

4.2.7 Stupnice klasifikace informací

Podnik MHK používá dle tabulky 6 třístupňovou klasifikaci informací, kde stupeň udává míru důvěrnosti informace. Klasifikace informací respektuje hledisko DŮVĚRNOSTI. Podnik/zákazníci, ani další zainteresované strany neměly do současné doby požadavek na vyšší stupeň přístupů/ochrany informací (tajné, přísně tajné apod.).

Tabulka 6 Kvalifikační stupně podniku

Kvalifikační stupeň	**Slovní označení kvalifikačního stupně**
I. stupeň	veřejné informace
II. stupeň	neklasifikované informace
III. stupeň	neveřejné informace

Zdroj: Vlastní zpracování (2021)

Do I. klasifikačního stupně podnik zařazuje informace, které nejsou z hlediska důvěrnosti omezeny. Informace zařazené do tohoto klasifikačního stupně jsou určeny zaměstnancům podniku a dále veřejnosti. Způsob značení se provádí nápisem „veřejné informace“. Jsou to například informace poskytované na veřejných internetových stránkách podniku, marketingové publikace určené veřejnosti. Veřejné informace nepodléhají utajení. Pracovník podniku při předávání informací jinému subjektu, nebo při použití informace jako zdroje pro tvorbu dalších odvozených informací je povinen si ověřit, zda informace jsou v aktuální verzi.
Do II. klasifikačního stupně (neklasifikované informace) patří informace, které jsou z hlediska důvěrnosti určeny zaměstnancům podniku v souladu s jejich pracovní činností. Informace nejsou určeny pro veřejnost. Tyto informace a dokumenty jsou neoznačené. Příkladem jsou podnikové směrnice a předpisy, nařízení a příkazy ředitele atd. Pracovník podniku při předávání informací II. klasifikačního stupně jinému subjektu, nebo při použití informace jako zdroje pro tvorbu dalších odvozených informací je povinen si ověřit, zda jsou informace v aktuální verzi. Předání informací zajistí pracovník tak, aby informace byly dostupné pouze

oprávněným příjemcům. Poskytování informací cizím subjektům je možné pouze za podmínek, že cizí subjekt má s podnikem uzavřeny příslušné dohody o mlčenlivosti (o ochraně informací) a pracovník podniku je z výkonu své pracovní funkce oprávněn poskytnout informaci cizímu subjektu

Do III. klasifikačního stupně patří informace, které jsou z hlediska důvěrnosti určeny pouze pověřeným pracovníkům podniku. Jsou to například osobní údaje zaměstnanců, mzdové výměry, smlouvy. Způsob značení těchto dokumentů se provádí nápisem „neveřejné informace“. Pracovník podniku při předávání těchto informací jinému subjektu, nebo při použití informace jako zdroje pro tvorbu dalších odvozených informací je povinen si ověřit, zda jsou informace v aktuální verzi. Předání informací zajistí pracovník tak, aby informace byly dostupné pouze oprávněným příjemcům. Poskytování informací cizím subjektům je možné pouze za podmínek, že cizí subjekt má s podnikem uzavřeny příslušné dohody o mlčenlivosti, o ochraně informací a pracovník podniku je z výkonu své pracovní funkce oprávněn poskytnout informaci cizímu subjektu.

4.2.8 Stávající rizika/aspekty

Analýza rizik/aspektů je prováděna kombinovaným způsobem, formou konzultací s řídícími/odbornými pracovníky podniku, kteří jsou vybráni na základě požadavků subjektu provádějícího analýzu rizik/aspektů. Analytické práce zahrnují identifikaci a ohodnocení aktiv, odhad a ohodnocení zranitelnosti, určení pravděpodobnosti výskytu hrozeb ve vztahu ke zranitelnosti, určení dopadu ohrožení aktiva a výpočet koeficientu rizika pro jednotlivá aktiva. Účelem postupu pro provádění analýzy rizik je stanovit pravidla, na základě kterých je prováděna analýza rizik/aspektů v podniku. Tento postup je závazný pro všechny zaměstnance tohoto podniku, kteří jsou pověřeni provedením analýzy rizik/aspektů. Analýzu rizik provede subjekt (interní/externí osoby) určený vedením podniku v součinnosti s bezpečnostním manažerem. Bezpečnostní manažer je za provedení analýzy rizik odpovědný. V následující části bude přiblížen postup, jak s riziky pracují v podniku MHK. Jako zdroj je používán postup Řízení informačních rizik vypracovaný pro MHK.

Identifikace a ohodnocení aktiv

Pověření pracovníci podniku identifikují a hodnotí aktiva z hlediska nákladů na jejich pořízení a udržování a také z hlediska nepříznivých dopadů na činnost podniku plynoucí ze ztráty důvěrnosti, dostupnosti a integrity při ztrátě, zničení či neoprávněné modifikaci těchto

aktiv. Níže uvedená tabulka 7 určuje provázanost mezi hodnotou aktiva (číselně) a (slovním) ohodnocením dopadu ztráty bezpečnosti aktiva na fungování podniku.

Tabulka 7 Dopad ztráty bezpečnosti aktiva na fungování podniku

Hodnota aktiva	Dopad ztráty bezpečnosti aktiva na fungování podniku
1	velmi nízký
2	nízký
3	střední
4	vysoký
5	katastrofální

Zdroj: Vlastní zpracování (2021)

Odhad a ohodnocení zranitelností

Správné určení úrovně zranitelnosti (slabého místa) má velký význam, pro zhodnocení, jak je riziko závažné a jak rychle se jím musíme zabývat. Na základě pohovorů se zaměstnanci podniku a po prostudování existující dokumentace vztahující se k problematice bezpečnosti informací, jsou identifikovány existující zranitelnosti a odhadnuta snadnost jejich využití hrozbami. Hrozba a zranitelnost jsou oceněny v níže uvedené tabulce 8. Pověření pracovníci podniku identifikují potenciální hrozby a určí pravděpodobnost, s jakou se mohou vyskytnout.

Tabulka 8 Ocenění hrozby/zranitelnosti

Ocenění hrozby / zranitelnosti	Slovní ohodnocení
1	velmi malá
2	malá
3	střední
4	velká

Zdroj: Vlastní zpracování (2021)

Určení pravděpodobnosti výskytu hrozeb ve vztahu ke zranitelnosti

Velmi důležitým parametrem je pravděpodobnost výzkumu. Pověření pracovníci podniku identifikují potenciální hrozby a určí pravděpodobnost, s jakou se mohou vyskytnout ve vztahu ke zranitelnosti. Při hodnocení je použita hodnotící škála 1-5 s následujícím slovním vyjádřením pravděpodobnosti: 1 - nejnižší; 2 - nízká; 3 - střední; 4 - vysoká; 5 - nejvyšší.

Určení dopadu ohrožení aktiva

Pověření zaměstnanci podniku identifikují dopad ohrožení aktiva. Při hodnocení je použita hodnotící škála 1-5 s následujícím slovním vyjádřením pravděpodobnosti: 1 – velmi nízký; 2 - nízký; 3 - střední; 4 - vysoký; 5 - katastrofální.

Výpočet koeficientu rizika pro jednotlivá aktiva

Výpočet je stanoven násobkem pravděpodobnosti a hodnoty aktiva (dopadu). Pověření zaměstnanci podniku identifikují a hodnotí aktiva z hlediska nákladů na jejich pořízení a udržování a také z hlediska nepříznivých dopadů na činnost podniku plynoucí ze ztráty důvěrnosti, dostupnosti a integrity při ztrátě, zničení či neoprávněné modifikaci těchto aktiv. Pro aktiva ohodnocená 1 (s dopadem velmi nízký) není potřeba stanovovat míru rizika.

4.2.9 Identifikace rizik

Identifikace rizik v podniku MHK je první fází procesu řízení rizik. Vyhledávání nebezpečí probíhá následujícím způsobem. Pověření pracovníci podniku identifikují a hodnotí aktiva z hlediska nákladů na jejich pořízení a udržování a také z hlediska nepříznivých dopadů na činnost podniku plynoucí ze ztráty důvěrnosti, dostupnosti a integrity při ztrátě, zničení či neoprávněné modifikaci těchto aktiv. Identifikovaná aktiva podniku MHK jsou uvedeny v tabulce 9.

Tabulka 9 Identifikovaná aktiva v podniku

Identifikovaná aktiva v podniku	**Aktivum**
Informační aktiva	Databáze, systémová dokumentace, soubory dat, služby
SW aktiva a HW aktiva	Software včetně aplikací databází, operační systémy serverů, operační systémy pracovních stanic a notebooků, kancelářský SW (MS Office), účetní, personální a skladový systém, program pro projektování, rozpočtový program, bezpečnostní SW (firewall, antivirový SW), server, pracovní stanice administrátora, pracovní stanice – provoz, aktivní síťové prvky, UPS
Fyzická aktiva	Vybavení místností, média, kabeláž, komunikační zařízení
Lidské zdroje	Klíčoví pracovníci z pohledu zachování chodu podniku
Ostatní	Ostatní aktiva nezařazená do předchozích kategorií

Zdroj: Vlastní zpracování (2021)

Způsob evidence aktiv je v podniku MHK sestavován a aktualizován v pravidelném intervalu

stanoveném bezpečnostním manažerem. Seznam obsahuje název aktiva, jeho identifikační číslo a umístění. Vlastníkem všech aktiv je jednatel podniku. Sestavení přehledu aktiv (HW a SW) provádí pověřený pracovník – správce výpočetní techniky. V případě přidělení konkrétního HW a SW určité osobě je zaznamenáváno na předávacím protokolu, který je uložen v podniku a kopie u externího IT podniku. Kontrola správnosti je prováděna v pravidelném intervalu stanoveném bezpečnostním manažerem, minimálně však 1x ročně. Je prováděno srovnání přehledu aktiv (HW a SW) k určitému datu s evidencí majetku vedenou v účetním software ke stejnému datu. Srovnání provádí interní auditor systému řízení bezpečnosti informací.

Informační aktiva podniku

Přístup k informačním aktivům je řízen na logické i fyzické úrovni. Popis logického řízení přístupu je předmětem směrnice ISMS, řízení fyzického přístupu je předmětem postupu Popis fyzického zabezpečení. Tato směrnice pokrývá oblasti přístupu k aplikacím, operačním systémům počítačů, mobilním prostředkům a k počítačové síti.

Tabulka 10 Konkrétní případ informačního aktiva podniku MHK

Identifikace aktiva	Data v mobilních telefonech
Ohodnocení aktiva	2
Odhad hrozby	Únik informací, požár, falzifikace smluv
Ohodnocení zranitelnosti	Nedodržení bezpečnostních předpisů pro zacházení s daty ukládanými do mobilních telefonů, nedodržení bezpečnostních předpisů pro zacházení se smlouvami, nedostatečné protipožární zabezpečení, poškození image podniku
Určení pravděpodobnosti	1
Určení dopadu ohrožení života	2
Určení rizika	4
Návrh opatření	Úprava organizačně řídící dokumentace, vytvoření pravidel pro data v mobilních telefonech a stanovení odpovědnosti, nastavení stálého perimetru prověřování znalostí zaměstnanců s daty v mobilních telefonech

Zdroj: Vlastní zpracování (2021)

Konkrétní případ informačního aktiva podniku MHK je uveden ve výše uvedené tabulce 10.

Odpovědnost za definování přístupových práv je přiřazena přímému nadřízenému pracovníku. Existuje formální postup registrace a zrušení registrace uživatele před tím, než je přístupové oprávnění vytvořeno. Pro tento postup registrace má podnik zaveden v maximální možné míře standardizované uživatelské profily a definované požadované přístupové oprávnění pro každý uživatelský profil. Odpovědnost za definování přístupových práv je přiřazena vedoucím pracovníkům. Je dodržován formální postup registrace a zrušení registrace uživatele před tím, než je přístupové oprávnění vytvořeno. Nadřízený pracovník při registraci nového zaměstnance určí rozsah přístupových práv, které sdělí externímu IT podniku, systémový administrátor přístupová práva zavede, elektronicky potvrdí zavedení a potvrzení zašle všem zúčastněným a také v kopii na bezpečnostního manažera. Při odchodu zaměstnance platí podobný postup - nadřízený pracovník požádá o odebrání příslušných uživatelských oprávnění a zašle jej systémovému administrátorovi, který přístupová práva neprodleně zruší, zrušení elektronicky potvrdí a potvrzení zašle všem zúčastněným a také v kopii na bezpečnostního manažera. V případě změny přístupových práv se postupuje stejně.

V níže uvedené tabulce 11 jsou zjištěná informační aktiva podniku MHK s nejvyšším stupněm rizika.

Tabulka 11 Informační aktiva podniku s nejvyšší hodnotou rizika

Aktivum s nejvyšším stupněm	**Slabé místo aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami**
Data na serveru	Nedostatečné zabezpečení, prozrazení přístupových hesel administrátorů, krádež serveru, odposlech po lokální síti, nedostatečné prověření zaměstnanců, chybný zásah administrátora, chybný zásah uživatele, nedostatečně specifikovaná opatření, neautorizovaný přístup, selhání HW, selhání SW, zlomyslné kódy, nedostatečné zabezpečení, nedostatečné bezpečnostní podvědomí, neautorizovaný přístup, úmyslný zásah uživatele

Data na přenosných discích (externí výměnný disk, flash disk)	Nedostatečné zabezpečení přenosného zařízení proti krádeži / proti přečtení, nedostatečné povědomí zaměstnanců, nedostatečné zabezpečení přenosného zařízení proti krádeži / proti přečtení, nedostatečné povědomí zaměstnanců, nezabezpečený přístup
Zálohovaná data na CD a DVD nosičích	Nedostatečné zabezpečení přenosného zařízení proti krádeži / proti přečtení, nedostatečné povědomí zaměstnanců
Zálohovaná data na externím HDD	Nedostatečné zabezpečení úložných prostor, nedostatečné povědomí administrátora
Data (zdrojové kódy) přenášená na DVD nosičích od zákazníka	Nedostatečné zabezpečení přenosného zařízení proti krádeži / proti přečtení
Internet (UPC)	Nedostatečně zabezpečená sítě

Zdroj: Vlastní zpracování (2021)

Revize přístupových práv uživatelů informačních aktiv

Každý uživatel používá jednoznačný identifikátor (uživatelské ID - příjmení), aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti. Sdílení uživatelských ID není povoleno. Přístupová práva uživatelů jsou v podniku měněna nebo kontrolována dle potřeby. Zodpovědnost za provádění revize je přiřazena vlastníkům jednotlivých informačních aktiv. Případný nesoulad v přidělených přístupových právech se řeší požadavkem na změnu přístupových oprávnění u konkrétní osoby. Hesla zajišťují řádnou autentizaci uživatelů. Autentizace slouží k ověření identity uživatele a opravňuje uživatele k získání požadovaných služeb a přístupu k aplikacím a datům. Uživatelé odpovídají za volbu a ochranu svých hesel. Hesla jsou uchovávána v tajnosti, nesmí být vyzrazena dalším uživatelům, zapsaná na papíře, uložena v systémech apod. Uživatelé musí mít aktivován spořič obrazovky s požadavkem znovu zadání hesla při 30 minutové nečinnosti počítače. Zároveň musí svůj počítač zamykat spořičem obrazovky vyžadující heslo při vzdálení se od počítače. Při odchodu domů se uživatelé musí ze svého počítače odhlásit, nebo jej převést do režimu spánku (či podobného). Spuštění počítače po obnově z režimu spánku musí být požadováno obnovení přihlášení. Hesla musí být silná, délka hesla musí být nejméně 7 znaků, hesla musí obsahovat velká písmena (A až Z), musí obsahovat malá písmena (a až z), dále musí obsahovat čísla (0 až 9) a v poslední řadě musí obsahovat ne-alfanumerické znaky (např.!, $, #, %).

Systém musí vyžadovat změnu dočasně přiděleného hesla při prvním přihlášení. Uživatelský účet musí být uzamčen po 5 neúspěšných pokusech o přihlášení a automaticky odemknut po uplynutí 15 minut. Systém si musí pamatovat minimálně 5 posledních používaných hesel, aby nebylo možné se přihlašovat pod stejným heslem několikrát po sobě. Minimální doba, za kterou si uživatel může sám znovu změnit heslo, musí být 1 den.

Monitorování přístupu k systému a jeho použití

Monitorování aktivit uživatelů se provádí z důvodu získání důkazů pro případ výskytu bezpečnostního incidentu. Auditní záznamy připravuje externí podnik (vzhledem k outsourcingu IT služeb) a předává je bezpečnostnímu manažerovi podniku k vyhodnocení. Tento proces probíhá dle potřeby. Auditní záznamy musí být uchovávány dostatečně dlouhou dobu a musí obsahovat identifikátory uživatelů (uživatelská ID), datum a čas přihlášení a odhlášení, záznam o úspěšných a odmítnutých pokusech o přístup k systému, použití privilegovaných účtů, záznam o úspěšných a odmítnutých pokusech o přístup k datům a jiným zdrojům a změny systémové konfigurace.

SW aktiva a HW aktiva

V pravidelném intervalu stanoveném bezpečnostním manažerem je sestavován a aktualizován přehled aktiv (HW a SW), který obsahuje název aktiva, a jeho zatřídění do skupin v souladu s postupem „Rozsah aktiv“. Vlastníci aktiv jsou uvedeni v Analýze rizik. Sestavení přehledu aktiv (HW a SW) provádí pověřený zaměstnanec (bezpečnostní manažer ve spolupráci se správcem výpočetní techniky). V případě přidělení konkrétního HW a SW určité osobě je zaznamenáváno na předávacím protokolu, který je uložen v podniku. Kontrola správnosti je prováděna v pravidelném intervalu stanoveném bezpečnostním manažerem, kde je prováděno srovnání přehledu aktiv (HW a SW) k určitému datu s evidencí majetku vedenou v účetním software ke stejnému datu. Srovnání provádí bezpečnostní manažer. V níže uvedené tabulce 12 jsou zjištěná SW a HW aktiva podniku MHK s nejvyšším stupněm rizika.

Tabulka 12 SW aktiva a HW aktiva podniku s nejvyšší hodnotou rizika

Aktivum s nejvyšším stupněm	**Slabé místo aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami**
Operační systémy a ostatní programy	Nedostatečné bezpečnostní povědomí, viry, trojany, nenainstalování antivirových programů, poškození na HW, nedodržení licenční politiky, nestahování potřebných aktualizací a záplat

Zdroj: Vlastní zpracování (2021)

Fyzická aktiva

Fyzická aktiva podniku jsou vyhodnocena na základě popisu fyzického zabezpečení. Účelem postupu je stanovení pravidel klíčového hospodářství a fyzického přístupu do objektů a vybraných prostor podniku. Tento postup je závazný pro všechny pracovníky podniku. Prostory podniku jsou v třípodlažní administrativní budově, která se nachází v Hradci Králové. Budova je uzavřena na vchodu a dále každé patro samostatně. Pracovníci oprávnění vstupovat do jednotlivých podlaží mají svá přístupová hesla, která je pustí pouze do toho podlaží, kam mohou vstupovat. Objekt je střežen kamerovým systémem s napojením na pult centrální ochrany. Toto zajišťuje externě zajištěný podnik (podloženo smlouvou). V níže uvedené tabulce 13 je uveden konkrétní příklad fyzického aktiva podniku MHK.

Tabulka 13 Konkrétní případ fyzického aktiva podniku MHK

Identifikace aktiva	Budova provozovny
Ohodnocení aktiva	5
Odhad hrozby	Krádež, vykradení
Ohodnocení zranitelnosti	Nedostatečné zabezpečení
Určení pravděpodobnosti	2
Určení dopadu ohrožení života	5
Určení rizika	10
Návrh opatření	Úprava organizačně řídící dokumentace, vytvoření pravidel pro zabezpečení budovy a stanovení odpovědnosti.

Zdroj: Vlastní zpracování (2021)

Přístup do budovy je zajištěn klíčem a EZS. Pracovník podniku, který má právo odemykat a zamykat objekt, je vybaven odpovídajícím klíčem budovy a kódem EZS. Pracovník podniku je při odchodu z objektu povinen provést kontrolu přítomnosti ostatních pracovníků. Pokud je posledním pracovníkem je povinen budovu uzamknout a uvést v činnost EZS - uzamčení.
Pokud je uživatel po odemčení budovy upozorněn na status uzamčeno (akustický signál), zadá neprodleně přidělený kód a změní EZS do stavu odemčeno. Pokud je zadán chybný kód může uživatel svůj pokus opakovat. V takovém případě stiskne tlačítko CLEAR a poté vloží celý kód znovu. Pokud je kód zadán opět nesprávně a EZS aktivuje poplach, je pracovník podniku povinen okamžitě kontaktovat bezpečnostního manažera.

Pokud uživatel opouští budovu, ve které se nenacházejí žádné další osoby je povinen uvést

před uzamčením budovy EZS do stavu uzamčeno. Provede kontrolu uzavření všech bezpečnostních zón (světelný signál), zadá kód (potvrzeno akustickým signálem) a neprodleně opustí a uzamkne budovu. Pokud pracovník zjistí, že je některá bezpečnostní zóna otevřena a není schopen ji samostatně uzavřít (zóna se nachází v místnosti, kam nemá přístup) je povinen uvědomit o tom bezpečnostního manažera.

Vstup do jednotlivých kanceláří je zajištěn prostřednictvím klíčů. Pohyb cizích osob v kancelářích bez doprovodu pracovníka podniku je zakázán. Pracovníci podniku, kteří svou pracovní činnost vykonávají v této lokalitě, případně další osoby, se kterými jsou uzavřeny příslušné smlouvy, mohou disponovat klíči ke vstupu. Klíče jsou přiděleny jednotlivým pracovníkům oproti podpisu, evidence je vedena u personalistky. Klíčová politika je vedena prostřednictvím záznamů Klíčové hospodářství a Předávací protokol klíče. Záznam Klíčové hospodářství obsahuje přehled místností, které podléhají tzv. režimu povinného zamykání a přehled pověřených pracovníků, kteří smějí přistupovat do dané místnosti (resp. seznam klíčů, které jednotliví pracovníci převzali). Na základě těchto informací jsou v tabulce 14 zjištěná fyzická aktiva podniku s nejvyšší hodnotou rizika.

Tabulka 14 Fyzická aktiva podniku s nejvyšší hodnotou rizika

Aktivum s nejvyšším stupněm	**Slabé místo aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami**
Server	Stáří, výpadek HW, živelná pohroma, lidský faktor, nedostatečné preventivní požární opatření
Budova provozovny	Nedostatečné zabezpečení

Zdroj: Vlastní zpracování (2021)

Přístup k serveru a aktivním síťovým prvkům je povolen pouze oprávněným pracovníkům, resp. osobám, kteří mají uzavřenu příslušnou smlouvu o správě těchto zařízení. Místnost s umístěnými servery a aktivními síťovými prvky podléhá režimu povinného zamykání.

Lidské zdroje

Lidské zdroje v podniku MHK představují prostředky vyčleněné na systematické zvyšování kvality v souladu s politikou a cíli, a to zejména v oblastech personálních, investičních a informačních. V oblasti personální jde především o přijímání pracovníků a externích spolupracovníků s odpovídajícími kvalifikačními předpoklady, podpora neustálého vzdělávání a školení pracovníků. V oblasti investiční se jedná o modernizaci počítačového

vybavení, modernizaci komunikačních prostředků, autoparku, internetových stránek, reklamy. V oblasti informační se jedná zejména o internet a média. Kvalifikační personální požadavky představují souhrn požadovaných znalostí, vědomostí, schopností, dovedností a případně dalších specifikovaných znalostí potřebných pro výkon dané pracovní funkce. Těmito požadavky se řídí přijetí všech nových pracovníků. Všichni pracovníci (i externí), jejichž pracovní činnost může mít dopad na životní prostředí, bezpečnost a ochrany zdraví při práci nebo ISMS musí být seznámeni s riziky a dopady práce, kterou vykonávají. Konkrétní příklad aktiva lidských zdrojů podniku MHK je uveden v níže uvedené tabulce 15.

Tabulka 15 Konkrétní příklad aktiva lidských zdrojů podniku MHK

Identifikace aktiva	Obchodní partneři klíčoví
Ohodnocení aktiva	4
Odhad hrozby	Nedostupnost, porušení smluvních závazků, odstoupení od smlouvy
Ohodnocení zranitelnosti	Zpomalení efektivnosti našich procesů, ohrožení provozu systémů, ohrožení efektivnosti našich procesů, ohrožení činností podniku
Určení pravděpodobnosti	1
Určení dopadu ohrožení života	4
Určení rizika	4
Návrh opatření	Úprava organizačně řídící dokumentace, vytvoření pravidel pro tvorbu smluv a stanovení odpovědnosti, nastavení stálého perimetru prověřování znalostí zaměstnanců s nakládáním dat a informací obchodních klíčových partnerů

Zdroj: Vlastní zpracování (2021)

Personalistka podniku MHK provádí kontrolu realizace školení, sleduje termíny platnosti absolvovaného výcviku. Závěry z této činnosti pak promítne do plánu školení. Společná školení se realizují za účasti všech pracovníků. Na těchto školeních jsou doplňovány znalosti z obecně závazných předpisů a legislativních předpisů dotýkajících se aktivit podniku. Pracovníci, pro jejichž činnosti je nutná odborná způsobilost či oprávnění, se účastní příslušných odborných školení k získání či obnovení tohoto oprávnění. V případě zjištěných nedostatků uplatní školený pracovník stížnost u MIS. Nadřízený školeného je povinen se

přesvědčit (pohovorem, přezkoušením či testem), zda bylo výcvikem dosaženo plánovaných záměrů. Hodnocení efektivnosti školení, využití získaných zkušeností v praxi provádí 1x ročně personalistka.

Všichni pracovníci, jejichž pracovní činnost může mít dopad na životní prostředí a BOZP, musí mít povědomí o registru rizik a dopadech vykonávané práce. Externí pracovníci dostávají k podpisu „Pokyny pro dodavatele“ včetně „Registru EA“ a Registru rizik. Je tedy nezbytné, aby jejich pracovní činnosti předcházela odborná příprava zaměřená na tuto oblast. Prokazatelnost naplnění tohoto požadavku je zajištěna tak, že každý pracovník musí být odpovídajícím způsobem proškolen, aby mohl minimalizovat nebo předcházet možným negativním environmentálním dopadům, které vyplývají z jeho činnosti, rizikům BOZP. Současně je pracovník poučen o následných opatřeních ke zmírnění vzniklých následků havárií a nehod nebo na ochranu ŽP a BOZP. Pracovníci provádějící úkony, které mohou mít významné environmentální dopady či rizika BOZP, musí být k tomu způsobilí na základě odpovídajícího vzdělání, výcviku a zkušeností. Na základě těchto získaných informací jsou v tabulce 16 vypsána zjištěná fyzická aktiva podniku s nejvyšší hodnotou rizika.

Tabulka 16 Aktiva lidských zdrojů podniku s nejvyšší hodnotou rizika

Aktivum s nejvyšším stupněm	**Slabé místo aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami**
Jednatel podniku	Nezastupitelnost v provádění finančních operací, nezastupitelnost v jednání za podnik
Zákazníci	Zneužití dodané služby, poškození know-how podniku

Zdroj: Vlastní zpracování (2021)

4.2.10 Identifikace rizik plynoucích z přístupu třetích stran

Fyzický nebo logický přístup třetí strany k aktivům podniku MHK nemůže být povolen dříve, dokud nejsou zvážena všechna rizika, která mohou tato aktiva ohrozit. Identifikovaná rizika plynoucí z přístupu třetích stran musí být pokryta odpovídajícími opatřeními. Přístup třetích stran musí být schválen bezpečnostním manažerem, který odpovídá za vyhodnocení možných rizik a návrh opatření na snížení těchto rizik a musí o tom existovat písemný doklad (např. smlouva).

4.2.11 Hodnocení rizik

Pro hodnocení rizik je v MHK používána škála vysoká úroveň rizika, střední úroveň rizika a nízká míra rizika. Vysoká úroveň rizika při výsledné hodnotě 21 – 25 vyžaduje urychlené přijetí nápravných opatření. Střední úroveň rizika při výsledné hodnotě 16 – 20 jsou ta rizika, kterými je potřeba se zabývat po odstranění vysokých rizik. Nízká úroveň rizika při výsledné hodnotě 1 – 15 jsou rizika akceptovatelná, není potřeba implementovat nápravné opatření.
Míra rizika byla vypočítávána pro každé identifikované aktivum zvlášť. Z výsledků analýzy rizik vyplývá, že mezi nejvíce ohrožená aktiva patří informační aktiva, fyzická aktiva a lidské zdroje z pohledu vrcholového vedení podniku.

4.2.12 Přehodnocení rizik

Vysoká a střední rizika nejsou v podniku MHK identifikována. Všechna ohodnocená aktiva jsou zařazena do úrovně **nízká úroveň rizika** s maximálním bodovým ohodnocením 15. V níže uvedené tabulce 17 jsou aktiva ohodnocená bodem 15.

Tabulka 17 Maximální ohodnocená aktiva

INFORMAČNÍ AKTIVA		
Aktivum	**Hrozba**	**Zranitelnosti**
Data na serveru	Krádež dat zvenku	Prozrazení přístupových hesel
	Zničení / ztráta záznamů	Chybný zásah administrátora Chybný zásah uživatele Zlomyslné kódy
FYZICKÁ AKTIVA		
Aktivum	**Hrozba**	**Zranitelnosti**
PC a notebooky zaměstnavatele		Výpadek HW
Server		Výpadek HW
LIDSKÉ ZDROJE		
Aktivum	**Hrozba**	**Zranitelnosti**
Jednatel podniku zaměstnavatele	Neschopnost provádět finanční operace	Nezastupitelnost v provádění finančních operací
Server		Výpadek HW

Zdroj: Vlastní zpracování (2021)

4.2.13 Vyhodnocení rizik

Z výsledků analýzy rizik je patrné, že v podniku existují rizika, která jsou možná akceptovat a je potřeba se jimi zabývat, ať už v krátkodobém (vysoká úroveň rizika) či dlouhodobém (střední úroveň rizika) horizontu. Všechna ohodnocená aktiva jsou zařazena do nízké úrovně rizika s maximálním bodovým ohodnocením 15. Nízká úroveň rizika při výsledné hodnotě 1 – 15 jsou rizika akceptovatelná, není potřeba implementovat nápravná opatření a navrhovat možná řešení na snížení rizik. Tato rizika však musí být neustále sledována, aby zůstala pod hranicí přijatelnosti. Veškerá zjištěná aktiva podniku MHK jsou uvedena v příloze 2 této diplomové práce.

4.2.14 Identifikace nových rizik informační bezpečnosti

Identifikace nových rizik informační bezpečnosti a plánování reakcí na tyto situace, probíhá v rámci výstupu interních auditů podniku MHK. Dle výstupu z posledního auditu, nejsou stanoveny nové pracovní postupy, není tedy v současné době nutnost identifikovat nová rizika informační bezpečnosti. Účelem tohoto postupu je stanovit pravidla pro nová rizika, která vycházejí z nových pracovních činností a postupů a pro vytváření ošetření rizik v podniku MHK. Tento postup je závazný pro všechny pracovníky podniku, kteří jsou pověřeni sestavováním Plánu ošetření rizik.

4.2.15 Neustálé zlepšování

Z předložené politiky integrovaného systému podniku MHK, příruček a předložené dokumentace vyplývá neustálé zlepšování efektivity zavedeného integrovaného systému podniku MHK. Podnik MHK neustále zlepšuje efektivnost zavedeného integrovaného systému, a to prostřednictvím nových cílů a cílových hodnot, výsledků auditů, analýzy údajů, opatření k nápravě, preventivních opatření a přezkoumání managementu.

5 Zhodnocení výsledků a návrhy opatření

5.1 Zhodnocení výsledků

V rámci přezkoumání integrovaného systému podniku, které proběhlo v rámci interního auditu, a předložených podkladů manažerem integrovaného systému můžeme zhodnotit, že systém managementu je způsobilý plnit aplikovatelné požadavky a dosahovat očekávaných výsledků. Systém je nastaven optimálně, je třeba ho i nadále udržovat, především seznamovat pracovníky se všemi povinnostmi a dodržování kontrolovat i mimo termíny interních auditů. Podnik má integrovaný systém zastřešen jedním pracovníkem, manažerem integrovaného systému řízení. Politika integrovaného systému odpovídá záměrům podniku, zahrnuje osobní angažovanost a aktivitu při plnění požadavků a neustálé zlepšování efektivnosti IS. V politice integrovaného systému, však není zahrnut soulad s GDPR.

Podnik prokázal, že má dostatek kvalifikovaných pracovníků k zajištění realizace procesů Organizační struktura a rozdělení odpovědnosti respektují všechny komponenty integrovaného systému řízení. Podnik má zdroje pro řízení a zabezpečování procesů. K řízení podniku je využívána dokumentace, která je souborem všech interních a externích dokumentů a záznamů, nezbytných k řízení podniku. Základním interním řízeným dokumentem je příručka IS a dále pak další navazující záznamy a dokumenty.

Pro sledování aktuálních právních požadavků má podnik vytvořen Registr právních a jiných požadavků, který je tvořen zákony, vyhláškami, nařízeními a dalšími legislativními předpisy z oblasti ochrany životního prostředí a bezpečnosti a ochrany zdraví při práci. Tyto požadavky jsou důsledně sledovány přes internet.

Kontrola, zkoušení a měření jsou neoddělitelnou součástí výrobních procesů v tomto podniku a jsou podkladem pro vyhodnocování IS. Podnik v pravidelných intervalech monitoruje, prověřuje a vyhodnocuje procesy včetně realizace procesů interních auditů a přezkoumání systému managementu. Posuzované procesy jsou realizovány ve shodě se stanovenými požadavky. Závěry se využívají pro plánování kontrolních operací, s cílem zabezpečení shody a neustálého zlepšování činností souvisejících s produktem a procesem. V oblasti procesů vývoje a podpory nebyla předložena pravidla pro penetrační testy na přístup do serverů.

Přezkoumávání integrovaného systému provádí vedení podniku v pravidelných intervalech. Cílem přezkoumávání IS je zajištění jeho přiměřenosti potřebám podniku, jeho kontinuita a efektivnost. V rámci přezkoumání tohoto interního auditu nebyla formulována opatření ani

rozhodnutí a opatření ke zlepšování efektivnosti integrovaného systému, vyplynula pouze zjištění, která nemají na chod integrovaného systému žádný vliv.

Shrnutí

Na základě provedeného přezkoumání integrovaného systému a zhodnocení systému řízení bezpečnosti informací v rámci integrovaného systému řízení ve vybraném podniku byla shledána následující zjištění:

- **v politice integrovaného systému není zahrnut soulad s GDPR;**
- **v oblasti procesů vývoje a podpory nebyla předložena pravidla pro penetrační testy na přístup do serverů;**
- **v oblasti rizik bezpečnosti informací, byla v podniku identifikována rizika s nízkou úrovní rizika bezpečnosti.**

5.2 Navrhovaná opatření

Soulad dokumentace s GDPR

V rámci přezkoumání bezpečnostní politiky integrovaného systému podniku, vyplynulo zjištění chybějícího souladu s požadavky GDPR. Politika je aktuální a přiměřená podniku, zahrnuje požadované normativní body, není zde však zahrnut soulad s GDPR. Podnik opatření realizoval pouze samostatnou příručkou a certifikátem GDPR. Podnik by měl zvážit rozšíření dokumentu Politika ISMS o prohlášení k souladu s požadavky GDPR, případně Kybernetického zákona. Organizačním návrhem je přítomnost jednoho specialisty v podniku, který by komplexně zabezpečoval a zajišťoval soulad dokumentace s GDPR. Tento specialista by byl nucen soustavně dohlížet na zapracování, kontrolu a aktualizaci všech dokumentů týkající se GDPR. Hodinová sazba specialisty pro GDPR se zpravidla pohybuje okolo 1 000 – 1 500 Kč. Při předpokladu minimálně 5 návštěv podniku, kdy jedna návštěva včetně občasného školení a poradenství zabere přibližně 5 hodin, a při kalkulaci 1 250 Kč za 1 hodinu práce specialisty, budou celkové finanční náklady činit 31 250 Kč.

Pravidla pro penetrační testy na přístup do serverů

V oblasti procesů vývoje a podpory nebyla předložena pravidla pro penetrační testy na přístup do serverů. Cílem penetračních testů je odhalení zranitelností cílového informačního systému, stanovení způsobu jejich možného využití a doporučení vedoucí k jejich nápravě. V rámci zabezpečení informací by bylo vhodné zvážit vytvoření přesných pravidel pro procesy. Pro vytvoření těchto pravidel je pro podnik MHK nejvýhodnější oslovení bezpečnostního správce

se kterým spolupracuje. Ten již připomínkuje aplikaci opatření z hlediska použitých technologií, řeší bezpečnostní události a zajišťuje informační bezpečnost z technického hlediska. Hodinová sazba bezpečnostního správce je dána smlouvou, kterou má s podnikem MHK uzavřenou a kde je zahrnuta i sazba mimořádných bezpečnostních informačních událostí, pod kterou se zpracování těchto pravidel může zahrnout. Při předpokladu 5 hodin práce a při kalkulaci 1 500 Kč za 1 hodinu práce, budou celkové finanční náklady činit 7 500 Kč.

Dále by bylo vhodné postoupit penetrační testy na přístup do sítě a záložních zdrojů. Nejlepším řešením by bylo přijetí opatření antiviru ESET NOD 32, který průběžně operační systémy aktualizuje. Jedna licence tohoto antiviru stojí 999 Kč, při zakoupení 10 licencí (což je pro podnik dostačující) je cena 8 800 Kč. V ceně licence jsou standardně zahrnuty aktualizace. Během platnosti licence může majitel stahovat virové i programové aktualizace z Internetu, popřípadě tuto činnost ponechat přímo na k tomu určeném modulu zakoupeného software společnosti ESET.

Rizika s nízkou úrovní rizika bezpečnosti

V oblasti rizik bezpečnosti informací, nebyla v podniku MHK identifikována vysoká a střední rizika. V rámci vyhodnocení analýzy rizik je patrné, že v podniku existují rizika, která je možné akceptovat a je potřeba se jimi zabývat, ať už v krátkodobém (vysoká úroveň rizika) či dlouhodobém (střední úroveň rizika) horizontu. Z výsledků analýzy rizik vyplývá, že mezi nejvíce ohrožená aktiva patří informační aktiva, fyzická aktiva a lidské zdroje z pohledu vrcholového vedení podniku. Všechna ohodnocená aktiva jsou zařazena do nízké úrovně rizika s maximálním bodovým ohodnocením 15. Nízká úroveň rizika při výsledné hodnotě 1 – 15 jsou rizika akceptovatelná, není potřeba implementovat nápravná opatření a navrhovat možná řešení na snížení rizik. Tato rizika však musí být neustále sledována, aby zůstala pod hranicí přijatelnosti. Pokud budou v podniku identifikována aktiva, která budou zařazena do vysoké úrovně s bodovým ohodnocením nad 15, musí se navrhnout řešení na snížení těchto rizik. Řešení spočívá ve vytvoření nových opatření k eliminaci potenciálních škod u zjištěných rizik, jež by v případě realizace hrozby mohly nastat. Musí být provedeno přezkoumání celého procesu řízení rizik, zejména identifikace a ohodnocení rizik. Dále musí být provedena aktualizace posouzení dopadu rizik, což zahrnuje identifikaci hrozeb a zranitelnosti a rovněž nové posouzení pravděpodobnosti dopadů těchto hrozeb. Na základě výsledných hodnot, by byla provedena eliminace potenciálních škod.

V podniku MHK jsou vytvářeny procesem řízení bezpečnosti informací předpoklady pro běžný provoz a pro maximální výkon zaměstnanců podniku. Je zde velmi důležitá činnost bezpečnostního manažera podniku, který je povinen dodržovat zákony, vyhlášky, normy a vnitřní předpisy a směrnice zaměstnavatele. Pro minimalizaci rizika, má velký význam systematická kontrola všech pracovních činností, proto bych doporučila při celkovém počtu 180 kmenových zaměstnanců MHK přijmout dalšího specialistu, který by se zaměřil pouze na rizika v této oblasti.

6 Závěr

Tato diplomová práce se zabývá jednou z nejdůležitějších činností, kterou se musí každý podnik v dnešní době zabývat. Proces řízení bezpečnosti informací je založen na stanovené posloupnosti činností pracujících zejména s riziky, kde řízení rizik je nejdůležitější součástí procesu bezpečnosti informací. Součástí procesu, který zahrnuje identifikaci, analýzu, vyhodnocení, kontrolování všech rizik, je rozhodovací proces, vycházející z analýzy rizika. Pro úspěšné fungování podniku je nezbytné, aby byla rizika průběžně identifikována a efektivně řízena. Fungování systému řízení bezpečnosti informací, řízení rizik a jeho efektivita v podniku MHK, byly v rámci této diplomové práce podrobeny analýze.

Hlavním cílem diplomové práce bylo zhodnotit systém řízení bezpečnosti informací v rámci integrovaného systému řízení ve vybraném podniku a v případě zjištěných nedostatků navrhnout vhodná opatření.

V první části mé diplomové práce byla představena na základě studia odborné literatury, ISO norem a standardů řízení rizik, teoretická východiska. Byl definován informační systém a jeho základní znaky, včetně normy systému řízení bezpečnosti informací. Podrobně byl představen celý systém řízení bezpečnosti informací. Detailně byl představen proces řízení rizik, který pomáhá eliminovat účinek nežádoucích vlivů, a naopak umožňuje využít příležitosti působení pozitivních vlivů.

V praktické části v kapitole Vlastní práce byl představen a charakterizován podnik MHK, který byl pro analýzu procesu řízení bezpečnosti informací vybrán. Na základě účasti interních auditů podniku a osobních rozhovorů s manažerem integrovaného systému, byla přestavena zjištění funkčnosti integrovaného systému. Byly předloženy interní směrnice, příručky a další dokumenty, ze kterých vyplývá soulad integrovaného systému včetně souladu s normou systému řízení bezpečnosti informací. Interní auditorce byly předloženy otázky týkající se fungování systému, na základě kterých byla provedena analýza integrovaného systému podniku a procesu řízení bezpečnostních rizik.

Z výsledků výzkumu provedeného v podniku MHK vyplynulo, že systém řízení bezpečnosti informací v rámci přezkoumání integrovaného systému podniku, je způsobilý plnit aplikovatelné požadavky a dosahovat očekávaných výsledků. Na základě provedeného přezkoumání integrovaného systému ve vybraném podniku sice byla shledána zjištění, avšak ta nemají na chod systému žádný vliv. Systém je nastaven optimálně, je třeba ho i nadále udržovat.

V oblasti rizik bezpečnosti informací, nebyla v podniku MHK identifikována vysoká a střední rizika. V rámci vyhodnocení analýzy rizik je patrné, že v podniku existují rizika, která jsou možná akceptovat a je potřeba se jimi zabývat, ať už v krátkodobém či dlouhodobém horizontu. Z výsledků analýzy rizik vyplývá, že mezi nejvíce ohrožená aktiva patří informační aktiva, fyzická aktiva a lidské zdroje z pohledu vrcholového vedení podniku. Všechna ohodnocená aktiva jsou zařazena do nízké úrovně rizika s maximálním bodovým ohodnocením 15. Nízká úroveň rizika při výsledné hodnotě 1 – 15 jsou rizika akceptovatelná, není potřeba implementovat nápravná opatření a navrhovat možná řešení na snížení rizik. Tato rizika však musí být neustále sledována, aby zůstala pod hranicí přijatelnosti.

Na základě zhodnocení systému řízení bezpečnosti informací v rámci integrovaného systému řízení ve vybraném podniku, vyplynula pouze zjištění, která nemají na chod integrovaného systému žádný vliv. Systém je nastaven optimálně, je třeba ho i nadále udržovat.

7 Seznam použitých zdrojů

(1) SMEJKAL, Vladimír a RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích.* Praha: Grada Publishing, 2006, 296s. ISBN 80-247-1667-4.

(2) DOUCEK, Petr, NOVÁK Luděk, NEDOMOVÁ Lea a SVATÁ Vlasta. *Řízení bezpečnosti informací, Druhé rozšířené vydání o BCM.* Praha: Professional Publishing. 2011, 286 s. ISBN 978-80-7431-050-8.

(3) KNÝ, Milan a POŽÁR Josef. *Aktuální pojetí a tendence bezpečnostního managementu a informační společnosti.* Brno: Tribun EU s.r.o., 2010, 128 s. ISBN 978-80-7399-067-1.

(4) ONDRÁK, Viktor, SEDLÁK Petr, MAZÁLEK Vladimír. *PROBLEMATIKA ISMS V MANAŽERSKÉ INFORMATICE.* Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM, s.r.o.. 2013, 377 s. ISBN 978-80-7204-872-4.

(5) PALEČEK, Miloš a kol. *PREVENCE RIZIK*. Praha: VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE. Fakulta podnikohospodářská. 2006, 257 s. ISBN 80-245-1117-7.

(6) NQA Globální certifikační orgán. *Integrované systémy managementu* [online]. 2020. [cit. 2020-08-30]. Dostupné z: https://www.nqa.com/cs-cz/certification/systems/integrated-management-systems.

(7) ČSN ISO/IEC 27001. *Dokumentace - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

(8) SMEJKAL, Vladimír, SOKOL Tomáš, KODL Jindřich. *BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ podle zákona o kybernetické bezpečnosti.* Plzeň: Aleš Čeněk, 2019, 378 s. ISBN 978-80-7380-765-8.

(9) EUNICS-CZ. Národní sdružení Evropské organizace pro Univerzitní Informační Systémy. *Bezpečnostní politika IS.* Plzeň: Západočeská univerzita v Plzni. 2007, 78 s. ISBN 978-80-7043-554-0.

(10) NEZMAR, Luděk. *GDPR PRAKTICKÝ PRŮVODCE IMPLEMENTACÍ.* Praha: GRADA Publishing, a.s.. 2017, 301 s. ISBN 978-80-271-0920-3.

(11) POŽÁR, Josef. *Informační bezpečnost, vysokoškolská učebnice.* Plzeň: Aleš Čeněk. 2015, 309 s. ISBN 80-86898-38-5.

(12) ČERMÁK, Miroslav. Strategie informační bezpečnosti. [online]. 2013. [cit. 2020-08-24]. Dostupné z: WWW: https://www.cleverandsmart.cz/strategie-informacni-bezpecnosti/.

(13) SMEJKAL, Vladimír, RAIS Karel. *Řízení rizik ve firmách a jiných organizacích.* Třetí, rozšířené a aktualizované vydání. Praha: Grada Publishing. 2010, 354 s. ISBN 978-80-247-3051-6.

(14) XEVOS Solutions s.r.o. *Analýza současného stavu.* [online]. 2020. [cit. 2020-11-30]. Dostupné z: WWW: https://www.xevos.eu/sluzby/cyber-security/konzultacni-sluzby/.

(15) MINAŘÍK, Pavel, LACINA, Petr, VONDRÁČEK Lukáš, MIKŠOVIČ Petr, LINKE Petr. *KYBERNETICKÁ BEZPEČNOST* [online]. 2015. [cit. 2020-08-30]. Dostupné z: WWW: http://elearning.kybernetickabezpecnost.eu/files/download/program-1/demo-verze/vmkz-kap-1-2-demo.pdf/.

(16) HANÁČEK Petr, STAUDEK Jan. *BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ. Metodická příručka.* Praha: Úřad pro státní informační systém. 2000, 127 s. ISBN 80-238-5400-3.

(17) POŽÁR Josef, NOVÁK Luděk. *Systém řízení informační bezpečnosti.* [online]. 2020. [cit. 2020-07-27]. Dostupné z: WWW: https://www.cybersecurity.cz/data/SRIB.pdf.

(18) ICZ a.s. *Řízení bezpečnosti informací ISMS*. [online]. 2020. [cit. 2020-07-27]. Dostupné

z: WWW: https://www.iczgroup.com/wp-content/uploads/2017/ 08/ICZ_PL_SEC_ISMS _CZ _1506_01.pdf.

(19) MHK s.r.o. Hradec Králové. *Směrnice ISMS.* 2020. vyd. Hradec Králové

(20) ČERMÁK, Miroslav. *Řízení informačních rizik v praxi.* Brno: Tribun EU, 2009, 134 s. Knihovnicka.cz. ISBN 978-80-7399-731-1.

(21) MHK s.r.o. Hradec Králové. *Registr aspektů.* 2020. vyd. Hradec Králové.

(22) MHK s.r.o. Hradec Králové. *Příručka integrovaného systému*. 2020. vyd. Hradec Králové.

(23) POŽÁR Josef. *Vybrané hrozby informační bezpečnosti organizace*. [online]. 2021. [cit. 2021-02-13]. Dostupné z : WWW: https://www.cybersecurity.cz/data/Pozar2.pdf.

(24) PERSONALISTA. *Krádež firemních dat a infikace malwarem patří mezi největší hrozby pro digitální firmy.* [online]. 2021. [cit. 2021-02-13]. Dostupné z: WWW:

https://www.personalista.com/technologie/kradez-firemnich-dat-a-infikace-malwarem-patri-mezi-nejvetsi-hrozby-pro-digitalni-firmy-v-roce-2019.html.

(25) KOVACICH, Gerald L. *Průvodce bezpečnostního pracovníka informačních systémů: zavádění a prosazování bezpečnostní politiky informačních systémů.* Brno: UNIS Publishing, 2000, 200s. ISBN 80-86097-42-0.

(26) Alexander Sophoclis Pieri. *Accenture and HfS Research release study on threats to digital business.* [online]. 2020. [cit. 2020-12-08]. Dostupné z: WWW: https://www.itp.net/608341-accenture-and-hfs-research-release-study-on-threats-to-digital-business.

8 Přílohy

Seznam příloh

Příloha 1 Seznam otázek pokládaných bezpečnostnímu manažerovi podniku

Příloha 2 Identifikovaná aktiva bezpečnosti informací podniku

Příloha 3 Přehled skupin aktiv bezpečnosti informací

Příloha 1 Seznam otázek položených bezpečnostnímu manažerovi podniku

1. Jaká je charakteristika a struktura Vašeho podniku?
2. Dle kterých systémů má Váš podnik zavedený integrovaný systém?
3. Máte vytvořenou politiku integrovaného systému?
4. Jakým způsobem plánujete, udržujete a zlepšujete integrovaný systém?
5. Jakým způsobem ochraňujete v podniku dokumenty, záznamy a data k řízení podniku a integrovaného systému?
6. Jakým způsobem dodržujete a udržujete všechny právní i jiné požadavky, související s integrovaným systémem řízení?
7. Jakým způsobem monitorujete a zlepšujete procesy integrovaného systému?

Příloha 2 Identifikovaná aktiva bezpečnosti informací podniku

Informační aktiva

V níže uvedené tabulce jsou identifikována informační aktiva.

Tabulka 18 Informační aktiva

AKTIVUM	HODNOTA	HROZBA	ZRANITELNOSTI	PRAVDĚPODOBNOST	DOPAD	RIZIKO
	stupnice 1-5 (1 - nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší)	potenciální příčina nechtěného incidentu, která může vyústit v poškození systému	slabé místo aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami	hrozby ve vztahu k zranitelnosti (bodové hodnocení 1-5); 1– nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší	hodnota aktiva	pravděpodobnost x dopad
Data na serveru	5	krádež dat – zvenku	nedostatečné zabezpečení	1	5	5
			prozrazení přístupových hesel administrátorů	1	5	5
			prozrazení přístupových hesel uživatelů	3	5	15
			krádež serveru	1	5	5
		nedodržení bezpečnostních opatření	odposlech po lokální síti (LAN)	1	5	5
			nedostatečné prověření zaměstnanců	2	5	10
		zničení / ztráta záznamů	chybný zásah administrátora	3	5	15
			chybný zásah uživatele	3	5	15
			nedostatečně specifikovaná opatření	1	5	5
			neautorizovaný přístup	1	5	5
			selhání HW	2	5	10
			selhání SW	1	5	5

			zlomyslné kódy	3	5	15
		prozrazení hesla administrátora	nedostatečné bezpečnostní povědomí	1	5	5
			nedostatečné zabezpečení (neúmyslné prozrazení)	1	5	5
		prozrazení hesla uživatele	nedostatečné bezpečnostní povědomí	2	5	10
			nedostatečné zabezpečení (neúmyslné prozrazení)	2	5	10
		falzifikace záznamů	neautorizovaný přístup	1	5	5
			úmyslný zásah uživatele	1	5	5
		chybný zásah uživatele	nedostatečné bezpečnostní povědomí	2	5	10
			osobní selhání	2	5	10
		zlomyslné kódy	nezabezpečený přístup	1	5	5
			nedostatečné prověření zaměstnanců	2	5	10
		neautorizovaný přístup	nedostatečné bezpečnostní povědomí	2	5	10
			nedostatečné zabezpečení	2	5	10
			nedostatečné zabezpečení	1	5	5
Data na ostatních PC	1	krádež dat	nedostatečné zabezpečení	1	1	1
			prozrazení přístupových hesel	2	1	2
			krádež telefonů (synchronizovaná data)	3	5	15
			krádež notebooků	3	1	3
			krádež PC (podniku)	1	1	1
			krádež PC (domácí zaměstnanců)	1	1	1
			odposlech po lokální síti (LAN)	1	1	1

			nedostatečné prověření zaměstnanců	2	1	2
		nedodržení bezpečnostních opatření	krádež dat	2	1	2
			odposlech po lokální síti (LAN)	1	1	1
			nedostatečné prověření zaměstnanců	2	1	2
		zničení / ztráta záznamů	chybný zásah administrátora	1	1	1
			chybný zásah uživatele	1	1	1
			nedostatečně specifikovaná opatření	1	1	1
			neautorizovaný přístup	1	1	1
			chybný zásah uživatele	1	1	1
			selhání HDD	1	1	1
			selhání SW	1	1	1
			zlomyslné kódy	1	1	1
		prozrazení hesla k NTB, PC	nedostatečné bezpečnostní povědomí	2	1	2
			nedostatečné zabezpečení (neúmyslné prozrazení)	1	1	1
		falzifikace záznamů	neautorizovaný přístup	1	1	1
			úmyslný zásah uživatele	1	1	1
		chybný zásah uživatele	nedostatečné bezpečnostní povědomí	4	1	4
			osobní selhání	4	1	4
		zlomyslné kódy	nezabezpečený přístup	1	1	1
			nedostatečné prověření zaměstnanců	2	1	2
		neautorizovaný přístup	nedostatečné bezpečnostní povědomí	2	1	2
			nedostatečné zabezpečení	1	1	1

			nedostatečné zabezpečení na domácích PC	4	1	4
		úmyslné poškození	neautorizovaný přístup	2	1	2
			nedostatečné zabezpečení	1	1	1
Data na přenosných discích (externí výměnný disk, flash disk)	5	krádež dat – únik informací	nedostatečné zabezpečení přenosného zařízení proti krádeži / proti přečtení	2	2	4
			nedostatečné povědomí zaměstnanců	2	2	4
		ztráta přenosného zařízení	nedostatečné zabezpečení přenosného zařízení proti krádeži / proti přečtení	2	2	4
			nedostatečné povědomí zaměstnanců	2	2	4
		přenos zlomyslných kódů	nezabezpečený přístup	2	2	4
Zálohovaná data na CD a DVD nosičích	5	krádež dat – únik informací	nedostatečné zabezpečení přenosného zařízení proti krádeži / proti přečtení	2	5	10
			nedostatečné povědomí zaměstnanců	2	5	10
		ztráta přenosného zařízení	nedostatečné zabezpečení přenosného zařízení proti krádeži / proti přečtení	1	5	5
Zálohovaná data na externím HDD	5	krádež dat – únik informací	nedostatečné zabezpečení úložných prostor	2	4	8
			nedostatečné povědomí administrátora	1	5	5

Data (zdrojové kódy) přenášená na DVD nosičích od zákazníka	5	krádež dat – únik informací	nedostatečné zabezpečení přenosného zařízení proti krádeži / proti přečtení	2	5	10
			nedostatečné povědomí zaměstnanců	1	5	5
		ztráta přenosného zařízení	nedostatečné zabezpečení přenosného zařízení proti krádeži	1	5	5
Smlouvy se zákazníky v listinné podobě	4	krádež smluv – únik informací	nedostatečné zabezpečení úložných prostor	2	3	6
			nedodržení bezpečnostních předpisů pro zacházení se smlouvami	2	4	8
		požár	nedostatečné protipožární zabezpečení	1	4	4
		falzifikace smluv	poškození image podniku	1	4	4
Smlouvy s dodavateli v listinné podobě	3	krádež smluv – únik informací	nedostatečné zabezpečení úložných prostor	1	3	3
			nedodržení bezpečnostních předpisů pro zacházení se smlouvami	2	3	6
		požár	nedostatečné protipožární zabezpečení	1	3	3
		falzifikace smluv	poškození image podniku	1	3	3
Dokumentace k zakázkám v listinné	2	krádež dokumentace – únik informací	nedostatečné zabezpečení úložných prostor	1	2	2

podobě						
			nedodržení bezpečnostních předpisů pro zacházení s projektovou dokumentací	1	2	2
		požár	nedostatečné protipožární zabezpečení	1	2	2
Nabídky a objednávky se zákazníky	4	krádež dokumentů – únik informací	nedostatečné zabezpečení úložných prostor	1	4	4
			nedodržení bezpečnostních předpisů pro zacházení s dokumenty (nabídkami, objednávkami)	1	4	4
		požár	nedostatečné protipožární zabezpečení	1	4	4
Objednávky s dodavateli	1	krádež dokumentů – únik informací	nedostatečné zabezpečení úložných prostor	1	2	2
			nedodržení bezpečnostních předpisů pro zacházení s dokumenty (objednávkami)	1	2	2
		požár	nedostatečné protipožární zabezpečení	1	2	2
Provozní dokumentace (autoprovoz, záruční listy, licence apod.)	2	krádež provozní dokumentace	nedostatečné zabezpečení úložných prostor	1	2	2
			nedodržení bezpečnostních předpisů pro zacházení s provozní dokumentací	1	2	2
		požár	nedostatečné protipožární zabezpečení	1	2	2

Podklady pro účetnictví (faktury, pokladní doklady, výpisy z účtů)	4	krádež dokumentů	nedostatečné zabezpečení úložných prostor	1	4	4
			nedodržení bezpečnostních předpisů pro zacházení s podklady pro účetnictví	1	4	4
		požár	nedostatečné protipožární zabezpečení	1	4	4
Personální agenda (pracovní smlouvy, osobní listy zaměstnanců, podklady pro mzdy – pracovní neschopenky, mzdová agenda, apod.)	3	krádež dokumentů týkající se personální agendy	nedostatečné zabezpečení úložných prostor	1	3	3
			nedodržení bezpečnostních předpisů pro zacházení s těmito dokumenty	1	3	3
		prozrazení osobních údajů	zneužití osobních údajů	1	3	3
		požár	nedostatečné protipožární zabezpečení	1	3	3
Internet	5	nabourání sítě	nedostatečně zabezpečená sítě	1	5	5

(UPC)						
Data v mobilních telefonech	2	únik informací	nedodržení bezpečnostních předpisů pro zacházení s daty ukládanými do mobilních telefonů	1	2	2
			nedodržení bezpečnostních předpisů pro zacházení se smlouvami	2	2	4
		požár	nedostatečné protipožární zabezpečení	1	2	2
		falzifikace smluv	poškození image podniku	1	2	2

Zdroj: Vlastní zpracování (2021)

Softwarová aktiva

V níže uvedené tabulce jsou identifikována softwarová aktiva.

Tabulka 19 Softwarová aktiva

AKTIVUM	HODNOTA	HROZBA	ZRANITELNOSTI	PRAVDĚPODOBNOST	DOPAD	RIZIKO
	stupnice 1-5 (1 - nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší)	potenciální příčina nechtěného incidentu, která může vyústit v poškození systému	slabé místo aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami	hrozby ve vztahu k zranitelnosti (bodové hodnocení 1-5); 1– nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší	hodnota aktiva	pravděpodobnost x dopad
Operační systémy a ostatní programy	3	selhání systému (aplikace)	nedostatečné bezpečnostní povědomí	3	3	9
			viry, trojany	2	3	6
			nenainstalování antivirových programů	1	3	3
			poškození na HW	2	3	6
		ztráta licencí	nedodržení licenční politiky	1	3	3
		ne aktualizace programu	nestahování potřebných aktualizací a záplat	1	3	3

Zdroj: Vlastní zpracování (2021)

Fyzická aktiva

V níže uvedené tabulce jsou identifikována fyzická aktiva.

Tabulka 20 Fyzická aktiva

AKTIVUM	HODNOTA	HROZBA	ZRANITELNOSTI	PRAVDĚPODOBNOST	DOPAD	RIZIKO
	stupnice 1-5 (1 - nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší)	potenciální příčina nechtěného incidentu, která může vyústit v poškození systému	slabé místo aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami	hrozby ve vztahu k zranitelnosti (bodové hodnocení 1-5); 1– nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší	hodnota aktiva	pravděpodobnost x dopad
PC a notebooky zaměstnavatele	2	poškození (selhání) zařízení	stáří	1	3	3
			výpadek HW	3	5	15
			živelná pohroma	1	5	4
			lidský faktor (např.: polití kávou)	2	3	6
			přepětí v síti	1	4	4
		vandalismus	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	1	3	3
		neúmyslné poškození	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	1	3	3
			neodborná a nedbalá manipulace	1	3	3
		ztráta	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	1	3	3
			nedostatečné fyzické zabezpečení	1	3	3
		odcizení	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	1	3	3

			nedostatečné fyzické zabezpečení	1	3	3
		živelné katastrofy (např. požár)	nedostatečné preventivně požární opatření a další	1	3	3
Server	5	poškození (selhání) zařízení	stáří	1	4	4
			výpadek HW	3	5	15
			živelná pohroma	1	5	5
			lidský faktor	2	3	6
		živelné katastrofy (např. požár)	nedostatečné preventivně požární opatření a další	2	4	8
Flashdisky	1	poškození (selhání) zařízení	stáří	1	1	1
			výpadek HW	1	1	1
			živelná pohroma	1	1	1
			lidský faktor	2	1	2
		neúmyslné poškození	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	2	1	2
			neodborná a nedbalá manipulace	2	1	2
		ztráta	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	2	1	2
			nedostatečné fyzické zabezpečení	2	1	2
		odcizení	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	2	1	2
			nedostatečné fyzické zabezpečení	2	1	2
		živelné katastrofy (např. požár)	nedostatečné preventivně požární opatření a další	1	1	1
Mobilní telefony zaměstnanc	1	neúmyslné poškození	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	2	1	2

ů						
			neodborná a nedbalá manipulace	2	1	2
		ztráta	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	2	1	2
			nedostatečné fyzické zabezpečení	2	1	2
PC a notebooky domácí včetně příslušenství	1	neúmyslné poškození	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	1	3	3
			neodborná a nedbalá manipulace	1	3	3
		ztráta	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	2	3	6
			nedostatečné fyzické zabezpečení	2	3	6
Externí zálohovací HDD	1	neúmyslné poškození	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	1	2	2
			neodborná a nedbalá manipulace	1	2	2
		ztráta	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	1	2	2
			nedostatečné fyzické zabezpečení	1	2	2
Ostatní zařízení (fotoaparát, tiskárny, faxy, GPS, apod.)	2	neúmyslné poškození	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	1	2	2
			neodborná a nedbalá manipulace	1	2	2

		ztráta	nedodržení bezpečnostní politiky (např.: ponechání bez dozoru)	1	2	2
			nedostatečné fyzické zabezpečení	1	2	2
Automobily osobní	2	krádež, vykradení	nedostatečné zabezpečení	2	4	8
		zničení	nedostatečné zabezpečení	2	4	8
			havárie	2	4	8
		vandalismus	nedostatečně zajištěné parkování na ulici	3	4	12
		živelná pohroma	nedostatečná preventivní opatření	1	4	4
Budova provozovny	5	krádež, vykradení	nedostatečné zabezpečení	2	5	10

Zdroj: Vlastní zpracování (2021)

Aktiva lidských zdrojů

V níže uvedené tabulce jsou identifikována aktiva lidských zdrojů.

Tabulka 21 Lidské zdroje

AKTIVUM	HODNOTA	HROZBA	ZRANITELNOSTI	PRAVDĚPODOBNOST	DOPAD	RIZIKO
	stupnice 1-5 (1 - nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší)	potenciální příčina nechtěného incidentu, která může vyústit v poškození systému	slabé místo aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami	hrozby ve vztahu k zranitelnosti (bodové hodnocení 1-5); 1– nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší	hodnota aktiva	pravděpodobnost x dopad
Jednatel podniku	5	neschopnost provádět finanční operace	nezastupitelnost v provádění finančních operací	4	4	15
		neschopnost jednat za podnik	nezastupitelnost v jednání za podnik	2	4	8
		neschopnost schvalovat interní předpisy	nezastupitelnost	2	4	8
		neschopnost rozhodování o vizi a strategii podniku + o firemní identitě	nezastupitelnost	2	4	8
Vedoucí zaměstnanci	3	neschopnost vykonávat náplň svých kompetencí	snížená zastupitelnost	3	4	12
Administrátor	3	nemoc	nepředání hesel, kódů atd	1	3	3
Ostatní zaměstnanci +	2	neschopnost vykonávat náplň	snížená zastupitelnost	2	4	8

přímí dodavatelé		svých kompetencí				
Podpůrní dodavatelé (účetní, daňový poradce, právní poradce apod.)	2	neschopnost vykonávat náplň svých kompetencí	zpomalení efektivnosti svěřených procesů	1	2	2
		nedostupnost	zpomalení efektivnosti svěřených procesů	3	2	6
		prozrazení informací	narušení integrity našeho podniku	1	2	2
Služby vztahující se k sídlu podniku (technické služby budovy, úklid apod.)	1	neschopnost vykonávat náplň svých kompetencí	zpomalení efektivnosti svěřených procesů	1	1	1
		nedostupnost	zpomalení efektivnosti svěřených procesů	3	1	3
		prozrazení informací	narušení integrity našeho podniku	3	1	3
Obchodní partneři klíčoví	4	nedostupnost	zpomalení efektivnosti našich procesů	1	4	4
			ohrožení provozu systémů	1	4	4
		porušení smluvních	ohrožení efektivnosti našich procesů	1	4	4

		závazků				
		odstoupení od smlouvy	ohrožení činností podniku	1	4	4
Zákazníci	5	prozrazení informací	zneužití dodané služby	1	5	5
		nekorektnost	poškození know-how podniku	1	3	3

Zdroj: Vlastní zpracování (2021)

Ostatní aktiva

V níže uvedené tabulce jsou identifikována ostatní aktiva.

Tabulka 22 Ostatní aktiva

AKTIVUM	HODNOTA	HROZBA	ZRANITELNOSTI	PRAVDĚPODOBNOST	DOPAD	RIZIKO
	stupnice 1-5 (1 - nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší)	potenciální příčina nechtěného incidentu, která může vyústit v poškození systému	slabé místo aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami	hrozby ve vztahu k zranitelnosti (bodové hodnocení 1-5); 1– nejnižší; 2 – nízká; 3 – střední; 4 – vysoká; 5 – nejvyšší	hodnota aktiva	pravděpodobnost x dopad
Image podniku	4	nefunkční www stránky	jakýkoliv problém u poskytovatele	4	1	4
		úmyslné poškození zaměstnancem	nedodržení bezpečnostní politiky, pracovního řádu	2	5	10
		nekvalitně odvedená práce zaměstnancem	osobní selhání	2	5	10

Zdroj: Vlastní zpracování (2021)

Příloha 3 Přehled skupin aktiv bezpečnosti informací

V níže uvedené tabulce je uveden přehled aktiv.

Tabulka 23 Přehled skupin aktiv podniku MHK

Aktivum	Hrozba (počet)
Informační aktiva	49
Softwarová aktiva	29
Fyzická aktiva	25
Aktiva lidských zdrojů	18
Ostatní aktiva	3
Celkem	**124**

Zdroj: Vlastní zpracování (2021)