Návrh metrik pro stanovení efektivity procesů spojených se Systémem řízení bezpečnosti informací

Bc. Radek Válka

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Radek Válka**
Osobní číslo:	**A20683**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Návrh metrik pro stanovení efektivity procesů spojených se Systémem řízení bezpečnosti informací**
Téma práce anglicky:	**Design of Metrics for Determining the Effectiveness of Processes Associated with the Information Security Management System**

Zásady pro vypracování

1. Vypracujte literární rešerši na dané téma.
2. Popište strukturu a procesy společnosti.
3. Navrhněte metriky pro měření efektivity procesů spojených se Systémem řízení bezpečnosti informací.
4. Navrhněte postup vyhodnocování metrik.
5. Uveďte výsledné hodnocení metrik ve společnosti.
6. Vyhodnoťte výsledky metrik dle navrhnutého postupu.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KOHL, Herfried. Standards for Management Systems: A Comprehensive Guide to Content, Implementation Tools, and Certification Schemes. Springer Nature, 2020.
2. DRASTICH, Martin. Systém managementu bezpečnosti informací. Praha: Grada, 2011. Průvodce (Grada). ISBN 9788024742519.
3. THE OPEN GROUP. Open Information Security Management Maturity Model O-ISM3. Van Haren, 2011.
4. BROTBY, Krag. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement. CRC Press, 2009.
5. HALIBOZEK, Edward a Gerald L. KOVACICH. Security Metrics Management: Measuring the Effectiveness and Efficiency of a Security Program. Butterworth-Heinemann, 2016.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. prosince 2021**
Termín odevzdání diplomové práce: **23. května 2022**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 7. února 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 27.5.2022

Radek Válka, v.r.
podpis studenta

ABSTRAKT

V této práci jsou na základě analýzy rizik pro bezpečnost informací podniku stanoveny procesy spojené se systémem řízení bezpečnosti informací, které nejsou efektivní. Pro tyto procesy jsou navrhnuty metriky dle postupu normy ISO/IEC 27004. Spolu s návrhem metrik je také navrženo jejich měření a vyhodnocení výsledků. Na základě vyhodnocení je stanovena efektivita procesů a jsou navrhnuta adekvátní bezpečnostní opatření pro zvýšení efektivity.

Klíčová slova:

Metriky, bezpečnost informací, efektivita procesů, efektivita bezpečnosti informací, ISO/IEC 27001, ISO/IEC 27004, ISMS, měření ISMS

ABSTRACT

In this thesis are identified the processes associated with the information security management system that are not effective, based on an analysis of the information security risks to the company. For these processes are proposed metrics according to the ISO/IEC 27004 procedure. Along with the design of metrics are also proposed their measurement and evaluation of results. Based on the evaluation, the effectiveness of the processes is determined and adequate security measures are proposed to increase the effectiveness.

Keywords:

Metrics, information security, process effectiveness, information security effectiveness, ISO/IEC 27001, ISO/IEC 27004, ISMS, ISMS measurement

Poděkování

Tímto bych rád poděkoval svému vedoucímu práce prof. Mgr. Romanu Jaškovi, Ph.D., za jeho rady, vstřícný přístup a čas, který mi věnoval při tvorbě této práce. Zároveň bych chtěl poděkovat zaměstnancům podniku za jejich spolupráci a poskytnutí potřebných údajů k práci a také přátelům a rodině, kteří mě při psaní práce podporovali.

OBSAH

ÚVOD

Na podniky jsou v dnešní době kladeny od zákazníků stále vyšší požadavky na kvalitu služeb. Spolu s vyšší kvalitou služeb zákazníci očekávají také zajištění bezpečnosti informací, které zákazníci podnikům předávají. Některé podniky jsou i legislativou vázané, zajistit bezpečnost jejich informací, například dle zákona o kybernetické bezpečnosti.

Aby podniky mohly splnit tyto požadavky na zabezpečení informací, zavádějí takzvané systémy řízení, které jim pomohou definovat a standardizovat své vnitřní a vnější procesy. Správně standardizované procesy, které jsou jakýmkoliv způsobem spojené s bezpečností informací, výrazně pomohou podniku zvýšit bezpečnost svých dokumentů a dat.

Jak ale podnik nejlépe pozná, že tyto procesy zavedl správně a jsou co nejvíce efektivní? K měření efektivity procesů slouží takzvané metriky. Pro návrh metrik je v této práci zvolen postup, popsaný normou ISO/IEC 27004. Tato norma definuje požadavky normy ISO/IEC 27001, která se stala velice uznávaným mezinárodním standardem, jenž specifikuje požadavky pro řízení bezpečnosti důvěry informací, procesů, IT systémů, zařízení a strategií společnosti.

Návrh metrik je v této práci řešen pro malou společnost, která se zabývá převážně vývojem softwaru, ICT službami a službami operátora sítě. Návrh metrik pro měření efektivity procesů spojených s bezpečností informací je součástí přípravy společnosti na certifikaci systému managementu bezpečnosti informací dle normy ISO/IEC 27001 a také certifikaci systému managementu jakosti dle normy ISO 9001.

I. TEORETICKÁ ČÁST

1 INTEGROVANÝ SYSTÉM ŘÍZENÍ (IMS)

V dnešní době se podniky nachází v neustále se více měnícím prostředí a jsou na ně od zákazníků kladeny stále vyšší požadavky na kvalitu výrobků nebo jejich služeb. Aby tyto změny dokázaly podniky předvídat a vhodně na ně i na požadavky od zákazníků reagovat, je nutné uvnitř podniku vybudovat systém. Podniky se proto snaží standardizovat své vnitřní i vnější procesy na základě jednotlivých systémů řízení [1].

Jelikož požadavky jednotlivých systémů jsou si v některých částech podobné nebo se dokonce překrývají, je možná jejich integrace v jeden celek. Integrovaný systém řízení, anglicky Integrated Management System (IMS), propojuje tyto jednotlivé systémy řízení (např. jakosti, managementu životního prostředí, bezpečnosti a ochrany zdraví při práci, bezpečnosti informací) do jednoho uceleného, komplexního a harmonizovaného systému řízení. Díky tomuto přístupu poskytuje hodnotný přehled o důležitých podnikových procesech [2].

1.1 Systém řízení bezpečnosti informací (ISMS)

ISMS, anglicky Information security management system, je efektivní dokumentovaný systém řízení a správy informačních aktiv. Cílem systému je eliminovat možnou ztrátu, odcizení nebo poškození informačních aktiv [3].

Informační aktiva mohou být samostatné informace v podobě dat nebo znalostí, mohou to však být i systémy, zařízení či dokumenty, které obsahují informace. Tato aktiva jsou pro podnik významná a mohou být osobou či entitou mimo podnik zneužita.

Pro zajištění bezpečnosti informačních aktiv je v ISMS brán ohled na tzv. bezpečnostní atributy, které každá informace má. Těmito atributy jsou důvěrnost, integrita a dostupnost.

Aby informace zůstala důvěrná, musí podnik zajistit, aby byla přístupná pouze těm osobám, či entitám, které jsou oprávněné k ní přistupovat a s informací pracovat. Integritou je zabezpečení přesnosti, správnosti a kompletnosti informace. Zabezpečením posledního atributu, atributu dostupnosti, zajišťujeme, aby informace a jakékoliv aktivum s ní spojené bylo dostupné vždy, když jej oprávněné osoby požadují [4].

Jelikož způsobů zajištění bezpečnosti výše zmíněných atributů může být v podniku mnoho, je jedním z cílů systému řízení bezpečnosti informací určit pro informační aktiva s nimi spojená rizika. Rizikem je působení jakékoliv hrozby na aktivum díky jeho zranitelnosti. To

znamená, že pokud identifikujeme zranitelnosti, které daná informační aktiva mají a hrozby, které mohou těchto zranitelností využít a mít pro podnik jakýkoliv nepříznivý dopad, dokážeme určit rizika. Nejvíce pravděpodobná a nejnebezpečnější rizika musí být odpovídajícím způsobem řízena, a to například přenesením odpovědnosti za riziko na někoho jiného, eliminací aktiva, aby nám riziko vůbec nemohlo vzniknout, nebo stanovením takzvaných opatření, které nám výši rizika pro podnik sníží.

1.1.1 Řada norem ISO/IEC 27000

Celosvětově uznávaných standardů určených k zavedení systému řízení bezpečnosti informací není mnoho. Tím nejrozšířenějším standardem je ISO/IEC 27001 – Information Security Management System, patřící do rodiny mezinárodních norem ISO 27000, zaměřené na řízení informační bezpečnosti v organizacích. Tyto mezinárodní standardy jsou navrženy pro poskytnutí podpory pro ustanovení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací (ISMS) [5].

Jednotlivé normy z rodiny ISO 27000 se zaměřují na různé aspekty systému řízení informační bezpečnosti. Nepodstatnějšími z norem, kromě hlavní normy ISO/IEC 27001, jsou norma ISO/IEC 27002, která definuje sto čtrnáct dílčích opatření rozdělených do čtrnácti oblastí pro zvýšení bezpečnosti informací v rámci ISMS [6] a dále norma ISO/IEC 27003, která je návodem pro zavedení ISMS.

1.1.2 Zákon o kybernetické bezpečnosti

Kromě norem ISO/IEC 27000 je zavedení systému řízení bezpečnosti informací také cílem zákona č.181/2014 Sb., o kybernetické bezpečnosti. Tento zákon není však, jako norma ISO/IEC 27001, obecným doporučením, ale závazným předpisem, který firmám, zajišťujícím důležité služby pro chod státu ukládá, jak mají svá informační aktiva chránit [7].

Stejně jako norma ISO/IEC 27001 je založený na Demingově cyklu, viz kapitola 1.3 a jeho cílem je bezpečnost informací, je tedy postavený na systému řízení bezpečnosti informací.

Hlavním rozdílem mezi zákonem o kybernetické bezpečnosti a normou ISO/IEC 27001 je zaměření zákona převážně na zabezpečení významných systémů pro stát a digitálních služeb, tedy bezpečnosti elektronických dat. Dalším hlavním rozdílem je porušení bezpečnosti informačních aktiv v rámci normy, kdy se toto porušení bezpečnosti nazývá „bezpečnostní incident“. V rámci zákona se porušení bezpečnosti informací nazývá

„kybernetický bezpečnostní incident“, na rozdíl od normy je povinné ho ohlašovat státu a souvisí zejména s kybernetickým prostředím.

1.1.3 Chráněné informace

Všechny informace v podniku jsou klasifikovány na základě potřebnosti a důležitosti pro podnik, tzn. jaké je potřeba zajistit zabezpečení pro zajištění, že informace nebude dostupná nebo nebude odhalena neoprávněným jednotlivcům nebo entitám.

V rámci klasifikace je každé informaci přiřazen klasifikační stupeň. Klasifikační stupeň se informaci přiřadí podle významu a závažnosti jejího obsahu. Celkový postup klasifikace informací je v ISMS poněkud komplikovanější, výsledkem klasifikace je však rozdělení informací v podniku na:

- veřejné informace: veřejnými informacemi jsou ty, které zahrnují široký okruh informací k zajištění činností podniku a jsou schváleny ke zveřejnění, nebo informace které se staly obecně dostupnými veřejnosti jinak než následkem jejich zpřístupnění přímo či nepřímo zaměstnancem podniku. U veřejných informací není podnik povinen chránit jejich důvěrnost.
- neveřejné informace (chráněné):
    - interní informace: interní informace podniku jsou neveřejné informace, jejichž vyzrazení, zneužití nebo poškození může být pro podnik nevýhodné. Prozrazení těchto informací může ovlivnit činnosti podniku.
    - citlivé informace: citlivé informace podniku jsou informace, u nichž nutnost ochrany vyplývá z legislativy nebo ze závazků podniku a jejichž vyzrazením či zneužitím mohou být výrazně ohroženy zájmy podniku.

Při řízení systému bezpečnosti informací musí společnosti udržovat zejména důvěrnost citlivých informací. Zajištění důvěrnosti citlivých informací je zakomponováno do návrhu metrik pro stanovení efektivity procesů, kterým se práce věnuje.

1.2 Systém řízení kvality (QMS)

V dnešním rychle se měnícím prostředí je potřeba vyrovnávat se s novými výzvami, požadavky a být na ně jako podnik připraven. Z tohoto důvodu je nutné si osvojit správné manažerské návyky a činnosti, které umožní odhadovat tyto změny včas a také včas na ně reagovat [8]. S narůstajícím trhem se podniky snaží být konkurenceschopné a splňovat v co

nejvyšší míře požadavky zákazníka. Pro tyto účely se v podnicích zavádí systém řízení kvality, anglicky Quality Management System.

V devadesátých letech bylo řízení kvality považováno za výhodu oproti konkurenci, podniky ji však nepovažovaly za jednu z klíčových činností pro podnik a klíčový faktor pro úspěch. V současné době se situace změnila natolik, že kvalita se stala v podnicích nejenom okrajovou záležitostí, ale naopak jednou z hlavních priorit podniku.

Pro kvalitu se stal přelomovým rokem rok 1950, kdy byl hlavním rozdílem přechod od orientace podniků na výrobek k orientaci podniku na výrobní proces. V Japonsku se podařilo rozšířit řízení procesů i do dalších oblastí a činností podniku, zejména do etap, které se netýkaly čistě výroby, ale i do předvýrobních a závěrečných etap. Vznikl jeden z moderních systémů řízení kvality označovaný jako Company Wide Quality Control (zkráceně CWQC). Následujícím zdokonalením a přepracováváním tohoto přístupu došlo k prvním pokusům o komplexní metodu zvanou Total Quality Management (zkráceně TQM), která i v dnešní době představuje dynamicky se vyvíjející metodu používanou v podnicích. Tato metoda klade důraz na řízení kvality ve všech částech života a činností podniku.

Poté v roce 1987 vstoupily v platnost dnes známé normy ISO řady 9000, které se snažily o rozsáhlou dokumentaci všech podnikových procesů.

Zavedením systému řízení kvality je sledována a hodnocena kvalita výrobku nebo služby, což je pro podnik velmi důležité, jak z hlediska ekonomického, tak i z hlediska spokojenosti zákazníka. Přístup k péči o kvalitu je založený nejen na činnostech spojených s výrobou daného výrobku nebo služby, ale i na tom, co můžeme označit za následné služby, jako jsou např. způsob prodeje, úroveň servisní činnosti atd.

Kvalita výrobku či služby je definována také kvalitou zaměstnanců, a proto je v zájmu rozvíjejícího se podniku řídit výběr, vzdělávání a vedení svých zaměstnanců. Pro kvalitní výrobu nebo služby je nutné zaměstnance vhodně motivovat, aby vznikl jednotně fungující tým. Dalším přínosem kvality může být úspora materiálu a energií.

Systém řízení kvality se projevuje pozitivně uvnitř podniku i v jeho okolí. Účinky uvnitř podniku se mohou projevovat například snížením podílu neshod na celkovém výkonu podniku, stoupáním vytíženosti materiálu a účinnějšími vnitropodnikovými procesy. Jedním z externích účinků systému řízení kvality je převážně stoupající míra spokojenosti zákazníků a stoupající spokojenost dodavatelů. Tyto účinky vedou ke zvyšování zisku, zlepšování

finančních toků a dalších výsledků podniku. Jedním z cílů systému řízení kvality je tedy garantovat maximální míru spokojenosti zákazníka při minimálních nákladech.

Dle norem ISO 9000 je systém řízení kvality založen na principu procesního přístupu. Díky tomuto procesu podniky pracují efektivněji a výsledků dosahují účinněji, pokud vzájemně související činnosti jsou chápány a řízeny jako procesy. Základní filosofií moderního systému řízení je tedy průběžně monitorovat a řídit procesy. Jsou-li v pořádku vstupy a probíhá-li proces co nejefektivněji, lze očekávat i dokonalý výrobek nebo službu. V procesech je výrobek nebo služba nejen realizována, ale i plánována, vyvíjena, hodnocena a zlepšována. Více o procesním přístupu a řízení procesů je popsáno v kapitole 2 [8].

1.2.1 Řada norem ISO 9000

Řada norem ISO 9000 definuje systém řízení kvality. Tyto normy vydává Mezinárodní organizace pro normalizaci. Tato rodina norem umožňuje daným podnikům prokázat schopnost výroby či distribuci produktů v souladu se všemi právními předpisy, které se na podnik vztahují a s potřebami zákazníka [9].

Normy ISO 9000 byly poprvé zveřejněny v roce 1987 a vzešly z řady norem BS 5750 (British Standard). Určité úpravy a revize proběhly v roce 1994, ale nová ucelená řada ISO 9000 (viz výše) vznikla až v roce 2000.

Z rodiny norem ISO 9000 jsou nejdůležitější tyto normy:

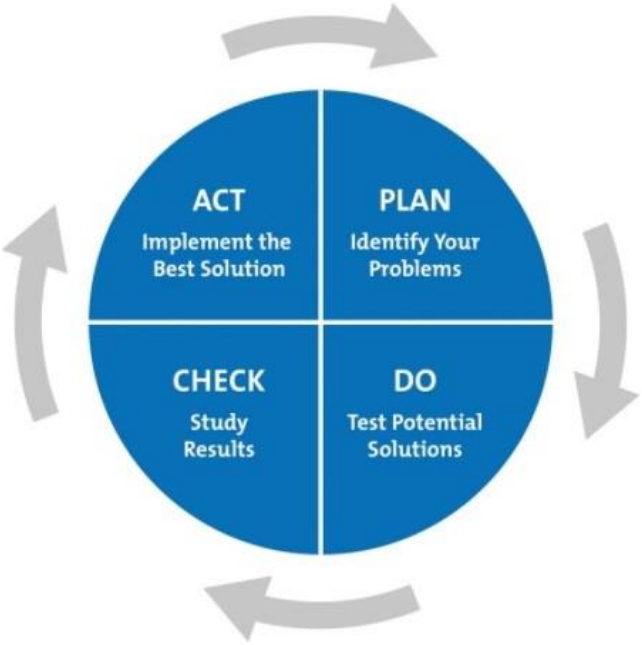
- ČSN EN ISO 9000: norma slouží jako přehled zásad a výrazů řízení kvality. Obsahuje výklad nejdůležitějších pojmů týkajících se kvality a jejího zajištění.
- ČSN EN ISO 9001: tato norma je považována za stěžejní a na základě této normy je zaváděn, udržován a monitorován systém řízení kvality. Požadavky této normy musí podnik splnit, pokud potřebuje prokázat úspěšné fungování řízení kvality.
- ČSN EN ISO 9004: účelem této normy je poskytnout podniku možnosti, které může podnik dále zavést nad rámec požadavků uvedených v normě ISO 9001 v zájmu dalšího rozšíření a zlepšení systému managementu kvality (viz výše).

1.3 Demingův cyklus

Demingův cyklus je pojmenovaný podle autora Williama Edwardse Deminga, jenž byl americký matematik a fyzik. Deming se nechal velmi inspirovat fyzikem a inženýrem

Walterem A. Shewhartem a jeho myšlenkami z oblasti statistických metod aplikovaných při kontrole výroby a v řízení. Toto téma následně rozvinul do oblasti řízení kvality [10].

Demingův cyklus, jinak také zvaný PDCA cyklus, navrhl William Deming jako metodu pro postupné zlepšování například kvality výrobků, služeb, procesů či systémů probíhající formou opakovaného provádění čtyř základních činností [11]:



Obrázek 1. Vyobrazení Demingova cyklu [11]

- plan (plánuj) – naplánování zamýšleného zlepšení (záměr),
- do (dělej) – realizace plánu,
- check (kontroluj) – ověření výsledku realizace oproti původnímu záměru,
- act (jednej) – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe (viz výše).

Tento cyklus se stal moderním pojetím všech standardů zaměřených na systém řízení. Je tedy zejména jádrem standardů, kterým se tato práce věnuje, a to řízení kvality ISO 9001 a řízení informační bezpečnosti ISO 27001.

Jelikož se systémy řízení drží tohoto cyklu, je možné tyto zaváděné nebo zavedené systémy integrovat. U obou systémů cyklus zavádí kontinuální systém řízení v podniku, jehož jednotlivé kroky zaručují, že zavedení systému není pouze jednorázovou aktivitou, ale systém je neustále rozvíjen a posouván dopředu [5]. V případě systému řízení bezpečnosti informací s využitím tohoto modelu je systém udržován aktuální a jsou brány v jednotlivých

cyklech v potaz jakékoliv změny v podniku nebo jakékoliv hrozby, které by mohly mít vliv na bezpečnost informací.

Metriky pro stanovení efektivity procesů, kterým se tato práce věnuje, jsou jednou z hlavních prostředků pro měření systému řízení a jednou ze čtyř základních činností Demingova cyklu - check (kontroluj).

1.4 Monitorování a měření v systémech řízení

K nejvýznamnějším nástrojům, napomáhajících efektivnímu fungování systémů řízení, patří měření. Podstatou měření je shromáždění potřebných informací, jejich následná analýza a zlepšování systému na základě zjištěných výsledků analýzy. Povinnost monitorovat a měřit, ať se jedná o procesy, výrobky, služby, bezpečnostní opatření nebo prvky systému, je jedním ze základních principů řízení kvality, řízení bezpečnosti informací a obecně systémů řízení.

Splňovat požadavky zákazníků a uspokojit jejich potřeby kvalitními výrobky nebo službami může podnik pouze, pokud monitoruje, měří a vyhodnocuje informace. Informacemi z vyhodnocení lze doložit a prokázat splnění těchto požadavků, požadavků norem nebo závazných legislativních požadavků.

Ve všech systémech řízení je postup podobný. Je nutné monitorovat a měřit faktický stav prověřovaného prvku. Daný prvek porovnat se stanovenými požadavky a v případě, že bude zjištěn nesoulad s požadavky nebo nějaký nedostatek (tzv. neshoda), je přijato opatření k následnému odstranění této neshody a zároveň jsou přijaty kroky pro aplikaci nápravného nebo preventivního opatření [12].

Monitorování a měření procesů v systémech řízení je v ISO normách povinné. Cílem tohoto monitorování a měření je prokázat, že procesy mohou dosahovat plánovaných výsledků a tím přispívat ke zlepšení systému řízení. Více o monitorování a měření procesů je popsáno v kapitole 2.5 Monitorování a měření výkonnosti procesů.

1.5 Organizace rolí v rámci integrovaného systému řízení

Pro splnění požadavku ISO norem a možnost efektivně řídit jednotlivé systémy řízení musí podnik určit relevantní role. Osoby, zastávající tyto role, mají rozděleny odpovědnosti a pravomoci v rámci integrovaného systému řízení, jsou definovány ISO normami a zajišťují, že činnosti vykonávané v podniku odpovídají požadavkům ISO norem.

1.5.1 Manažer informační bezpečnosti

Tato osoba je odpovědná za celkové řízení systému bezpečnosti informací a měla by pro tuto roli být odborně vyškolená a způsobilá. Zastávat roli manažera informační bezpečnosti může člen vyššího vedení podniku, který má pravomoc řídit zaměstnance a je v dostatečném spojení s vrcholovým vedením podniku. Roli zastává nejčastěji vedoucí pracovník oddělení či úseku, zodpovědného za správu ICT infrastruktury nebo informací podniku.

Kromě celkového řízení ISMS je jednou z dalších povinností manažera informovat vrcholové vedení podniku o stavu ISMS a slouží tak jako jakýsi mezičlánek mezi vrcholovým vedením podniku a zaměstnanci. V praxi manažer poskytuje pokyny, řídí a koordinuje činnosti zaměstnanců spojené s bezpečností informací [13].

1.5.2 Manažer kvality

Jedná se o osobu odpovědnou za celkové řízení kvality v podniku. Manažer stanovuje a zlepšuje procesy řízení kvality v celém podniku. Podílí se na vytváření interních směrnic a norem kvality a následně vyžaduje jejich dodržování. Manažer kvality řídí proces vytváření, udržování a rozvoje systému řízení kvality dle norem ISO nebo odvětvových standardů. Stejně jako manažer informační bezpečnosti informuje vrcholové vedení podniku o stavu kvality [14].

V praxi, pokud zaměstnanec je dostatečně vyškolený a způsobilý, může zastávat zároveň funkci manažera kvality i manažera informační bezpečnosti. Tato funkce se často pojmenovává jako „Představitel pro integrovaný systém řízení“. Funkce manažerů mohou být i svěřené externím společnostem, které poté externě koordinují a řídí systém řízení bezpečnosti informací nebo systém řízení kvality ve spolupráci s vedením podniku.

1.5.3 Garant aktiva

Garant aktiva je osoba, která má za cíl zajištění rozvoje, použití a bezpečnosti aktiva, ke kterému je přiřazena. Nejčastěji bývá touto osobou vedoucí určitého oddělení. Zajištěním bezpečnosti aktiva je v rámci ISMS myšleno zajištění tří bezpečnostních atributů u aktiva, tedy důvěrnosti, integrity a dostupnosti.

V praxi je garantovou odpovědností rozhodování u svěřených aktiv o jejich zabezpečení a na základě své znalosti aktiva a svého uvážení rozhoduje o tom, jaká opatření by měla být pro aktivum zavedena. Garant vždy svá rozhodnutí konzultuje s rolí, odpovídající za řízení a koordinaci systému řízení bezpečnosti informací [13].

1.5.4 Správce ICT

Jelikož garanti aktiv z velké části nejsou IT ani techničtí specialisté a rozhodují o bezpečnosti aktiv zejména z organizačního hlediska, musí existovat osoba, která úkony garanta aktiv technicky vykoná. Takovou osobou je správce ICT. Jeho odpovědností je plnit rozhodnutí garanta aktiva a manažera informační bezpečnosti z technické stránky. Garant se stará o správu, provoz, použití a údržbu aktiva. Nejčastěji tuto funkci ve společnosti zastává vedoucí IT oddělení nebo úseku.

1.5.5 Interní auditor

Interní auditor v podniku zajišťuje nezávislou, objektivní a poradenskou činnost, která je zaměřená na kontrolu a zdokonalování procesů v podniku. Auditor se může zaměřovat na kontrolu systémů, procesů nebo výrobku. Kontrolou pomáhá k rozvoji a zlepšování podniku. Interní auditor musí být vždy nezávislá osoba, která nezodpovídá pracovní činností za auditovaný systém, proces nebo výrobek. Interní audity může vykonávat i externí společnost, která bude mít nezávislý pohled na auditovanou oblast.

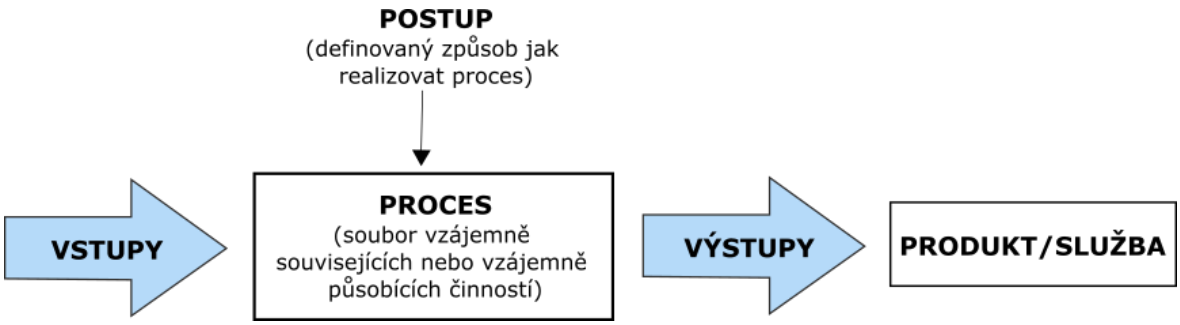
2 ŘÍZENÍ PROCESŮ

Pro pochopení řízení procesů v podniku je nutné nejprve vysvětlit, co samotný proces je. Procesy můžeme vidět na našich každodenních, opakujících se činnostech. Tyto opakující se činnosti se spojují v procesy. Jedná se o rutinní činnosti, které díky pravidelnému opakování děláme čím dál více automatičtěji a každým zopakováním tak zvyšujeme jejich efektivitu. Jelikož tyto procesy každodenně opakujeme, dochází ke zvyšování efektivity v jejich opakování, tímto způsobem zvyšujeme kvalitu a snižujeme časovou náročnost činností [15]. Dle Jiřího Urbánka v jeho knize „Teorie procesů“ je proces dynamická posloupnost vzájemně propojených činností, zdrojů nebo funkcí, které mají konkrétní cíl. Tímto cílem je přeměnit vstupy procesu na předem dané výstupy prostřednictvím možných činitelů, nástrojů nebo mechanismů [16].

Aby procesy a činnosti v nich správně fungovaly, je nutné zaručit určitá pravidla, kterými se budeme v procesu řídit, resp. je nutné zaručit, že tato pravidla budou námi řízena. Řízeny musí být na základě systémového přístupu, který umožnuje přezkoumávat a řídit pouze ty prvky, které odpovídají zájmu řízení procesu a účelu přezkoumávání. Aby byly procesy systémové, musí na sebe plynule navazovat podle předem definovaných pravidel a musí být současně řízeny [15].

Řízení procesů, neboli procesní přístup předpokládá, že hlavním objektem řízení je strukturovaný a jasně popsaný proces, který má zajištěné zdroje spolu s definovanými vstupy a výstupy. Takto definovaný proces zajišťuje přidanou hodnotu pro zákazníka a zodpovídá za něj jednoznačně přiřazený vlastník procesu. Při řízení procesů se management podniku zaměřuje na monitorování stanovených procesů v podniku, jejich analyzování, zlepšování a na jejich změny. Pokud jsou procesy v podniku správně nastaveny, zajišťují pro zákazníka kvalitní výrobky nebo služby.

Díky systémovému procesnímu řízení nahlížíme na podnik jako na systém mezi sebou provázaných procesů. Procesní řízení definuje i norma ČSN EN ISO 9001 jako systém, kde „požadovaného výsledku dosáhneme mnohem účinněji, jsou-li činnosti a související zdroje řízeny jako proces“.



Obrázek 2. Znázornění principu procesu [17]

Fungující procesní organizace přináší do podniku spoustu výhod oproti podniku, který je uspořádán útvarově. Procesní způsob uspořádání umožňuje manažerům kvalitní přehled o situaci v podniku zejména proto, že přináší nové možnosti provádění časových a finančních analýz v procesech a tím možné snižování provozních nákladů [15].

2.1 Procesní uspořádání

Uspořádání procesů má značný vliv na systémy řízení, jejich efektivitu a může snížit nutnou administrativu. Tato kapitola popisuje, jak by měly procesy být správně uspořádány a jaké nezbytné prvky se k procesům v rámci procesního řízení vážou.

2.1.1 Vlastník procesu

Vlastníkem procesu je osoba, která je v podniku zodpovědná za celkové řízení procesu, jeho rozvoj a koordinaci vnitřních činností. Pomáhá proces definovat tak, aby podniku přinesl co nejvíce přidanou hodnotu.

Vlastník nemusí nutně vykonávat jednotlivé činnosti procesu, musí jej však znát po teoretické a především praktické stránce. V praxi jsou vlastníci procesu manažeři, vedoucí daného oddělení nebo týmu podílejícího se na procesu [18].

2.1.2 Hranice procesů

Každý proces musí mít definovaný začátek a konec. Jedná se o místa, v nichž jednotlivé vstupy a výstupy do procesu vstupují a později ho opouštějí [15]. Procesy mohou být monitorovány mezi těmito hranicemi.

2.1.3 Vstupy a výstupy procesu

Vstupy procesu jsou výchozí zdroje podniku nebo výstupy z jiných, předcházejících procesů. Dále může být vstupem externí dodavatel nebo jeho činnost [15]. Vstupy dávají podnět k zahájení procesu a jsou pro jeho realizaci nezbytné.

Výstupy jsou výsledkem procesu a slouží poté jako vstup do následujícího procesu, nebo jsou přímo předány zákazníkovi v podobě produktu nebo služby. Jakmile proces dojde k jeho výstupu, je ukončen.

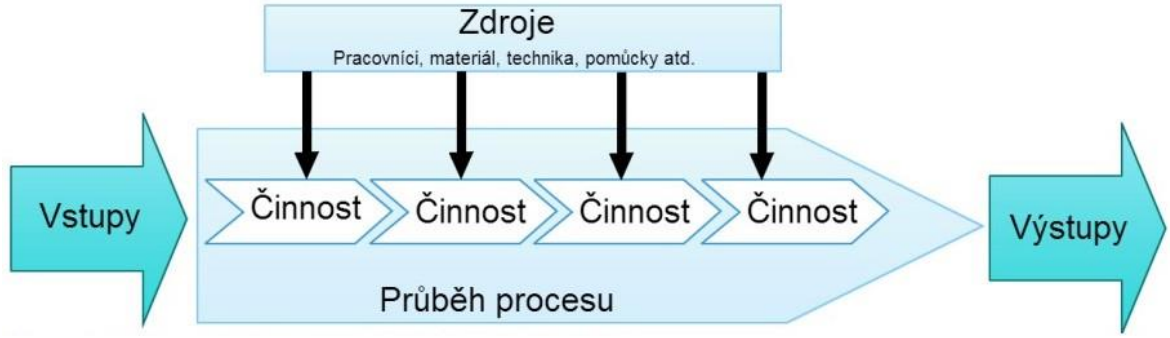
Vstupy procesu mohou být rozhodnutí vlastníků podniku, požadavky a očekávání zákazníků, legislativní požadavky, normativní požadavky nebo cíle podniku. Naopak výstupy procesu mohou být interní zdokumentované informace, strategické plány nebo konkrétní produkty [17].

2.1.4 Zdroje procesu

Zdroje procesu podnik využívá jako prostředek k přidání hodnoty vstupům, tedy k přeměně vstupů na výstupy. Jsou základními výrobními faktory a dělí se převážně na lidské zdroje, finanční zdroje, materiál, informace a znalosti, infrastrukturu nebo energii a čas.

Všechny zdroje podniku je nutné organizovat, plánovat, kontrolovat jejich stav a rozhodovat o jejich využití, aby nedošlo k jejich vyčerpání, jelikož jsou základním limitujícím prvkem pro každý podnik [19].

Příkladem zdrojů v podniku mohou být zaměstnanci, pracovní stroje, pracovní postupy, elektrický proud, dřevo pro výrobu, peníze a mnoho dalšího.



Obrázek 3. Začlenění zdrojů do procesu [20]

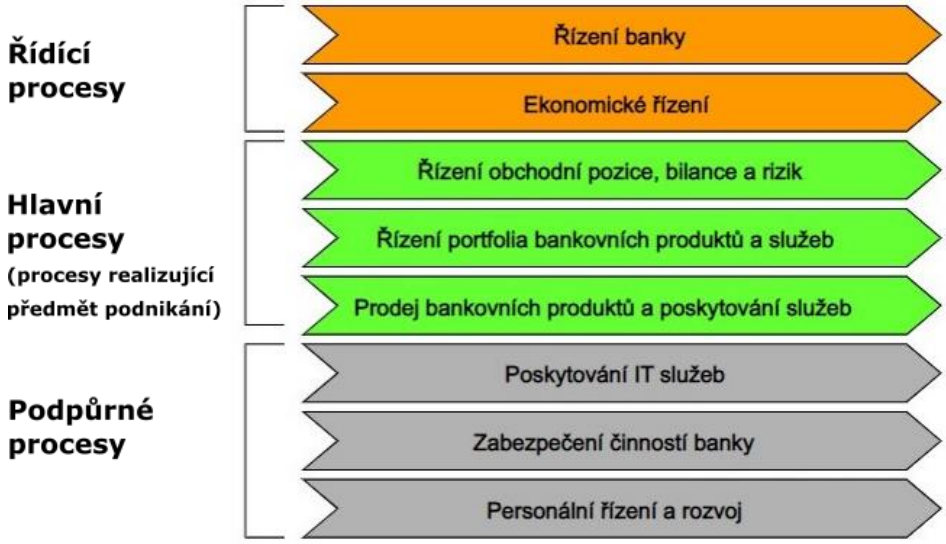
2.1.5 Členění a struktura procesů

Jelikož všechny procesy v podniku nemají stejnou váhu, je nutné je rozčlenit. Za nejdůležitější procesy v podniku jsou považovány procesy, které jsou hlavní činností podniku. Tyto procesy jsou pro podnik klíčové. Mohou jimi být výroba, služby nebo vývoj produktu.

Dalšími jsou řídící procesy, které v podniku určují správný směr rozvoje a dále zajišťují návaznost mezi řízením struktur podniku, strategií a operativou. Hlavními osobami v řídících procesech je vrcholový management a obsahem těchto činností může být tvoření interních směrnic, předpisů nebo plánování a řízení vztahů mezi zaměstnanci.

Třetí kategorií jsou podpůrné procesy. Úkolem těchto procesů je zajištění funkčnosti klíčových a řídících procesů. Patří mezi ně veškerá finanční, marketingová a logistická podpora spolu s řízením lidských zdrojů [15].

Stejně rozděluje procesy i norma ISO 9001, rovněž na hlavní, řídící a podpůrné. Na obrázku níže lze vidět praktický příklad rozdělení procesů v bankovnictví.



Obrázek 4. Praktická ukázka rozdělení procesů [21]

Pro celkový obraz podnikového pracovního toku se využívá tzv. procesní mapa. Tato mapa slouží jako nástroj pro popis podniku, nebo jeho části. Za pomoci procesní mapy můžeme analyzovat procesy, podprocesy a činnosti, které v těchto procesech probíhají [15].

2.2 Procesy spojené se systémem řízení bezpečnosti informací

Jelikož nikde není definováno, jak by v podniku měly být strukturovány procesy systému řízení bezpečnosti informací, je na každém podniku, aby si je samostatně stanovil. Pro tyto procesy je charakteristické, že se zaměřují na zavedení a udržování informační bezpečnosti v podniku. Těmito procesy můžeme zabezpečovat důvěrnost, integritu a dostupnost informací v podniku nebo jimi splňovat požadavky normy či legislativy.

Procesy systému řízení bezpečnosti informací mohou být stanoveny dle jednotlivých kapitol normy ISO/IEC 27001, tedy zavedení kontextu organizace, stanovení vůdčích rolí a podobně.

Dále mohou být procesy ISMS stanovené dle Přílohy A normy ISO/IEC 27001, ve které jsou popsána jednotlivá opatření, která musí podnik splňovat pro zajištění bezpečnosti informací. Procesy jsou často v tomto případě rozděleny dle jednotlivých kategorií opatření, jako jsou například: Mobilní zařízení a práce na dálku, Bezpečnost lidských zdrojů a další.

Je však čistě na daném podniku, jaké procesy pro ISMS si stanoví, vždy však budou mít za cíl splnění požadavků normy ISO/IEC 27001 nebo legislativy udávající povinnost zajistit bezpečnost informací a samotné zajištění bezpečnosti informací.

2.3 Procesní analýza

Procesní analýza je metoda, pomocí které analyzujeme tok činností v podniku a zjišťujeme nedostatky v procesech a jejich příčiny. Tato analýza je zaměřená na jednotlivé procesy od začátku procesu do jeho konce, přičemž popisuje jeho vstupy, výstupy, využití zdrojů a jednotlivé kroky v procesu. Zjednodušeně by se dalo říci, že procesní analýza je o tom, „jak se co dělá“ nebo „jak to probíhá“ [22].

Podniky mohou analyzovat své procesy, aby mohly být lépe popsány, lépe řízeny, či automatizovány nebo abychom mohli proces zlepšit a optimalizovat.

Analýza pomáhá podniku jednotlivé procesy identifikovat, popsat, vizualizovat a dát je do vzájemných souvislostí. Poskytuje detailní a přehledný pohled na podnikové procesy a zvýrazní jejich nedostatky či problémy. Výstupem procesní analýzy mohou být procesní modely, celková mapa procesů, nebo slovní či strukturovaný popis procesů [22].

Jednou z používaných metod procesní analýzy je i Demingův cyklus, popsaný v kapitole 1.3.

2.3.1 Analýza vnitřní stavby procesu

Tento typ analýzy je jeden z těch nejelementárnějších a představuje základní analýzu vnitřní struktury procesu. Zabývá se jeho logikou, posloupností, efektivitou a při této analýze je porovnáván s jinými, podobně řešenými procesy. Za pomoci tohoto porovnání zkoumá nedostatky a jejich možné příčiny [15].

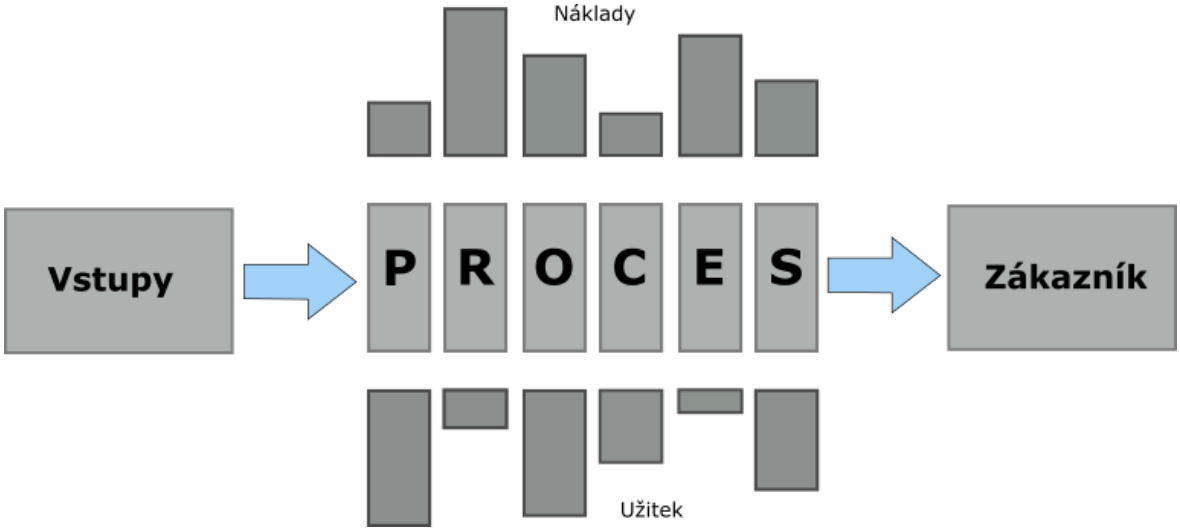
Svým způsobem je tato metoda založená na benchmarkingu[1], protože systematicky měří a porovnává vybrané ukazatele.

Při analýze se zaměřuje na celkovou strukturu procesu, to znamená i s jeho podprocesy a porovnává činnosti s normami nebo normativy. Monitorují se případné odchylky od předpokládaného stavu a zkoumá se, zda činnosti nemohly probíhat a fungovat jinak a lépe [15].

2.3.2 Analýza přidané hodnoty procesu

Pro zvýšení účinnosti procesů jsou při této analýze porovnány náklady na zdroje, které byly přidruženy k danému procesu nebo uskupení procesů se získanou funkcionalitou procesu. Zjednodušeně to znamená, že jsou porovnávány jednotlivé procesy spolu s činnostmi a vynaloženými zdroji, zda mají přidanou hodnotu vzhledem k užitku a požadavkům zákazníka. Pokud je při analýze zjištěno, že některá z činností nemá přidanou hodnotu (např. příliš vysoká cena za dopravu, nadměrná administrace), jsou u těchto činností náklady sníženy na co nejnižší úroveň, pokud nemohou být přímo eliminovány.

[1] proces porovnávání a měření produktů, procesů a metod vlastní organizace s jinou organizací, za účelem definovat cíle zlepšování vlastních aktivit



Obrázek 5. Procesní analýza nákladů a užitku pro zákazníka [17]

2.3.3 Analýza rizik

Mnoho podniků považuje za nebezpečná pouze rizika spojená s ekonomickým výsledkem Riziko pro podnik však může mít i množství jiných podob, např. obchodní, technické, personální atd. Riziko je tak součástí fungování podniku a musí být od něho odvozeny činnosti podniku a jeho organizační členění.

V rámci procesní analýzy je předmětem analýzy rizik nalézt činnosti v procesech, které představují jakékoliv riziko pro podnik a zajistit u nich minimalizaci jejich vzniku, popřípadě minimalizovat jejich dopad na podnik.

Součástí analýzy rizik je monitorování potencionálních rizik, pramenících z procesních činností, z toho vyplývá možnost mít tak organizaci lépe pod kontrolou [15].

V praxi je často postup při analýze rizik vymezen na čtyři části:

1. Vymezení obsahu analýzy rizik, identifikace jednotlivých rizik a určení jejich významnosti pro podnik.
2. Rozdělení rizik na ta, na která je nutné reagovat a na ta, na která to nutné není.
3. Definování přístupů a opatření pro snížení rizika v procesu nebo úplnému vyhnutí se riziku.
4. Monitorování a přezkoumání systému analýzy rizik [15].

2.4 Analýza chování procesů

Analýzu chování procesů můžeme považovat za část procesní analýzy. Při této analýze zkoumáme celkovou stabilitu procesu a možné variability námi měřených prvků. Tyto prvky zkoumáme v určitém čase nebo při určité činnosti a dostáváme tak přehled o chování (průběhu). Při analýze využíváme takzvané metriky, mohou se nazývat i indikátory kvality, norma ISO/IEC 27004 je nazývá mírami. Právě jejich chování, popřípadě odchylky monitorujeme a vyhodnocujeme.

Cílem analýzy chování procesů je nalézt odchylky za pomoci metrik v sesbíraných informacích. Tyto odchylky značí nestabilitu a nesprávný průběh procesu, který se poté snažíme odstranit.

Výstup z analýzy můžeme znázornit čísly, slovně, nebo využít vyjádření za pomocí grafů, které je popsáno v kapitole 2.4.2.

2.4.1 Vyhodnocování procesu

Abychom zjistili, zda proces probíhá dle námi stanovených kritérií, je nutné, aby si podnik stanovil limity. Za pomocí těchto limitů bude v analýze zkoumáno, zda nasbírané informace jsou v rámci těchto limitů [23]. Jako limity pro vyhodnocení procesu můžeme definovat patřičné metriky, viz kapitola 2.5.2.

Při analýze si podnik určí činnost nebo časový úsek, po který bude probíhat analýza a definuje si patřičné metriky. Po dobu této analýzy sbírá informace, popřípadě data, o probíhající činnosti či činnostech a tyto informace poté vyhodnotí. Pokud je při přezkoumání informací odhaleno, že některá z posbíraných relevantních informací překročila námi stanovený limit, jde o odchylku, jejímuž opakování se podnik poté snaží vyhnout, nebo snížit její pravděpodobnost.

Pro provedení analýzy chování a její vyhodnocení musíme znát, jak se má daný proces chovat. Lepšího vyhodnocení docílíme, pokud existují historická data, která by už popisovala výkonnost a chování procesu, se kterými bychom nově posbírané informace porovnali.

Odchylky vzniklé překročením pevných, např. zákazníkem stanovených limitů, jsou neměnné a při jejich vzniku se jedná o neshodu. Pokud není definována metrika s pevným limitem, na kterou by bylo nutné ihned reagovat, lze informace sledovat v čase a vyhodnocovat chování na základě shromážděných informací. Takové vyjádření informací

je nejčastěji, jak je uvedeno výše, vyobrazeno kontrolním grafem. Na grafu lze sledovat, zda námi naměřené hodnoty překračují stanovené limity a jak často nebo v jaké míře byly překročeny. Na základě těchto informací lze zavádět patřičná opatření pro snížení pravděpodobnosti odchylky nebo se může podnik rozhodnout, i vzhledem k naměřeným hodnotám, změnit dané limity.

2.4.2 Grafické znázornění chování procesu

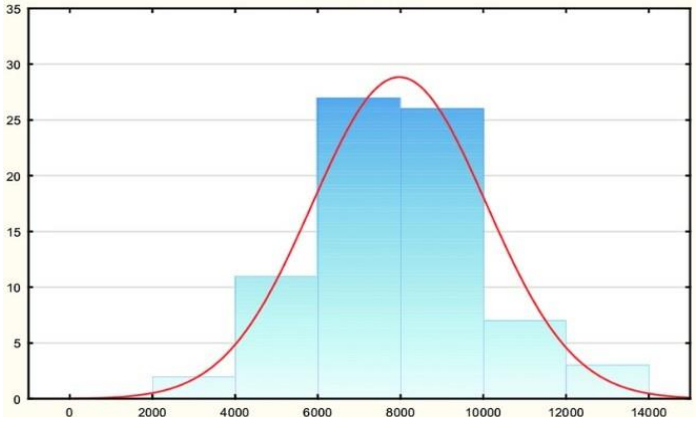
Po naměření a zaznamenání všech hodnot se v praxi využívají pro interpretaci a přehlednější vyhodnocení těchto hodnot grafická znázornění. Správná volba grafického znázornění chování procesu může podniku rychleji dopomoci k nalezení kořenové příčiny odchylek procesu, tedy nesprávného chování.

2.4.2.1 Histogram

V histogramu můžeme informace vyjádřit sloupci o stejné šířce, znázorňující naměřená statistická data. Šířka sloupce nám znázorňuje určitý interval čísel a výška sloupců nám vyjadřuje počet výskytů této hodnoty v daném intervalu. Zvolení nesprávné šířky intervalu může snížit informační hodnotu diagramu a vést tak ke zkreslení informací [24].

Pro histogram využíváme číselné hodnoty o běhu procesu, nebo činnosti. Jeho pomocí určíme, zda se naměřené hodnoty chovají v rámci stanovených kritérií a zda vyhovují požadavkům. Z diagramu je také možné sledovat, kdy došlo ke změnám v procesu a můžeme podle něj porovnávat výstupy ze dvou různých procesů.

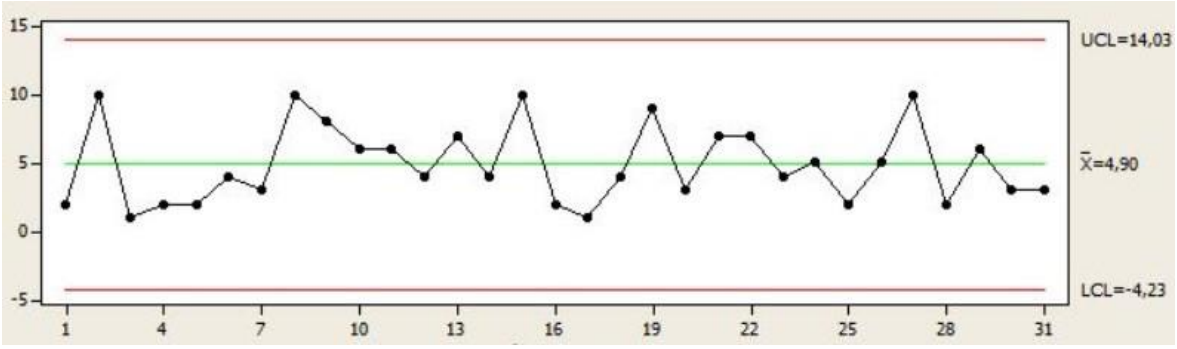
Výška sloupců je často porovnávána s kontrolním limitem, který znázorňuje hraniční, vertikální linie. Tato linie nám udává, že pokud výška sloupce přesáhla stanovený limit, proces je nestabilní a budou zavedeny patřičné kroky k nápravě procesu, nebo k tomu, aby se toto vychýlení už neopakovalo [25].



Obrázek 6. Chování procesu vyjádřené histogramem [26]

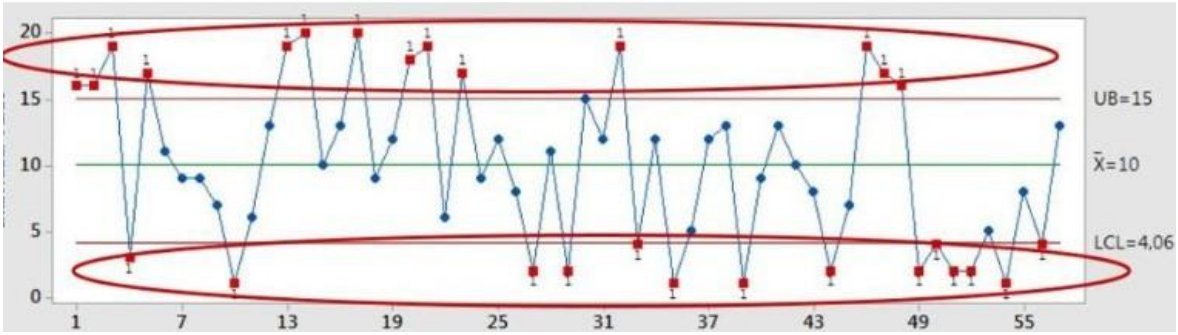
2.4.2.2 Regulační diagram

Regulační digram je v praxi nejpoužívanější interpretace naměřených hodnot. Při použití regulačního diagramu je chování procesu vyobrazené vždy středovou linií (označována jako CL - Central Line), která nám znázorňuje průměr naměřených hodnot. Dále jsou vyobrazeny hraniční linie na horní (označována jako UCL - Upper Control Line) a spodní straně středové linie (označována jako LCL - Lower Control Line), které znázorňují stanovené, kontrolní limity. Spodní linie nemusí být vždy součástí grafu, jelikož můžeme měřit pouze přesáhnutí určité hodnoty. Taková linie by se použila v případě monitorování, např. počtu chyb. Můžeme také vyznačit tzv. výstražné meze, tedy horní výstražnou mez (UWL – Upper Warning Limit) a dolní výstražnou mez (LWL – Lower Warning Limit). [24].



Obrázek 7. Příklad regulačního diagramu [24]

Data, která jsou v grafu vyobrazena, představují hodnoty jednotlivých měření v čase. V případě překročení hodnoty, v horní nebo dolní linii, jde o porušení stability procesu.



Obrázek 8. Příklad neustáleného procesního stavu [24]

Nestabilita procesu může být také vyhodnocena nejen při překročení stanovených limitů, ale i na daném chování procesu na základě naměřených hodnot. Např. může být z grafu viditelné, že naměřené hodnoty se periodicky mění v čase a proces tak neprobíhá konstantně, nebo že se naměřené hodnoty v určitém časovém úseku odchylují z horní hranice k dolní hranici. Jde o takzvané sledování trendů, tedy identifikaci neobvyklých vzorů v naměřených

hodnotách. Tato analýza z grafického znázornění chování procesu může také značně pomoci podniku k odstranění příčin nestability procesu [23]. Nejčastějšími vzory při sledování trendů, které nám poukazují na nestabilitu procesu, jsou:

- Kompozice – Tento trend je charakterizován sdružením podobných hodnot v okolí dvou nebo více navzájem různých středových linií. Takové sdružení hodnot může charakterizovat složení tohoto procesu z více podprocesů, z nichž každý má jinou středovou linii. V tomto případě se proces rozděluje na podprocesy a každý jednotlivý podproces se analyzuje a vyhodnocuje zvlášť.
- Cyklus – Cyklus je charakteristický periodickými změnami v naměřených hodnotách. V trendu lze vidět, že chování procesu se neustále opakuje v určitých cyklech. Lze z něho tedy vyčíst určité pravidelné časové úseky, kdy se snižují hodnoty. Takový trend může být zapříčiněný například nesouladem činností při výrobě nějakého produktu.
- Skok – Při tomto chování dochází v procesu k náhlým odchýlením hodnot směrem nahoru nebo dolů od předchozích hodnot. Chování naznačuje prudké zvýšení nebo snížení efektivity v procesu, které může být zapříčiněné například přijetím nového zaměstnance do procesu.
- Shlukování – Toto chování, nebo-li tento trend, je charakteristické shluknutím několika velmi blízkých hodnot, které trvají několik jednotek měření. Tento trend může způsobit nedostatečná specifikace v pracovním postupu, kdy při nedostatečných informacích je vždy zpomalen proces.
- Stratifikace – Tento graf je charakteristický rozmístěním všech hodnot velmi blízko středové linii a lze z něho vidět, že žádná z hodnot se nijak nepřibližuje stanoveným limitům. V tomto případě může jít o nesprávně nastavenou metriku nebo nepřesné měření [23].

2.5 Monitorování a měření efektivnosti procesů

Měření výkonnosti procesů je považováno za důležitý prvek řízení kvality v podnicích. Aby společnost věděla, zda její procesy fungují a měla příležitost je zlepšit a provést v nich změny, musí mít podnik znalosti o těchto procesech a jejich výkonnosti. Z tohoto důvodu se zavádí měření výkonnosti procesů.

V případě, že je podnik certifikován ISO normou, je jeho povinností zavést metody monitorování a měření procesů nebo bezpečnostních opatření, které prokáží schopnost

procesů dosáhnout naplánovaných cílů. V případě, že těchto výsledků není dosaženo, musí podnik určit dostatečnou nápravu, popřípadě provést opatření k nápravě [15].

Pro účely této práce bude popsán převážně způsob měření procesů spojených se systémem řízení bezpečnosti informací. Pro toto měření a návrh metrik je vytvořena norma ISO 27004, které se tato práce bude více věnovat. Norma se zaměřuje na měření naplnění cílů v procesech, týkajících se bezpečnosti informací, kterých se snaží dosáhnout zachováním důvěrnosti, integrity a dostupnosti informací v podniku.

Monitorování a měření efektivnosti procesů bezpečnosti informací umožní podniku zvýšit odpovědnost zaměstnanců za bezpečnost informací, zvýšit výkonnost zabezpečení a demonstrovat pokrok v dosažení cílů bezpečnosti informací podniku. Dále výsledky metrik slouží podniku jako důkazy o splnění požadavků norem a umožní podniku měřit úspěchy a selhání současných bezpečnostních opatření [27].

2.5.1 Fáze měření efektivnosti procesů

Průběh celého monitorování a měření efektivnosti systému řízení bezpečnosti informací lze rozdělit do následujících fází:

1. Identifikace informačních potřeb – Pro vytvoření metrik by měla být v této fázi provedena identifikace informačních potřeb, které mohou pomoci v pochopení provozu, nebo výkonnosti jakéhokoliv aspektu ISMS. Mohou jimi být politiky a cíle podniku, strategické směřování, schopnosti při zajištění zdrojů a priorita při ošetřování rizik (viz 2.3).
2. Vytvoření a udržování metrik – V této fázi jsou vytvořeny metriky, pro měření efektivity, které by měly reagovat na informace získané z bodu 1. Metriky by měly být identifikovány dostatečně podrobně, aby mohly být implementovány do provozu podniku. Měly by být rovněž pravidelně přezkoumávány, zda jsou stále aktuální. Přezkoumání by mělo také nastat, pokud v prostředí informační bezpečnosti dojde k podstatným změnám.
3. Stanovení postupů – Před samotným měřením musí být v této fázi definováno, jak budou data shromažďována, uchovávána a jakým způsobem budou ověřena. Dále musí být stanoven postup pro analýzu dat a četnost nahlášení výsledků metrik, spolu se stanovením metody podávání výsledků metrik.

4. Monitorování a měření – V této fázi jsou manuálním nebo automatizovaným způsobem informace dle definovaných postupů shromážděny, uchovány, ověřeny a připraveny na vyhodnocení.
5. Analýza výsledků měření – Během této fáze jsou shromážděná data pro každou jednotlivou metriku analyzována ve vztahu k vybranému cíli. Odpovědné osoby analyzující výsledky by měly být schopné dospět na základě těchto výsledků k identifikaci rozdílů mezi očekávanými a aktuálními výsledky měření.
6. Vyhodnocení efektivnosti bezpečnosti informací – Odpovědnou osobou jsou v této fázi posouzeny výsledky analýzy, zda odpovídají stanoveným informačním potřebám podniku, cílům a zda je proces efektivní.
7. Uchování a komunikování zdokumentovaných informací – Pro splnění povinnosti normy musí být v této fázi zdokumentovány všechny informace sloužící jako důkaz proběhlého monitorování a měření v daném podniku. Výsledky monitorování a měření by měly být sděleny odpovídajícím zainteresovaným stranám, kterými mohou být například management, věřitelé, nebo zákazníci [27].

2.5.2 Metriky efektivnosti procesů

Jak už bylo řečeno výše, metriky efektivnosti procesů jsou ukazatele, díky kterým podnik může zjistit efektivnost daného procesu nebo jeho části a také určit do jaké míry jsou splňovány cíle procesu vzhledem ke strategickým cílům podniku.

Jelikož je tato práce zaměřena na metriky efektivnosti procesů spojených se systémem řízení bezpečnosti informací, přiblížíme si, co je očekáváno od měření těmito metrikami.

Z důvodu zaměření procesů ISMS na zabezpečení důvěrnosti, integrity a dostupnosti informací (viz kapitola 2.2), by nám měly metriky měření efektivity těchto procesů udávat přehled o efektivitě zabezpečení informací v podniku. Metriky efektivity dle normy ISO/IEC 27004:2018 slouží k popisu efektivnosti a dopadu plánu na ošetření rizik, nebo k určení, zda procesy ISMS a opatření bezpečnosti informací fungují tak, jak bylo plánováno a zjištění, zda dosahují požadovaných výsledků [27].

V podniku by každá metrika měla být dokumentovaná formou, která je přizpůsobená příslušné informační potřebě (nebo potřebami) a poskytuje dostatečné informace o charakteristikách popisujících metriku. Také by měla poskytovat představu, jak pro ni informace shromažďovat, analyzovat a jak o nich podávat zprávu [27].

Pro měření efektivity procesů ISMS a měření bezpečnosti informací v podniku, je normou ISO/IEC 27004:2018 stanovena šablona pro definování všech potřebných, výše popsaných informací o metrice. Pro pochopení objasňuji, že výraz metrika je nahrazen výrazem míra. Šablona pro definování metrik je následující:

Tabulka 1. Šablona pro definici metrik ISMS [27]

Deskriptor informací	**Význam nebo účel**
ID míry	Specifický identifikátor.
Informační potřeba	Překlenující potřeba pro porozumění, ke kterému míra přispívá.
Míra	Prohlášení o měření, obecně popisováno s použitím slov jako „procento“, „počet“, „četnost“ a „průměr“.
Vzorec/bodování	Jak by měla být míra ohodnocena, vypočtena nebo obodována.
Cíl	Požadovaný výsledek měření, například milník nebo statistická míra nebo sada prahových hodnot. Pro zajištění trvalého dosažení cíle může být vyžadováno nepřerušené monitorování.
Důkaz implementace	Důkaz, který potvrzuje, že měření je provedeno, pomáhá identifikovat možné příčiny špatných výsledků, a poskytuje vstup do procesu. Tato data vstupují do vzorce.
Četnost	Jak často by měla být data shromažďována a hlášena. Může existovat důvod pro vícenásobné četnosti.
Odpovědné strany	Osoba odpovědná za získávání a zpracování míry. Měli by být identifikováni alespoň vlastník informací, osoba shromažďující informaci a zákazník měření.
Zdroj dat	Potenciálními zdroji dat mohou být databáze, sledovací nástroje, jiné části organizace, externí organizace, nebo specifické jednotlivé role.
Formát podávání zpráv	Jak by měla být míra shromažďována a hlášena, například jako text, numericky, graficky (kruhový graf, čárový graf, sloupcový graf atd.), jako část „stránky s přehledem“ nebo jiná forma prezentace.

Tato šablona bude v této práci použita pro definování všech potřebných informací o metrikách při stanovování potřebných metrik.

3 PRVKY BEZPEČNOSTI INFORMACÍ

Prvky bezpečnosti informací jsou technické a programové nástroje, či systémové činnosti, které zabezpečují důvěrnost, integritu nebo dostupnost informací podniku.

3.1 Antivirový program

Dle normy ISO/IEC 27002 je implementace aktivní a aktuální ochrany antivirovým programem jedno z nejdůležitějších opatření pro hrozby škodlivých programů, které mohou napadnout výpočetní zařízení a ohrozit tak bezpečnost informací podniku [28]. Antivirový program sleduje nejdůležitější místa, ať už jsou vstupní nebo výstupní, kterými by se mohl škodlivý program dostat do počítačového systému podniku. Sledováním těchto míst se snaží proniknutí škodlivých programů předcházet [29].

Antivirový program by měl být nainstalován na všech výpočetních zařízeních, která pracují s informacemi podniku a mají přístup do počítačové sítě podniku. Tato zařízení spolu s antivirovým programem by měla být pravidelně aktualizována, aby se předcházelo nově vzniklým hrozbám.

3.2 Firewall

Firewall je hardwarový nebo softwarový prvek, který v počítačové síti povoluje nebo naopak blokuje příchozí a odchozí komunikaci. Toto povolování a blokování provádí na základě nastavených pravidel. Tato pravidla mohou být přednastavená, nebo zvolená uživatelem [30]. Jelikož se jedná z hlediska bezpečnosti o jakousi základní bránu mezi bezpečností počítačové sítě podniku a vnějšími hrozbami, měl by každý podnik klást velký důraz na jeho správu.

Jak uvádí publikace „CyberSecurity“ docenta Jana Koloucha, ke zvýšení bezpečnosti je nutné nastavit firewall jako aplikační bránu (proxy bránu), nebo jako stavový paketový filtr pro filtrování příchozí a odchozí komunikace ze sítě [31].

Proxy brána slouží jako komunikační prostředník mezi klientem (uživatelem) a cílovým serverem. Proxy brána překládá požadavky klienta vůči serveru a přebírá jeho odpověď, kterou doručuje zpět klientovi. Během komunikace blokuje příchozí komunikaci podle jejího obsahu [32].

3.3 VPN (Virtual private network)

V případě, že je nutné propojit dvě zařízení a předávané informace mezi zařízeními nesmí být přístupné jakékoliv třetí osobě, je vhodné zvolit VPN. VPN je bezpečné propojení dvou a více zařízení. Mezi zařízeními se vytvoří tzv. tunel, v němž se přenáší všechny informace šifrovaně. Tuto metodu je vhodné využít např. při práci zaměstnanců mimo pracoviště v případě, že se potřebují připojit do sítě společnosti nebo při komunikaci více poboček společnosti [33].

3.4 Management logů

Důležitou součástí bezpečného provozu systémů, služeb a aplikací je zaznamenávání informací o jejich činnosti a běhu, tzv. logování. Záznamy (logy) mohou být ukládány ve formě prostého textového souboru, nebo mohou být ukládány do databázového souboru [31].

Logy slouží nejčastěji správci sítě nebo IT zaměstnanci ke zpětné analýze a zjištění, zda došlo k chybě, případně slouží také k určení, kdy a proč k chybě došlo.

Obecný koncept managementu logů je, že na centrální nástroj jsou sbírány logy z různých ostatních nástrojů. Tyto logy je možné poté vytřídit, vybrat pouze ty, které uživatele zajímají a ty si buď virtualizovat, nebo si nastavit upozorňování při zjištění nějakého nestandardního chování. Monitorování logů může být tedy užitečné pro včasné zachycení počítačového útoku, kontrolu uživatele a i mnoho dalších důvodů [34].

3.5 Analýza dopadů

Analýza dopadů, anglicky Business Impact Analysis (zkráceně BIA), má v IT oblasti za cíl zjistit, jaké aplikace nebo služby uživatelé potřebují a jaké dopady pro podnik by měla jejich nedostupnost či ztráta jejich dat.

Výsledky analýzy se využívají pro řízení kontinuity podnikání a umožňují podniku efektivně připravit plány kontinuity, zálohovací scénáře a záložní řešení v případě havárie či nedostupnosti IT systémů [35].

3.6 Zálohování dat

Zálohování dat je proces, při kterém je uložena kopie dat z jednoho datového nosiče na jiný datový nosič. Zálohovaná data mohou být poté využita v případě ztráty, poškození nebo jiné potřeby práce s daty uloženými v minulosti.

4 HROZBY PRO BEZPEČNOST INFORMACÍ

Hrozby jsou nežádoucí situace využívající zranitelností, které umožňující útočníkovi provést neoprávněnou nebo nevyžádanou akci, která by vedla k porušení bezpečnosti informací. V kapitolách níže si určíme, jak se pro podniky mohou tyto hrozby rozdělovat.

4.1 Vnější hrozby

Vnějšími hrozbami pro bezpečnost informací jsou takové hrozby, které jsou vedeny útočníky mimo počítačovou síť podniku.

4.1.1 Škodlivý kód

Jedná se o počítačový program nebo jakýkoliv kus programového kódu, vytvořený za účelem napadení uživatele. Napadení spočívá ve vniknutí do systému (jeho infikování) za účelem jeho poškození, ovládnutí, odcizení dat a sledování uživatele.

Pokud se jedná o dobře navrhnutý škodlivý kód (malware), je tato skutečnost pro běžného uživatele jen stěží odhalitelná. Napadení zařízení malwarem lze odhalit odbornými zaměstnanci například monitorováním komunikace zařízení v rámci internetu a monitorování chování zařízení [36].

4.1.2 Sociální inženýrství

Vnějšími hrozbami pro bezpečnost informací jsou takové hrozby, které jsou vedeny útočníky mimo počítačovou síť podniku.

Jedním z velmi rostoucích a nejčastějších typů vnějších útoků je sociální inženýrství. Tento útok se zaměřuje na selhání lidského faktoru, tedy zaměstnanců. Cílem je klamavým dojmem docílit získání informací nebo se dostat do počítačové sítě společnosti. Útok využívá řady triků, manipulačních technik nebo obcházení zabezpečení k tomu, aby uživatele obelstil k dobrovolnému vydání chráněné informace, nebo aby uživatel udělal úkon, který útočník požaduje [37].

Nejčastějším příkladem sociálního inženýrství je tzv. phishing, kdy např. velmi důvěryhodně vypadající e-mailová zpráva upozorňuje uživatele na nějaký problém. Ke vzniku tohoto problému nejčastěji stačí zadání osobních údajů o uživateli nebo zadání přístupových údajů (např. do IS společnosti nebo bankovnictví), čímž tyto údaje získá útočník [38].

4.2 Vnitřní hrozby

Vnitřní hrozby pro bezpečnost informací pochází z prostředí společnosti. Nejčastější vnitřní hrozbou je pochybení zaměstnanců. Dalšími vnitřními hrozbami může být např. povolení zařízení, které nemá společnost ve správě a nijak nerozhoduje o jeho zabezpečení, nebo porucha zařízení, které ohrozí bezpečnost informací.

4.2.1 Zaměstnanci

Lidský faktor je v současnosti nejzávažnější vnitřní hrozbou v podnicích. Zapříčiněno je to často nedostatkem odborníků na vykonávanou pracovní činnost, nebo neznalostí bezpečnostních pravidel při jejich pracovní činnosti. Norma ISO/IEC 27005 uvádí, že příčinou ohrožení bezpečnosti informací ze strany zaměstnance může být jeho zvědavost, ego, finanční prospěch v případě zneužití chráněných informací nebo úmyslné poškození společnosti bývalým zaměstnancem [39].

Pro předcházení hrozbám ze strany zaměstnanců by měla společnost ustanovit organizační a technická opatření nebo pravidla, která budou po zaměstnancích vyžadována. Dále by měli být zaměstnanci dostatečně a pravidelně školeni v oblasti bezpečnosti informací na základě údajů, ke kterým mohou mít přístup.

4.2.2 Paměťová média

Na základě bezpečnostních instrukcí vydaných Agenturou pro kybernetickou bezpečnost a infrastrukturu (CISA) jsou velkým bezpečnostním rizikem připojující se USB zařízení. USB zařízení může být využito pro infikování mobilního zařízení škodlivým kódem. Zaměstnanec může zařízení infikovat nevědomě, například stáhnutím malwaru na USB při osobním použití a poté jeho následujícím využitím v pracovní činnosti. V některých případech mohou zaměstnanci použít USB zařízení, která nejsou v jejich vlastnictví, pouze byla zaměstnanci nalezena a nejsou si sami vědomi jejích obsahu [40].

Bezpečnostní instrukce vydané agenturou CISA doporučují, aby zaměstnanci měli zakázáno používaní jakýchkoliv cizích USB zařízení, které jim nebyly poskytnuty organizací. Dále CISA uvádí, aby antivirové programy, implementované na mobilních zařízeních, vždy automaticky skenovaly USB zařízení a nepovolily jeho použití, dokud nebude skenování úspěšné [40].

II. ANALÝZA SOUČASNÉHO STAVU

5 CHARAKTERISTIKA PODNIKU

Informace získané pro stručnou charakteristiku podniku a pro představení současného stavu podniku, byly zjištěny během několika konzultací s vedením podniku, jmenovanými manažery v rámci integrovaného systému řízení a jinými vedoucími pracovníky jednotlivých oddělení. Dále byly informace, které jsou představeny v těchto kapitolách, shromážděny seznámením se s pracovní činností zaměstnanců, s navrhnutou strukturou IMS a analýzou výrobních procesů podniku.

Z důvodů zajištění bezpečnosti podniku bylo rozhodnuto, že podnik, který poskytl informace k vypracování této práce, nebude v této práci jmenován. Důvodem je nevhodnost zveřejnění rizik, zranitelností a využití procesních postupů, které mohou být proti podniku zneužitelné.

V následujících kapitolách bych rád popsal základní informace o vybraném podniku pro pochopení problematiky a představení stavu integrovaného systému řízení a podnikových procesů.

5.1 Předmět podnikání

Hlavní činností výše uvedeného podniku je poskytování komplexních služeb zahrnující vývoj softwaru, ICT služeb, tiskových služeb, dodávky hardwaru, budování datových sítí a kamerových systémů. Dále podnik dodává výpočetní a kancelářskou techniku.

Jedním z hlavních prvků portfolia podniku je i provozování služby operátora sítě, kdy pomocí tohoto systému provádí transakční výměnu získaných informací mezi dvěma stranami danými zákazníkem.

5.2 Základní údaje o podniku

Podnik vznikl a působí v České republice a v okolních státech České republiky. Sídlo podniku a pracoviště se nachází pouze na jednom místě v Jižních Čechách.

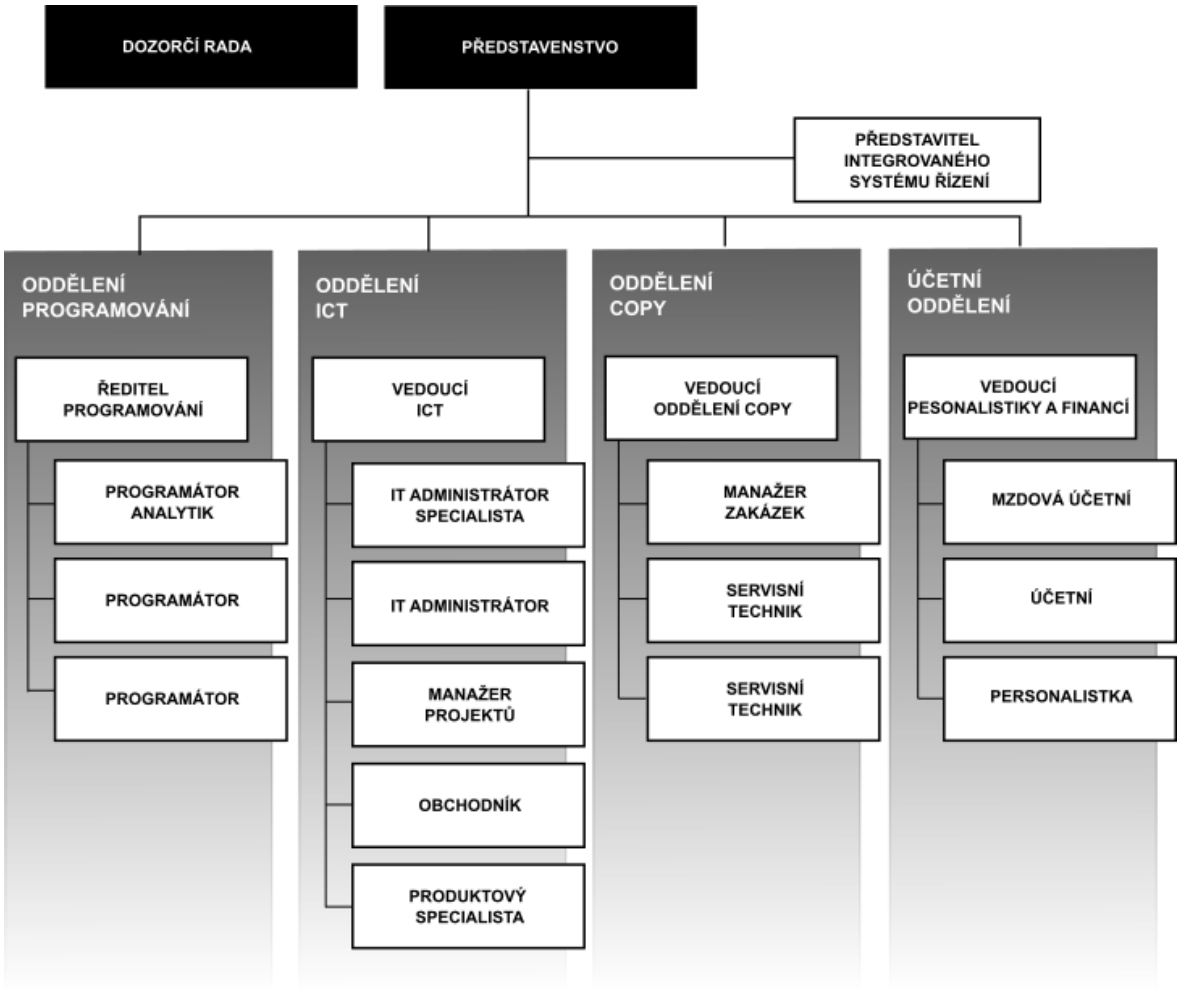
Podnik je akciová společnost s dvaceti zaměstnanci a hodnota aktiv podniku nepřesahuje 100 000 000 Kč. Jedná se tak dle zákona č. 563/1991 Sb., zákon o účetnictví o malou účetní jednotku [41].

Struktura v podniku je rozdělena na 4 oddělení a vedením podniku je pověřeno jeho představenstvo. Každé oddělení má svého vedoucího pracovníka a dělí se na:

- oddělení programování;
- oddělení ICT;
- oddělení copy;
- účetní oddělení.

Pokud je v podniku vytvořen projekt, může být do něho zapojeno více oddělení. V těchto případech vede a zodpovídá za projekt vybraný projektový manažer, který se zodpovídá předsedovi představenstva. Právní záležitosti jsou zajišťovány externí společností.

5.3 Organizační schéma podniku



Obrázek 9: Organizační schéma podniku [zdroj: vlastní tvorba]

6 ROZSAH SYSTÉMU ŘÍZENÍ KVALITY

Podnik od listopadu roku 2021 pracuje na implementaci systému řízení kvality, dle normy ISO 9001, který ve chvíli, kdy je psána tato práce, není ještě certifikován a metriky, které jsou navrhnuty v této práci, se stanou součástí metrik představených v procesu měření a zlepšování integrovaného systému řízení při certifikačním auditu.

Jako rozsah integrovaného systému řízení byly zvoleny následující činnosti podniku:

- Návrh, vývoj, implementace a údržba softwaru
- Dodávky a servis systémových řešení
- Poskytování služeb správy a údržby ICT (Helpdesk)
- Služby přenosu dat

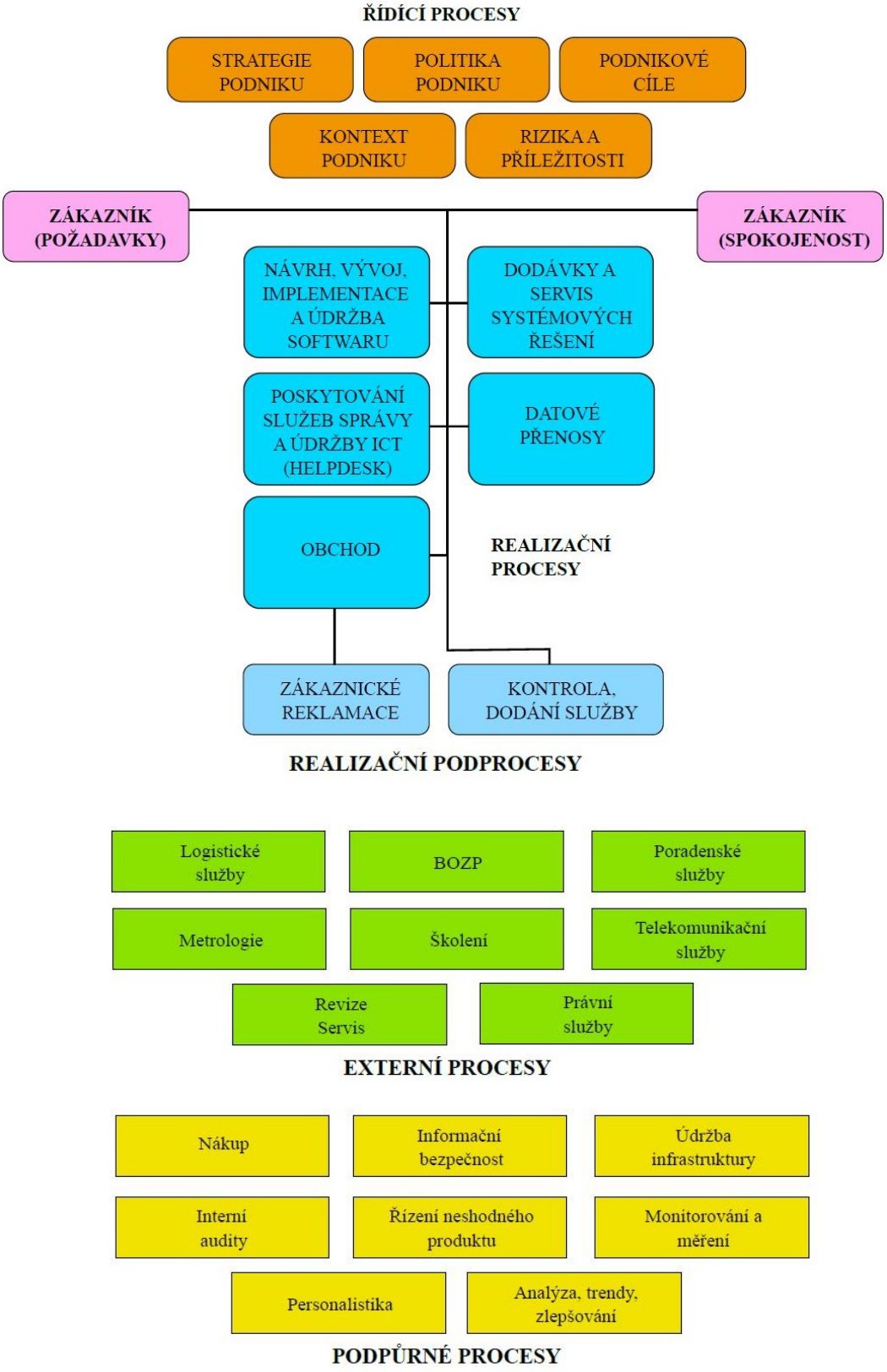
V rozsahu systému je pokryt celý podnik dle organizačního schématu a všechny provozované procesy a služby.

Za účelem řízení kvality jsou v podniku rozděleny procesy na řídící, realizační, externí a podpůrné. Jejich celkový přehled, tedy procesní schéma, je znázorněn v následující kapitole.

Pro rozdělení odpovědností v rámci integrovaného systému řízení zastává jednatel společnosti funkci Představitele pro integrovaný systém řízení. Jeho odpovědností je schvalování dokumentace, cílů, výsledků analýz a jiných rozhodnutí pro řízení IMS, předložených jednotlivými manažery v rámci IMS.

Jelikož v podniku není nikdo, kdo by měl odborné znalosti pro zastávání funkce manažera kvality, je tato funkce zastávána externí společností. V rámci systému řízení bezpečnosti informací jsou zvoleni dva Manažeři informační bezpečnosti, vybraní ze zaměstnanců podniku, více v kapitole 7.

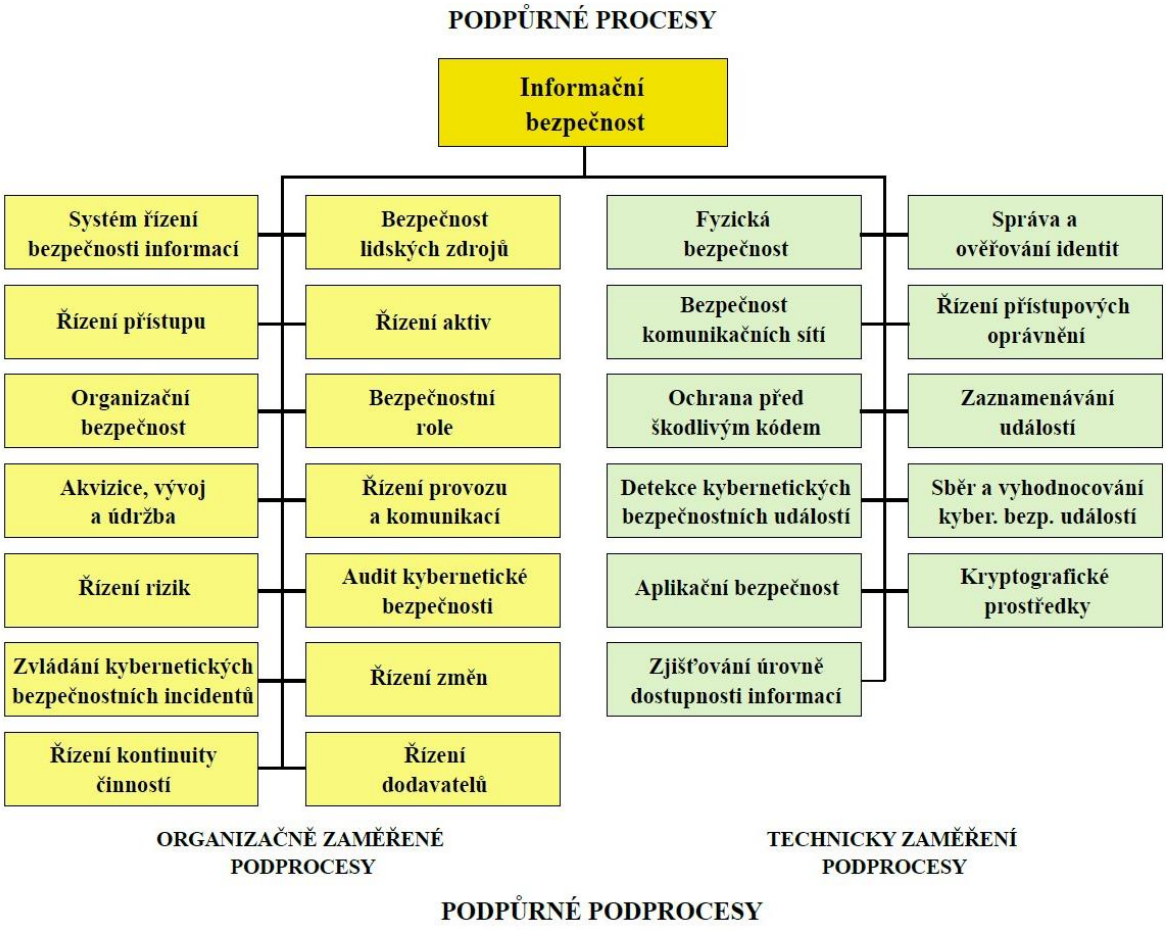
6.1 Procesní schéma podniku



Obrázek 10: Procesní schéma podniku [zdroj: vlastní tvorba]

Pro implementaci a udržování systému řízení bezpečnosti informací a řízení bezpečnostních opatření je v podniku podpůrný proces Informační bezpečnost rozdělen na podpůrné podprocesy. Tyto podpůrné podprocesy jsou strukturovány dle bezpečnostních opatření ve vyhlášce o kybernetické bezpečnosti č. 82/2018 Sb. Rozdělení je takto uzpůsobeno z důvodu přípravy podniku na možnou povinnost podřízení zákonu o kybernetické bezpečnosti, pokud by podnik uchovával utajované informace a figuroval by jako dodavatel v rámci kritické infrastruktury.

Podprocesy procesu Informační bezpečnost jsou v podniku strukturovány dle následujícího schématu.



Obrázek 11. Schéma podprocesů procesu Informační bezpečnost [zdroj: vlastní tvorba]

7 ROZSAH SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Na implementaci systému řízení bezpečnosti informací, dle normy ISO/IEC 27001, pracuje podnik, stejně jako u systému řízení kvality, od listopadu roku 2021, a také ještě není certifikován.

Do rozsahu systému řízení bezpečnosti informací jsou začleněny všechny činnosti dle rozsahu pro řízení kvality a dále jsou začleněna všechna aktiva podniku, která jsou využívána pro předmět podnikání podniku a zpracovávají, nebo jsou v nich zpracovávané, jakýmkoliv způsobem informace. Více informací o vytvořeném registru aktiv v podniku je v kapitole 7.1.

Z hlediska organizace jsou zahrnuty všechny organizační jednotky, které jsou uvedeny v organizačním schématu výše.

Garanty aktiv jsou v rámci ISMS zvoleni jednotliví vedoucí pracovníci těch oddělení, ke kterým se váže dané aktivum. Vzhledem k různorodosti činností, které podnik nabízí, bylo rozhodnuto o zvolení dvou Manažerů bezpečnosti informací. Jeden manažer řídí bezpečnost vývoje softwaru a druhý řídí ICT bezpečnost infrastruktury podniku. Tito manažeři jsou vybíráni z vedoucích pozic na základě jejich odborných znalostí.

7.1 Registr aktiv podniku

V rámci implementace systému řízení bezpečnosti informací byl v podniku vytvořen přehled všech aktiv podniku, která zpracovávají, nebo jsou v nich zpracovávané jakýmkoliv způsobem, informace.

U aktiv je v registru uveden název, stručný popis aktiva a jsou rozdělena do sedmi kategorií, kterými jsou služby, hardware, software, prostory, dodavatelé, zaměstnanci a informace/data. Dále je v registru uvedeno, který garant za aktivum odpovídá. Přehled registru aktiv v podniku je pro znázornění uveden v Příloze P1.

Mít přehled o používaných aktivech v podniku je důležité z důvodu, že aktiva, která jsou v registru uvedená, slouží jako prostředky používané při monitorování procesů a zároveň se jedná o podnikové zdroje. Tato aktiva budou klíčová pro definování metrik měření efektivity procesů.

Po identifikaci aktiv byla aktiva ohodnocena, zejména pro upřesnění, jak jsou jednotlivá aktiva pro podnik důležitá. Ohodnocení proběhlo podle základních kritérií bezpečnosti informací, kterými jsou důvěrnost, integrita a dostupnost.

Jako stupnice pro ohodnocení aktiva byly použity stupnice navrhované vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti. Tyto stupnice lze vidět níže. Na základě dopadu porušení bezpečnostního atributu je vybíráno mezi čtyřmi hodnotami „nízká“, „střední“, „vysoká“ a „kritická“. Každá z hodnot zastupuje hodnoty od 1 do 4. Aktiva byla ohodnocena individuálně pro každý bezpečnostní atribut [33].

Tabulka 2. Stupnice pro hodnocení důvěrnosti [42]

Úroveň		Popis
1	**Nízká**	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.
2	**Střední**	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.
3	**Vysoká**	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství, osobní údaje).
4	**Kritická**	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).

Tabulka 3. Stupnice pro hodnocení integrity [42]

Úroveň		Popis
1	**Nízká**	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy podniku.
2	**Střední**	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů podniku a může se projevit méně závažnými dopady na aktiva.
3	**Vysoká**	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů podniku s podstatnými dopady na aktiva.
4	**Kritická**	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů podniku s přímými a velmi vážnými dopady na aktiva.

Tabulka 4. Stupnice pro hodnocení dostupnosti [42]

Úroveň		Popis
1	**Nízká**	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
2	**Střední**	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů podniku.
3	**Vysoká**	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů podniku. Aktiva jsou považována jako velmi důležitá.
4	**Kritická**	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů podniku. Aktiva jsou považována jako kritická.

Přehled ohodnocení aktiv z pohledu důležitosti aktiv pro podnik v rámci bezpečnosti informací je uveden v Příloze P2.

7.2 Řízení rizik podniku

Pro identifikování rizik, která by mohla představovat vysoký dopad na bezpečnost informací, byla vytvořena v podniku analýza rizik. Tato analýza byla vytvořena v souladu s postupem navrhovaným vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti.

Do analýzy rizik byla zahrnuta všechna aktiva podniku. Vybraná aktiva byla následně sloučena do skupin, aby byla analýza rizik pro podnik jednodušší. Do jedné skupiny byla zahrnuta aktiva stejných vlastností nebo aktiva, na která následně vybrané hrozby a zranitelnosti mohou mít podobný dopad.

Po seskupení aktiv byly v podniku identifikovány hrozby, které mohou poškodit aktiva a byly identifikovány zranitelnosti, díky nimž mohou vybrané hrozby nastat. Při určování hrozeb a zranitelností bylo vycházeno ze seznamu hrozeb a zranitelností sestavených vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti. Použité hrozby byly následující:

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
2. poškození nebo selhání technického anebo programového vybavení,
3. zneužití identity,
4. užívání programového vybavení v rozporu s licenčními podmínkami,
5. škodlivý kód (například viry, spyware, trojské koně),

6. narušení fyzické bezpečnosti,
7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
8. zneužití nebo neoprávněná modifikace údajů,
9. ztráta, odcizení nebo poškození aktiva,
10. nedodržení smluvního závazku ze strany dodavatele,
11. pochybení ze strany zaměstnanců,
12. zneužití vnitřních prostředků, sabotáž,
13. dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
14. nedostatek zaměstnanců s potřebnou odbornou úrovní,
15. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
16. zneužití vyměnitelných technických nosičů dat,
17. napadení elektronické komunikace (odposlech, modifikace) [42].

Každá skupina aktiv byla porovnána s hrozbami, které jsou relevantní k dané skupině aktiv a byla ohodnocena pravděpodobnost, zda může hrozba pro daná aktiva nastat. Stupnicí pro ohodnocení pravděpodobnosti výskytu hrozby byla vybrána stupnice navrhovaná vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti.

Tabulka 5. Stupnice pro hodnocení pravděpodobnosti výskytu hrozby [42]

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

Jelikož jednu hrozbu může stanovit více zranitelností, byly u každé skupiny přiřazeny hrozbám relevantní zranitelnosti z předem vybraného seznamu. Tato skupina zranitelností byla následně ohodnocena podle dosavadních možností podniku jí zamezit ve vzniku [33]. Seznam uvažovaných zranitelností byl inspirován seznamem uvedeným vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti.

Vybrané zranitelnosti jsou následující:

1. nedostatečná údržba informačního a komunikačního systému,
2. zastaralost informačního a komunikačního systému,
3. nedostatečná ochrana vnějšího perimetru,
4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
5. nevhodné nastavení přístupových oprávnění,
6. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
7. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
8. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
9. nedostatečná ochrana aktiv,
10. nevhodná bezpečnostní architektura,
11. nedostatečná míra nezávislé kontroly,
12. neschopnost včasného odhalení pochybení ze strany zaměstnanců [42].

Stupnice pro ohodnocení zranitelností byla inspirována stupnicí pro ohodnocení snadnosti zneužití zranitelnosti navrhovanou vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti.

Tabulka 6. Stupnice pro hodnocení zranitelností [42]

Úroveň		Popis zranitelnosti
1	**Nízká**	Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
2	**Střední**	Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena.
3	**Vysoká**	Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	**Kritická**	Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Pro následné určení výsledného rizika byl použit vzorec navrhovaný vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti. V tomto vzorci jsou násobeny tři hodnoty. První hodnotou je nejvyšší ohodnocení jakéhokoliv bezpečnostního atributu aktiv v jedné skupině, tato hodnota se nazývá význam aktiva, nebo také význam skupiny aktiv. Druhou hodnotou je

ohodnocení pravděpodobnosti výskytu hrozby a třetí hodnotou je ohodnocení snadnosti zneužití zranitelnosti. Vzorec pro výpočet rizika vypadá následovně:

$$\mathbf{R = D \times H \times Z}$$

- R úroveň rizika,
- D nejvyšší ohodnocení bezpečnostního atributu aktiv ve skupině,
- H pravděpodobnost výskytu hrozby,
- Z snadnost zneužití zranitelností.

Tento postup výpočtu byl aplikován na všechny skupiny aktiv v analýze rizik a výsledek byl poté zapsán do jednotlivých analýz rizik.

Pro rizika byla vedením podniku stanovena hranice akceptovatelnosti určující, zda identifikované riziko může být akceptováno v jeho výši, nebo jestli je nutné zvolit adekvátní cestu pro snížení, či vyhnutí se riziku. Tato hranice byla vedením podniku stanovena na hodnotu 33. Z tohoto důvodu pro všechna rizika o hodnotě rovné, nebo vyšší než 33, musí být navrženo opatření pro snížení těchto rizik a vyšší bezpečnost informací.

V Příloze P3 jsou vyobrazeny analýzy rizik, ve kterých bylo vyhodnoceno neakceptovatelné riziko. Na těchto analýzách rizik lze vidět, která hrozba a zranitelnost k riziku vedla. Pro větší přehlednost jsou všechna neakceptovatelná rizika, napříč jednotlivými analýzami rizik, shromážděna do přehledu vyobrazeného níže.

Tabulka 7. Celkový přehled neakceptovatelných rizik v podniku [zdroj: vlastní tvorba]

ID rizika	Název analýzy	Hrozba	Zranitelnosti	Riziko
R 004	Analýza služeb ICT oddělení	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**36**
R 010	Analýza služeb ICT oddělení	Škodlivý kód (například viry, spyware, trojské koně)	Zastaralost informačního a komunikačního systému	**36**
R 012	Analýza služeb ICT oddělení	Škodlivý kód (například viry, spyware, trojské koně)	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**36**
R 015	Analýza služeb ICT oddělení	Ztráta, odcizení nebo poškození aktiva	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**36**
R 036	Analýza služeb ICT oddělení	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**36**

R 044	Analýza služeb ICT oddělení	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**36**
R 051	Analýza koncových zařízení (PC, notebooky)	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**48**
R 058	Analýza koncových zařízení (PC, notebooky)	Škodlivý kód (například viry, spyware, trojské koně)	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**48**
R 059	Analýza koncových zařízení (PC, notebooky)	Škodlivý kód (například viry, spyware, trojské koně)	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**48**
R 061	Analýza koncových zařízení (PC, notebooky)	Ztráta, odcizení nebo poškození aktiva	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**36**
R 068	Analýza koncových zařízení (PC, notebooky)	Pochybení ze strany zaměstnanců	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**36**
R 073	Analýza koncových zařízení (PC, notebooky)	Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**48**
R 077	Analýza koncových zařízení (PC, notebooky)	Zneužití vyměnitelných technických nosičů dat	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**36**
R 095	Analýza dodavatele kamerového systému	Zneužití nebo neoprávněná modifikace údajů	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**36**
R 098	Analýza dodavatele kamerového systému	Nedodržení smluvního závazku ze strany dodavatele	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**48**
R 105	Analýza dodavatele kamerového systému	Zneužití identity	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**36**

Pro rizika, jež jsou vyobrazena v tabulce výše, byla vedením podniku stanovena bezpečnostní opatření, která měla za cíl snížit výši rizika na akceptovatelnou úroveň, nebo se riziku zcela vyhnout. Bezpečnostních opatření bylo stanoveno 7, v tabulce níže je sestaven přehled uvedených opatření spolu s identifikátory rizik, které mají za cíl riziko snížit, nebo se mu vyhnout.

Tabulka 8. Přehled stanovených bezpečnostních opatření [zdroj: vlastní tvorba]

Název bezpečnostního opatření	Popis řízení rizika	Řízené riziko
Školení zaměstnanců e-learningovým nástrojem pro zvýšení bezpečnostního povědomí o sociálním inženýrství	Snížení rizika	R 004 R 051 R 061 R 068
Školení zaměstnanců vedoucím ICT ve spolupráci s externí společností pro zvýšení bezpečnostního povědomí o bezpečnostních opatřeních v podniku a jeho bezpečnostní dokumentaci	Snížení rizika	R 004 R 051 R 058 R 068 R 073 R 077
Nastavení pravidelného monitorování aktualizace virové databáze a antivirových nástrojů	Vyhnutí riziku	R 010 R 012 R 059
Centralizace výstupů z antivirových nástrojů za pomoci systému ESET PROTECT	Snížení rizika	R 010 R 012 R 059
Doplnění do smluvního ujednání s dodavateli povinnost hlášení bezpečnostních incidentů a povinnost přistupovat do interní sítě přes VPN	Vyhnutí riziku	R 095 R 098 R 105
Nastavení pravidelné kontroly správnosti provedení záloh	Snížení rizika	R 015
Vytvoření plánů kontinuity pro výpadek elektrického napájení a poškození produkčních serverů	Snížení rizika	R 010 R 015 R 036 R 044

III. PRAKTICKÁ ČÁST

8 STANOVENÍ METRIK PRO MĚŘENÍ EFEKTIVITY PROCESŮ

Z výsledků analýzy současného stavu podniku a teoretických poznatků vyplývá, že pro podnik existují rizika, která jsou pro vedení podniku neakceptovatelná a mohou mít značný dopad na bezpečnost informací. Jelikož tato rizika jsou vyhodnocena z pohledu bezpečnosti informací, jakékoliv z neakceptovatelných rizik je zapříčiněno neefektivním procesem. Přičemž cílem všech těchto procesů, zaměřených na bezpečnost informací je dosáhnout toho, aby právě tato rizika a zejména zranitelnosti spojené s tímto rizikem, nenastaly.

Podnik má stanovených 25 podpůrných podprocesů pro systém řízení bezpečnosti informací, zaměřených čistě na zabezpečení informací. Pro tuto práci jsem se rozhodl stanovit metriky pro měření efektivity procesů, které jsou zodpovědné za neakceptovatelná rizika, která byla při analýze rizik identifikována. Po konzultaci s vedením společnosti jsem se neakceptovatelná rizika rozhodl přiřadit k procesům ISMS následovně:

Tabulka 9. Přehled přiřazení neakceptovatelných rizik k procesům ISMS [zdroj: vlastní tvorba]

ID rizika	Název analýzy	Hrozba	Zranitelnosti	Proces
R 004	Analýza služeb ICT oddělení	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	**Bezpečnost lidských zdrojů**
R 051	Analýza koncových zařízení (PC, notebooky)	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	
R 058	Analýza koncových zařízení (PC, notebooky)	Škodlivý kód (například viry, spyware, trojské koně)	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	
R 061	Analýza koncových zařízení (PC, notebooky)	Ztráta, odcizení nebo poškození aktiva	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	
R 068	Analýza koncových zařízení (PC, notebooky)	Pochybení ze strany zaměstnanců	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	
R 073	Analýza koncových zařízení (PC, notebooky)	Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	
R 077	Analýza koncových zařízení (PC, notebooky)	Zneužití vyměnitelných technických nosičů dat	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	

R 010	Analýza služeb ICT oddělení	Škodlivý kód (například viry, spyware, trojské koně)	Zastaralost informačního a komunikačního systému	**Ochrana před škodlivým kódem**
R 012	Analýza služeb ICT oddělení	Škodlivý kód (například viry, spyware, trojské koně)	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	
R 059	Analýza koncových zařízení (PC, notebooky)	Škodlivý kód (například viry, spyware, trojské koně)	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	
R 015	Analýza služeb ICT oddělení	Ztráta, odcizení nebo poškození aktiva	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**Řízení kontinuity činností**
R 036	Analýza služeb ICT oddělení	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	
R 044	Analýza služeb ICT oddělení	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	
R 095	Analýza dodavatele kamerového systému	Zneužití nebo neoprávněná modifikace údajů	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	**Řízení dodavatelů**
R 098	Analýza dodavatele kamerového systému	Nedodržení smluvního závazku ze strany dodavatele	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	
R 105	Analýza dodavatele kamerového systému	Zneužití identity	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	

Z výše uvedené tabulky vyplývá, že rizika se vztahují ke čtyřem procesům, zaměřeným na bezpečnost informací, kterými jsou:

- **Bezpečnost lidských zdrojů;**
- **Ochrana před škodlivým kódem;**
- **Řízení kontinuity činností;**
- **Řízení dodavatelů.**

Následně je tato kapitola rozdělena na čtyři podkapitoly, z nichž každá je zaměřena na jeden z výše uvedených procesů. Součástí těchto podkapitol jsou mnou navržené metriky pro měření efektivity těchto procesů. Metriky jsou stanoveny tak, aby odrážely vývoj aspektů procesu, spojených s neakceptovatelnými riziky a zároveň efektivnost některých z bezpečnostních opatření, která byla podnikem pro řízení rizik stanovena. Efektivnost bezpečnostních opatření metriky vyhodnocují z důvodu, že měření bezpečnostních opatření, stanovených podnikem, je jeden z požadavků normy ISO/IEC 27001. Z tohoto důvodu jsou metriky stanoveny tak, aby vedení podniku poskytovaly přehled nejen o efektivitě procesu, ale i o efektivitě zavedeného bezpečnostního opatření.

Pro definování všech potřebných informací o metrice je použit upravený formulář z normy ISO/IEC 27004:2018 zobrazený v kapitole 2.5.2. U metriky je vždy uvedeno její označení v podniku, popis, její název, jakým způsobem by měla být metrika vypočtena nebo ohodnocena, jaké jsou cílové hodnoty nebo požadovaný výsledek metriky, jak často by data pro metriku měla být shromažďována a rovněž jak často by měla být vyhodnocována. Dále je u metrik uvedeno, kdo odpovídá za její měření, kdo za shromažďování dat, kdo je celkově odpovědný za metriku a z jakých dat nebo informací by se pro měření metriky mělo vycházet. V posledním bodu se uvádí zejména to, v jakém formátu jsou výsledky metriky předávány Představiteli pro integrovaný systém řízení, který by za pomoci těchto výsledků měl být schopný posoudit efektivnost měřeného procesu.

Pro pochopení průběhu procesu, jeho účelu a procesního uspořádání jsem vytvořil pro každý proces takzvanou „kartu procesu“, dle normy ISO 9001. Tato karta je uvedena vždy na začátku následujících podkapitol.

8.1 Měření efektivity procesu Bezpečnost lidských zdrojů

K tomuto procesu se váže, dle přehledu neakceptovatelných rizik, zranitelnost nedostatečného bezpečnostního povědomí uživatelů a administrátorů. Zejména se jedná o nedostatečné bezpečnostní povědomí o podnikové bezpečnostní dokumentaci a o tom, jak

mají zaměstnanci postupovat při ztrátě, nebo krádeži zařízení. Dále není dostatečné bezpečnostní povědomí o používání vyměnitelných nosičů dat a o hrozbách vyplývajících ze sociálního inženýrství. Jedním z částí procesu Bezpečnost lidských zdrojů je zejména školení zaměstnanců a zvyšování jejich povědomí o bezpečnosti informací. Ve spojitosti s tímto procesem jsou navrženy metriky pro měření efektivity procesu, zejména činností souvisejících se školením zaměstnanců.

V rámci řízení rizika bylo vedením podniku rozhodnuto o zavedení dvou bezpečnostních opatření, která se vztahují k tomuto procesu. Těmito opatřeními bylo provedení e-learningového školení, jehož tématem bylo sociální inženýrství. Dále bylo naplánováno a provedeno, ve spolupráci s externí společností, školení o bezpečnostních opatřeních v podniku a jeho bezpečnostní dokumentaci.

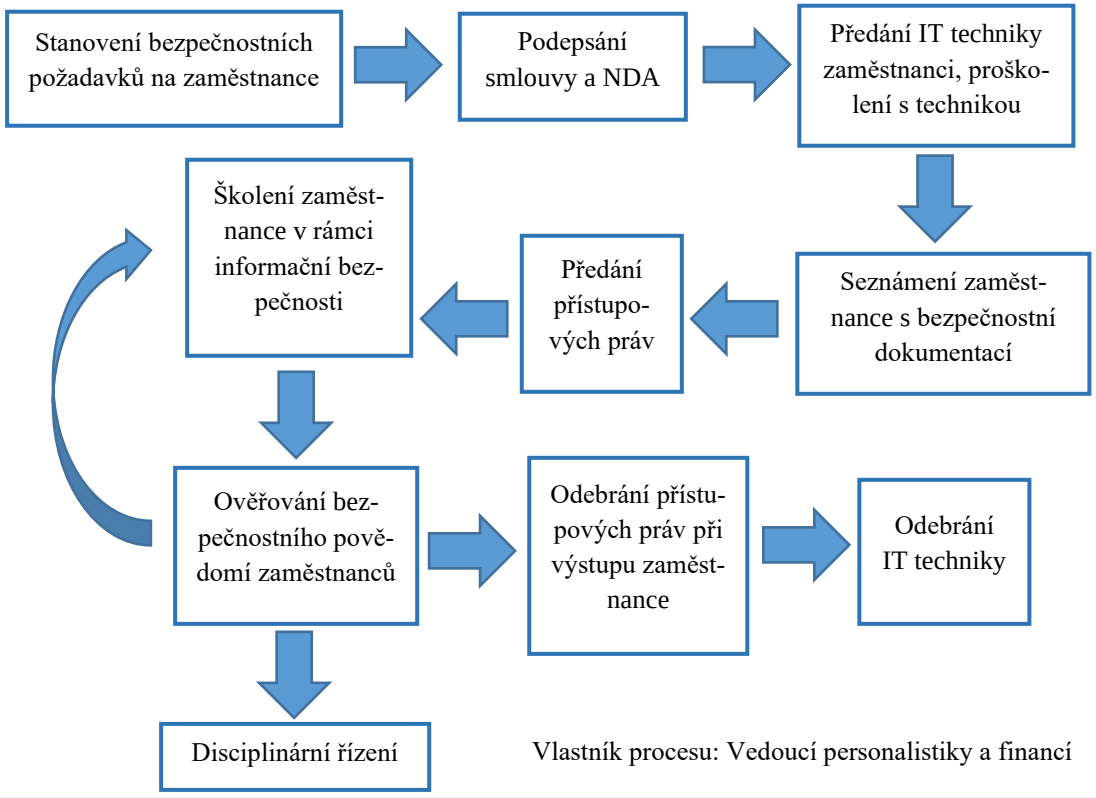
8.1.1 Karta procesu Bezpečnost lidských zdrojů

Účel procesu:
Účelem procesu je zajistit, aby přijímaní zaměstnanci podniku splnili všechny požadavky informační bezpečnosti dle své pozice a byli dostatečně proškoleni bezpečnostními pravidly v podniku a byli proškoleni o rizicích, která mohou v rámci informační bezpečnosti nastat.

Vstupy procesu:
- Požadavek managementu na obsazení pozice v podniku
- Požadavky na zaměstnance stanovené podnikem

Dodavatelé v procesu:
- Podniky zabývající se náborem zaměstnanců
- Podniky provádějící školení, zaměřené na bezpečnost informací

Činnosti procesu:



Vlastník procesu: Vedoucí personalistiky a financí

Výstupy procesu:
- Povědomí zaměstnanců o bezpečnosti informací a bezpečnostních opatřeních v podniku
- Výsledky kontroly ověřování bezpečnostního povědomí zaměstnanců
- Výstup zaměstnance bez dalšího přístupu k jakýmkoliv datům a informacím podniku

Jak:	S kým:	S čím:
– směrnice pro řízení lidských zdrojů – směrnice pro řízení bezpečnosti informací – norma ISO/IEC 27001 – norma ISO 9001	– představenstvo – vedoucí pracovníci – personalistka	– pracovní stanice – telefony, tablety – IS Target – Active directory – VPN

8.1.2 Proškolení zaměstnanců v rámci bezpečnosti informací

Kromě školení, zabývajícím se bezpečností informací, které bylo provedeno ve spolupráci s externí společností v rámci opatření pro řízení rizik, jsou ve společnosti prováděna jednou za dva roky pravidelná školení o bezpečnosti informací. Tato školení provádí vedoucí ICT a jsou do něho zahrnuti všichni zaměstnanci, kteří nebyli dosud proškoleni, nebo jim uplynuly 2 roky od posledního školení.

Tuto metriku navrhuji pro pravidelné vyhodnocování bezpečnostního povědomí zaměstnanců, aby mělo vedení společnosti o této skutečnosti přehled. Na základě výsledků metriky navrhuji, pokud bude zjištěna nízká výše bezpečnostního povědomí, provádět dodatečná školení o bezpečnosti informací, jelikož se tak v podniku neděje a tento stav se odráží na analýze rizik.

ID metriky: 001

Informační potřeba: Tato metrika poskytne podniku procentuálně vyjádřený přehled o tom, kolik zaměstnanců prošlo v posledních dvou letech školením o bezpečnosti informací. Na základě výsledků metriky bude moci vedení společnosti posoudit, zda je nutné zorganizovat nové školení pro bezpečnost informací a jaký počet zaměstnanců by se měl tohoto školení zúčastnit.

Název metriky: Proškolení zaměstnanců v rámci bezpečnosti informací

Vzorec/bodování: K1 – [Počet zaměstnanců, kteří absolvovali školení pro zvýšení povědomí o bezpečnosti informací nejpozději před 24 měsíci / Celkový počet zaměstnanců v podniku k datu měření] × 100. Výsledek je zaokrouhlen na jednotky, tedy bez uvádění desetinného místa.

Cíl: K1 > 95 % – není potřeba žádná akce, zaměstnanci jsou dostatečně proškoleni

96 % > K1 > 80 % – věnovat této skutečnosti zvýšenou pozornost, aby nedošlo ke zhoršení stavu. Nejpozději do 6 měsíců by mělo být naplánováno školení o bezpečnosti informací.
K1 < 81 % – mělo by být provedeno přezkoumání pro zjištění příčiny neshody a nízké efektivnosti. Školení informační bezpečnosti by mělo proběhnout v nejbližší možné době.

Důkaz implementace: Prezenční listiny z proběhlých školení pro zvýšení povědomí o bezpečnosti informací, obsahující program školení a podpis zúčastněné osoby. Přehled záznamů o školení zaměstnanců v systému IS Target, kde mají zaměstnanci v poli „školení ISMS“ zobrazenou hodnotu „Proškolen“.

Četnost: Shromažďování dat: Měsíčně, vždy na konci měsíce
Analýza: Čtvrtletně
Období měření: Dvouleté

Odpovědné strany: Osoba odpovědná za metriku: Vedoucí personalistiky a financí
Osoba shromažďující informace: Personalistka
Osoba odpovědná za analýzu výsledků: Vedoucí personalistiky a financí

Zdroj dat: Záznamy v systému IS Target, záznamy o školení, osobní složky zaměstnanců

Formát podávání zpráv: Regulační diagram vyjadřující sloupci, kolik zaměstnanců je proškolených o bezpečnosti informací. Výsledky jsou uvedeny v procentech. Součástí grafu by měl být přehled, co uvedené hodnoty vyjadřují a jaké jsou předpokládané akce vedení podniku.

8.1.3 Porozumění zaměstnanců e-learningovému školení

Pro snížení rizika, souvisejícího s nedostatkem povědomí zaměstnanců o sociálním inženýrství, bylo provedeno v podniku e-learningové školení, zaměřující se přímo na hrozby související se sociálním inženýrstvím. Zaměstnancům byl předložen on-line formou vědomostní test hodnotící jejich povědomí o této problematice před školením a po dokončení

školení, aby mohly být srovnány výsledky testů. Externí společností jsou po ukončení školení zaslány výsledky testů personalistce podniku a předsedovi představenstva.

Tuto metriku navrhuji pro měření efektivnosti daného školení. Metrika může být později podnikem použita i na jiná školení, ať už budou jednorázová nebo pravidelná. Metrika může být vyhodnocována na základě procentuální úspěšnosti, nebo mohou být bodově ohodnoceny jednotlivé části školení. Hodnocení bude vždy záviset na podniku.

ID metriky: 002

Informační potřeba: Tato metrika měří efektivitu proběhlého e-learningového kurzu o sociálním inženýrství u zaměstnanců podniku. Výsledky metriky jsou získány posouzením bezpečnostního povědomí o sociálním inženýrství a jeho hrozbách před provedením školení a následně po něm.

Název metriky: Porozumění zaměstnanců e-learningovému školení

Vzorec/bodování: K1 – [Počet zaměstnanců, kteří získali více, jak 80 % v testu po ukončení školení a zároveň získali 80 % nebo méně v testu před školením / Počet zaměstnanců, kteří získali více, jak 80 % v testu při hodnocení před školením] × 100. Výsledek je zaokrouhlen na jednotky, tedy bez uvádění desetinného místa.

Cíl: K1 > 50 % – není potřeba žádná akce, školení je považováno za efektivní
K1 < 51 % – školení je považováno za neefektivní a měly by být řešeny důvody neefektivnosti školení nebo nahrazení školení jiným školením

Důkaz implementace: Výsledky znalostních testů dodané dodavatelem e-learningového školení. Seznam zaměstnanců, kteří se zúčastnili e-learningového školení.

Četnost: Shromažďování dat: Do jednoho měsíce od provedení e-learningového školení zaměstnanců
Analýza: Při shromažďování dat
Období měření: Jednorázově

Odpovědné strany: Osoba odpovědná za metriku: Vedoucí personalistiky a financí
Osoba shromažďující informace: Personalistka
Osoba odpovědná za analýzu výsledků: Vedoucí personalistiky a financí

Zdroj dat: Výsledky znalostních testů dodané dodavatelem e-learningového školení. Databáze zaměstnanců podniku v IS Target.

Formát podávání zpráv: Sloupcový graf pro vyjádření vývoje bezpečnostního povědomí o sociálním inženýrství. Může být doplněn sloupcovým grafem, který bude vyjadřovat procentuální zastoupení úspěšnosti v testu před školením a po školení.

8.2 Měření efektivity procesu Ochrana před škodlivým kódem

Na základě analýzy rizik byla odhalena pro tento proces zranitelnost týkající se zastaralosti informačního sytému. V rámci analýzy byla brána jako systém virová databáze a bylo zjištěno, že se tato databáze neudržuje aktuální.

Dále byly odhaleny zranitelnosti, značící nedostatek stanovených bezpečnostních pravidel, souvisejících s pravidly pro zamezení průniku škodlivého kódu do interní sítě podniku. Jednalo se zejména o nestanovená pravidla pro kontrolu výstupů antivirových zařízení.

Pro snížení výše zmíněného rizika byly všechny výstupy z antivirových programů centralizovány za pomoci programu ESET PROTECT. Tato centralizace měla pomoci přehledu stavu aktualizací systémů a antivirového systému na koncových zařízeních a lepších výstupů o stavu sítě, při analýze centralizovaných dat. Dále bylo naplánováno bezpečnostní opatření, jehož cílem bylo zavedení pravidelného monitorování aktuálnosti virové databáze.

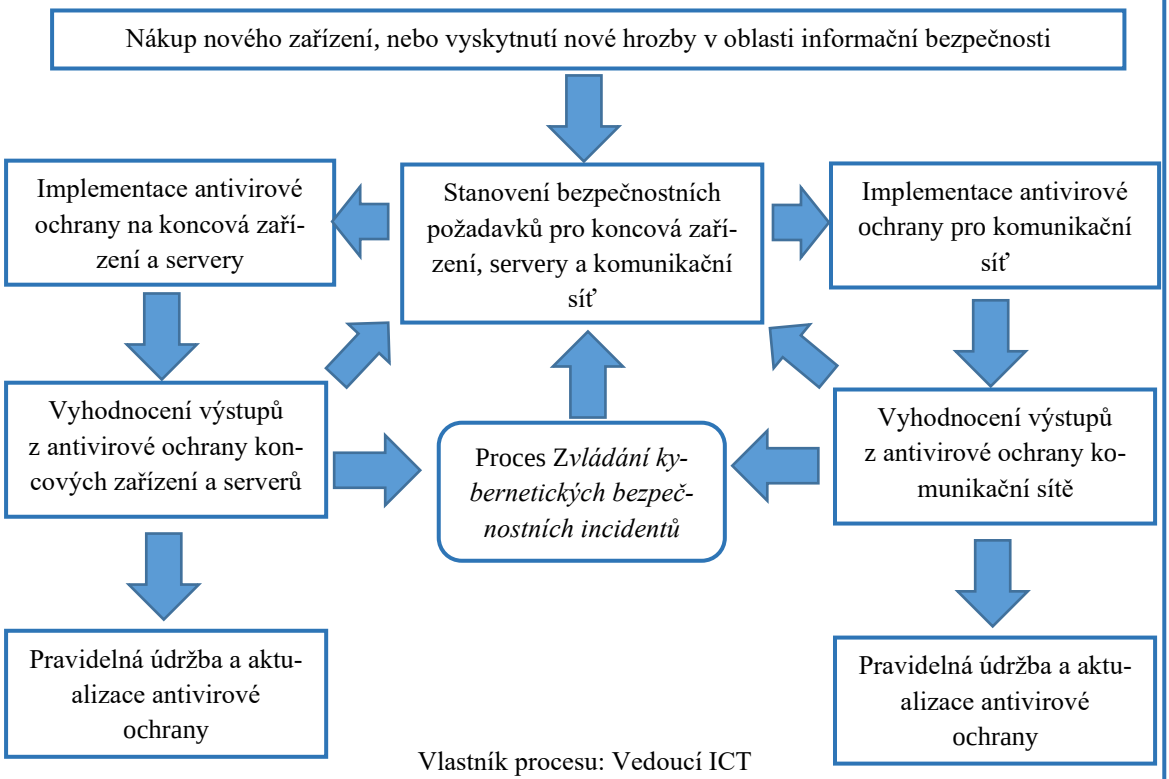
8.2.1 Karta procesu Ochrana před škodlivým kódem

Účel procesu:
Účelem procesu je zajistit antivirovou ochranu všem koncovým zařízením, serverům a komunikační síti. Dále sbírat informace z výstupů těchto antivirových nástrojů a na základě těchto výstupů zvýšit zabezpečení antivirové ochrany v podniku.

Vstupy procesu:
- Nákup nového zařízení, na které bude nutné aplikovat antivirovou ochranu
- Získání informace o nové hrozbě, novém škodlivém kódu, který může mít negativní dopad na podnik

Dodavatelé v procesu:
- Dodavatelé antivirových nástrojů

Činnosti procesu:



Vlastník procesu: Vedoucí ICT

Výstupy procesu:
- Zavedená účinná ochrana před viry a jinými škodlivými kódy na koncových zařízeních, serverové infrastruktuře a v komunikační síti podniku

Jak:	S kým:	S čím:
– materiály od zdrojů zabývající se problematikou (NÚKIB, antivirové společnosti, atd.) – směrnice pro řízení bezpečnosti informací – norma ISO/IEC 27001	– představenstvo – představitel integrovaného systému řízení – vedoucí ICT – IT administrátor specialista – IT administrátor	– pracovní stanice – síťové služby s vyšší prioritou – síťové služby s nižší prioritou, Optické převodníky, Wi-Fi – produkční servery – ESET PROTECT

8.2.2 Aktuálnost virové databáze

Pro splnění bezpečnostního opatření, požadujícího zavedení pravidelného monitorování aktuálnosti virové databáze, byla mnou navržena tato metrika. Níže popsaná metrika bude sloužit ICT oddělení pro udržování přehledu o aktuálnosti virové databáze a učinění potřebných kroků, pokud by metrikou byla databáze vyhodnocena jako neaktuální.

ID metriky: 003

Informační potřeba: Ověření, zda je virová databáze aktuální, nebo v případě, že není antivirová ochrana spravována centrálně, ověřuje se každé zařízení připojující se do interní sítě s nainstalovanou ochranou, zda je jeho virová databáze aktuální. Provádí se pouze u zařízení s nainstalovaným antivirovým nástrojem, která byla spuštěna a připojena k internetu ve sledovaném období.

Název metriky: Aktuálnost virové databáze

Vzorec/bodování: Počet dní, kdy je databáze neaktualizovaná. Při centralizované antivirové ochraně je brán počet dní přehledu centrální správy, jinak je brán počet dní u zařízení s nejvíce neaktuální databází.

Cíl: 0 – 7 dní – není požadována žádná akce

8 – 29 dní – věnovat zvýšenou pozornost, aby nedošlo ke zhoršení stavu.

30 dní a více – kontaktování vedoucího ICT, přezkoumání příčiny neaktuálnosti virové databáze a řešení vzniklé neshody

– Pokud je virová databáze aktualizována automaticky a aktualizace neproběhla, je možnost přítomnosti malwaru, který blokuje aktualizaci. V takovém případě je nutné ihned kontaktovat vedoucího ICT a provést přezkoumání problému.

Důkaz implementace: Záznamy o antivirové ochraně a aktuálnosti virové databáze v programu ESET PROTECT. Záznamy o aktuálnosti virové databáze v antivirových nástrojích na jednotlivých zařízeních.

Četnost: Shromažďování dat: Týdně
Analýza: Čtvrtletně
Období měření: Roční

Odpovědné strany: Osoba odpovědná za metriku: Vedoucí ICT
Osoba shromažďující informace: IT administrátor
Osoba odpovědná za analýzu výsledků: IT administrátor specialista

Zdroj dat: Záznamy v antivirových nástrojích

Formát podávání zpráv: Regulační diagram vyjadřující sloupci, kolik dní je neaktuální virová databáze v podniku.

8.2.3 Útoky škodlivým kódem s dopadem

Pro měření efektivity tohoto procesu navrhuji metriku, která bude měřit základní ukazatel jeho efektivity, jímž je poměr nezablokovaných průniků do interní sítě podniku, zapříčiněných útoky škodlivým kódem.

Základními nástroji v podniku pro zablokování těchto útoků jsou antivirový nástroj ESET PROTECT, firewall podniku a poštovní server. Ke snížení počtu útoků, které nebyly zablokovány, by mělo vést bezpečnostní opatření stanovené vedením. Tímto opatřením je centralizace výstupů z antivirových nástrojů.

Jako zdroje informací pro tuto metriku navrhuji logy z výše uvedených nástrojů a záznamy v systému OTRS, kam zaměstnanci zaznamenávají všechny události a incidenty v podniku, spojené s bezpečností informací.

ID metriky: 004

Informační potřeba: Tato metrika posuzuje efektivnost ochrany před škodlivým kódem v interní infrastruktuře podniku měřením detekovaných, nezablokovaných průniků do komunikační sítě a na koncová zařízení.

Název metriky: Útoky škodlivým kódem s dopadem

Vzorec/bodování:	**[**Počet zaznamenaných bezpečnostních incidentů způsobených škodlivým kódem v komunikační síti nebo koncových zařízení / Počet detekovaných a zablokovaných pokusů útoků způsobených škodlivým kódem] × 100. Výsledek je zaokrouhlen na jednotky, tedy bez uvádění desetinného místa.
Cíl:	Trend počtu nezablokovaných útoků, způsobených škodlivým kódem by měl být klesající nebo konstantní od posledního měření metrikou.
Důkaz implementace:	Záznamy o bezpečnostních incidentech ze systému OTRS. Logy z nástrojů obsahují protiopatření pro útoky škodlivým kódem (firewall, ESET PROTECT).
Četnost:	Shromažďování dat: Týdně Analýza: Čtvrtletně Období měření: Roční
Odpovědné strany:	Osoba odpovědná za metriku: Vedoucí ICT Osoba shromažďující informace: IT administrátor Osoba odpovědná za analýzu výsledků: IT administrátor specialista
Zdroj dat:	Záznamy „tiketovacích“ systémů. Logy z nástrojů obsahují protiopatření pro útoky škodlivým kódem
Formát podávání zpráv:	Směr trendu vyjádřený sloupcovým diagramem, znázorňující poměr mezi nezablokovanými a zablokovanými útoky v průběhu hlášeného období.

8.3 Měření efektivity procesu Řízení dodavatelů ISMS

Z identifikovaných rizik a z hodnocení v úvodu kapitoly 8 lze vidět, že nejvyšší rizika jsou způsobena v tomto procesu nedostatečně stanovenými bezpečnostními požadavky ve smlouvách s dodavateli. Ve smlouvách není na základě analýzy zejména dostatečně stanoven dopad nedodržení smluvních požadavků, spojených s bezpečností informací, dále není dostatečně určeno, jak mají dodavatelé nakládat s přihlašovacími údaji, pokud přistupují do sítě podniku a jak mají nakládat s informacemi, které jim jsou v rámci dodavatelského vztahu předány.

V rámci bezpečnosti informací jsou v podniku s dodavateli podepisovány dohody o mlčenlivosti a pokud jim jsou předávány osobní údaje nebo mají přístup k osobním údajům, je s dodavatelem uzavírána zpracovatelská smlouva podle zákona č. 110/2019 Sb., o zpracování osobních údajů. Pro splnění požadavků normy ISO/IEC 27001 jsou obchodníkem a vedoucím ICT vždy pro každý dodavatelský vztah, který ovlivňuje bezpečnost informací, vyhodnocena rizika s tímto dodavatelem a na základě těchto rizik stanoveny bezpečnostní požadavky, které jsou přidány do smlouvy s dodavatelem. Některé z bezpečnostních požadavků si podnik stanovil jako povinné, přidávají se do smlouvy vždy a jsou ve smlouvě označeny jako navrhované požadavky. Tyto požadavky jsou více rozvedeny v kapitole 8.3.2.

Pro měření efektivity procesu Řízení dodavatelů ISMS navrhuji metriky pro kontrolu začlenění výše zmíněných požadavků ve smlouvách s dodavateli a metriku pro měření výskytu incidentů spojených s bezpečností informací, které nastaly u dodavatelů.

8.3.1 Karta procesu Řízení dodavatelů ISMS

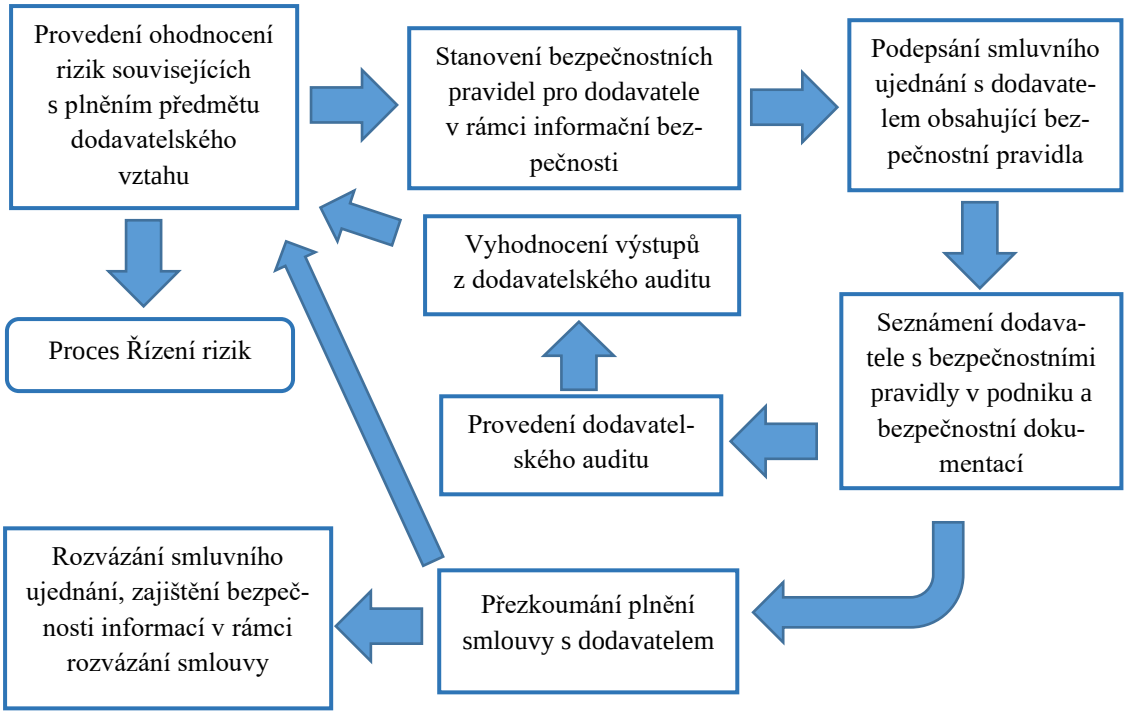
Účel procesu:
Účelem procesu je zajistit ve smluvním ujednání s dodavatelem bezpečnostní požadavky pro bezpečnost informací a pravidelně přezkoumávat u dodavatele plnění těchto bezpečnostních požadavků.

Vstupy procesu:
- Požadavek pro nový dodavatelský vztah (plánovaní vypsání výběrového řízení pro dodavatele)

Dodavatelé v procesu:
- Podniky provádějící dodavatelské audity v rámci informační bezpečnosti

Činnosti procesu:

Vlastník procesu: Manažer informační bezpečnosti ICT



Výstupy procesu:
- Stanovené bezpečnostní opatření ve smluvním ujednání s dodavatelem a efektivní zabezpečení informací v rámci dodavatelského vztahu
- Zabezpečení informací při rozvázání dodavatelského vztahu

Jak:
- směrnice pro řízení dodavatelů
- směrnice pro řízení bezpečnosti informací
- norma ISO/IEC 27001
- norma ISO/IEC 9001

S kým:
- představenstvo
- představitel integrovaného systému řízení
- vedoucí ICT
- obchodník
- manažer projektů

S čím:
- pracovní stanice
- OTRS ICT
- Byznys

8.3.2 Počet incidentů u dodavatelů

Jak už bylo zmíněno výše v úvodu kapitoly 8.3, tuto metriku navrhuji pro pravidelné monitorování vzniklých bezpečnostních incidentů u dodavatelů podniku. Výstupy z metriky by měly pomoci vedení společnosti pro změnu rizikových dodavatelů, nebo jako podnět pro zvýšení bezpečnostních požadavků do smlouvy s dodavatelem.

Pro tuto metriku mohou být vybráni pouze dodavatelé, se kterými je dohodnuto ve smluvních podmínkách, že dodavatel podniku hlásí bezpečnostní incidenty, které u něho vznikly.

ID metriky: 005

Informační potřeba: Tato metrika posuzuje efektivitu dodavatelských vztahů v rámci bezpečnosti informací. Efektivitu dodavatelského vztahu v této metrice určují bezpečnostní incidenty, které proběhly na straně dodavatele.

Název metriky: Počet incidentů u dodavatelů

Vzorec/bodování: 1 bod – U dodavatele za měřené období nenastal bezpečnostní incident ovlivňující bezpečnost informací.
2 body – U dodavatele za měřené období nastal bezpečnostní incident, neovlivňuje však smluvní vztah mezi podnikem a dodavatelem.
3 body – U dodavatele za měřené období nastal bezpečnostní incident, který ovlivňuje smluvní vztah mezi podnikem a dodavatelem. Pro podnik nevznikl žádný finanční nebo právní dopad.
4 body – U dodavatele za měřené období nastal bezpečnostní incident, který ovlivňuje smluvní vztah mezi podnikem a dodavatelem. Pro podnik vznikl v souvislosti s incidentem finanční nebo právní dopad.

Cíl: Dodavatel není hodnocen 3 ani 4 body v rámci měřeného období – Dodavatel je způsobilý a nejsou podniknuty žádné kroky.
Dodavatel není hodnocen 4 body, maximálně jedenkrát je hodnocen 3 body v měřeném období – Situace je monitorována, zda nedochází ke

zhoršení. Může být uvažováno o změně dodavatele, nebo změně smluvních podmínek s dodavatelem.
Výskyt hodnocení 4 body nebo dvě či více hodnocení 3 body - Musí být provedena změna dodavatele, nebo dodavatel musí přijmout bezpečnostní opatření pro zvýšení bezpečnosti informací.

Důkaz implementace: Databáze dodavatelů v systému Byznys. Záznamy o dodavatelích.

Četnost: Shromažďování dat: Čtvrtletně
Analýza: Ročně
Období měření: Roční

Odpovědné strany: Osoba odpovědná za metriku: Obchodník
Osoba shromažďující informace: IT administrátor specialista
Osoba odpovědná za analýzu výsledků: Obchodník

Zdroj dat: Databáze dodavatelů v systému Byznys. Záznamy o dodavatelích.

Formát podávání zpráv: Tabulka obsahující seznam dodavatelů. Ve sloupcích k dodavatelům přiřazené vyhodnocení počtu bezpečnostních incidentů. Může být přiloženo možné vyjádření IT administrátora k proběhlým bezpečnostním incidentům.

8.3.3 Sjednání požadavků na bezpečnost informací ve smlouvách s dodavateli

Kromě dalších bezpečnostních požadavků pro smlouvu s dodavatelem, které jsou určeny na základě vyhodnocení rizik spojených s dodavatelským vztahem, jsou v podniku stanoveny bezpečnostní požadavky, jež má podnik za cíl do nových smluv přidat vždy. Těmito požadavky jsou podepsání mlčenlivosti, povinnost hlášení bezpečnostních incidentů dodavateli, ustanovení o dodržování bezpečnostní dokumentace podniku, podmínky pro předávání dat a likvidace dat předaných v rámci dodavatelského vztahu.

Pro vyhodnocování, v jaké míře jsou řešeny vybrané bezpečnostní požadavky ve smlouvách s dodavateli, navrhuji následující metriku.

ID metriky: 006

Informační potřeba: Vyhodnocení stupně, v jakém je bezpečnost informací řešena ve smlouvách s dodavateli.

Název metriky:	Sjednání požadavků na bezpečnost informací ve smlouvách s dodavateli
Vzorec/bodování:	Kritérium 1: [Součet (pro každého dodavatele, ovlivňující bezpečnost informací) [Součet řešených bezpečnostních požadavků ve smlouvě s dodavatelem / Součet bezpečnostních požadavků navrhovaných, že by měly být řešeny ve smlouvách s dodavateli] / počet dodavatelů] × 100 Kritérium 2: Porovnání s předcházejícím výsledkem Kritéria 1
Cíl:	Kritérium 1: 60 % a vyšší – Řešení bezpečnostních požadavků s dodavateli je dostatečné. < 60 % – Musí být provedeno přezkoumání pro zjištění důvodu neřešených bezpečnostních požadavků. Musí být doplněny bezpečnostní požadavky do smluvních ujednání s dodavateli, aby se zvýšilo Kritérium 1 na akceptovatelnou úroveň. Kritérium 2: Trend vytvořený z porovnání výsledků z přechozích období měření by měl být stabilní nebo by měl narůstat.
Důkaz implementace:	Seznam navrhovaných bezpečnostních požadavků pro smlouvy s dodavateli. Smlouvy s dodavateli. Záznamy v systému Byznys.
Četnost:	Shromažďování dat: Ročně Analýza: Ročně Období měření: Roční
Odpovědné strany:	Osoba odpovědná za metriku: Obchodník Osoba shromažďující informace: Manažeři projektů Osoba odpovědná za analýzu výsledků: Obchodník
Zdroj dat:	Databáze dodavatelů v systému Byznys. Smlouvy s dodavateli.
Formát podávání zpráv:	Histogram znázorňující výsledek poměru bezpečnostních požadavků ve smlouvách porovnaný s předchozími výsledky měření.

8.4 Měření efektivity procesů Řízení kontinuity činností

K procesu Řízení kontinuity činností se váže zranitelnost nedostatečného stanovení bezpečnostních pravidel a nepřesné nebo nejednoznačné vymezení práv spolu se zranitelností nedostatečného bezpečnostního povědomí zaměstnanců.

Z analýzy rizik a konzultace s vedením podniku vyplynulo, že nejsou stanovena pravidla ani postupy pro případ, že by v podniku nastala porucha serveru a nebyl přítomný vedoucí ICT. V takovém případě nemá nikdo jiný potřebné znalosti pro vyřešení této situace, z toho důvodu je nutné nastavit postupy použitelné při výpadku serveru, aby i jiný IT zaměstnanec mohl vedoucího ICT při řešení tohoto problému zastoupit. Pro tento účel bylo v podniku naplánováno bezpečnostní opatření, jehož cílem bylo vytvoření plánu kontinuity pro případy poškození klíčových, tedy produkčních serverů. Dále i pro případy, pokud by nastala porucha serveru a nebyla dostupná potřebná data ze záloh, jelikož bylo zjištěno, že zálohy neprobíhají v pořádku a zaměstnanci tuto skutečnost opomíjeli kontrolovat.

Stejné riziko, týkající se problému s nedostatečnými znalostmi, bylo dle analýzy rizik vyhodnoceno i pro situace, kdy nastane výpadek elektrického napájení v podniku. I v tomto případě nemá žádný ze zaměstnanců, vyjma vedoucího ICT, potřebné znalosti pro vyřešení tohoto problému, a proto bylo rozhodnuto o vytvoření plánu kontinuity.

Tyto dva výše zmíněné plány kontinuity snižují zároveň i poslední identifikované neakceptovatelné riziko, spojené s nedostatkem odborných zaměstnanců. Vedením podniku bylo rozhodnuto, že nebudou přijímáni noví zaměstnanci, ale budou vypracovány zmíněné plány kontinuity, které budou poskytovat dostatečně srozumitelně formulované postupy i pro zaměstnance bez odborných znalostí.

Pro měření efektivity procesu Řízení kontinuity činností navrhuji metriky uvedené v kapitolách 8.4.1 a 8.4.2, které budou měřit správnost provedení záloh a stav implementování potřebných plánů kontinuity.

8.4.1 Karta procesu Řízení kontinuity činností

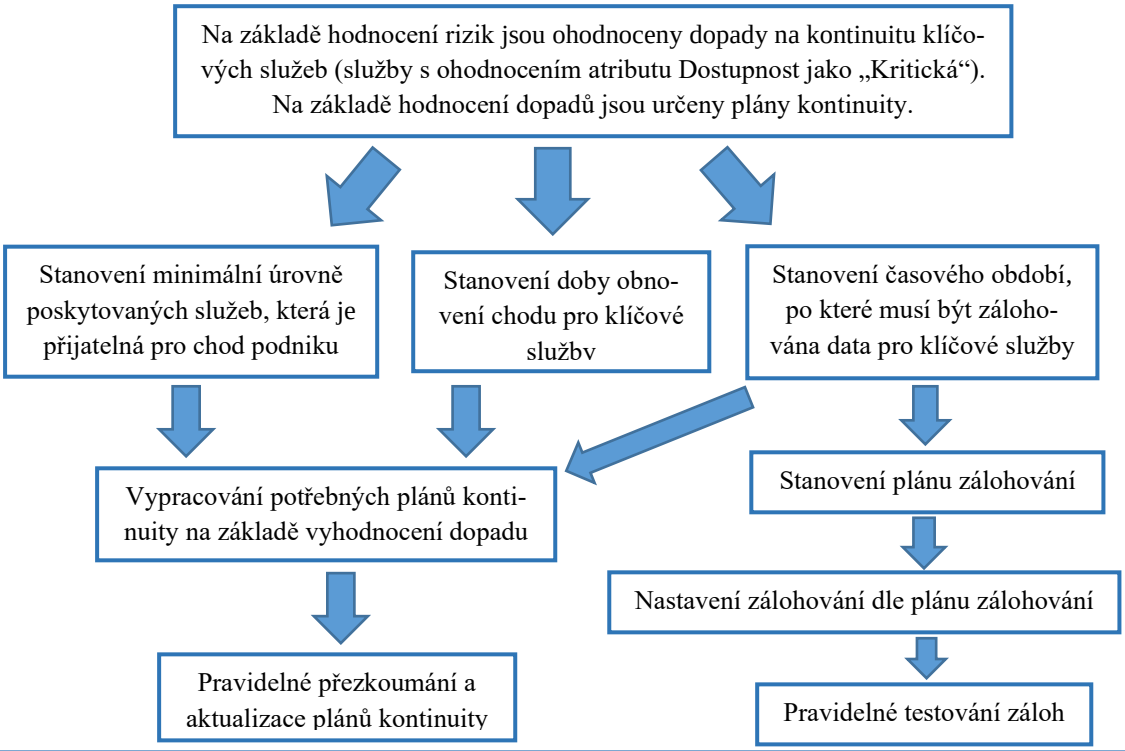
Účel procesu:
Účelem procesu je stanovení plánů kontinuity pro zajištění kontinuity klíčových činností v podniku v případech bezpečnostních incidentů. Dále je účelem procesu stanovit a nastavit adekvátní proces zálohování dat pro potřeby podniku.

Vstupy procesu:
- Výstup z procesu Řízení rizik
- Výstup z procesu Zvládání kybernetických bezpečnostních incidentů

Dodavatelé v procesu:
- Servis výpočetních zařízení

Činnosti procesu:

Vlastník procesu: Vedoucí ICT



Výstupy procesu:
- Vytvořené efektivní plány kontinuity pro udržení kontinuity klíčových činností při vzniku bezpečnostního incidentu
- Nastavené zálohování dat pro účely udržení kontinuity

Jak:
- metodika řízení rizik
- směrnice pro řízení bezpečnosti informací
- norma ISO/IEC 27001

S kým:
- představitel integrovaného systému řízení
- vedoucí ICT
- IT administrátor specialista

S čím:
- pracovní stanice
- úložiště záloh
- data na file serveru
- datastore
- záložní a testovací servery
- zálohy na NAS zařízeních

8.4.2 Správnost provádění záloh dat

V podniku probíhá pravidelné zálohování dat celého primárního úložiště na záložní úložiště jedenkrát měsíčně, dle stanoveného plánu zálohování. Na základě analýzy rizik bylo rozhodnuto o zasílání e-mailových zpráv o správném provedení záloh zálohovacím serverem oddělení ICT. Tato metrika by měla sloužit pro pravidelný přehled, kolik za poslední měřené období nastalo nepovedených záloh a je zde možnost porovnání výsledků s těmi z minulého období tak, aby odpovědní zaměstnanci získali přehled o vývoji situace.

ID metriky: 007

Informační potřeba: Touto metrikou je měřena správnost provedení záloh dle plánu zálohování pro předcházení dlouhodobé ztrátě dat.

Název metriky: Správnost provádění záloh dat

Vzorec/bodování: Počet hlášení o chybně provedených zálohách dat, nebo o nedokončení zálohy dat, které jsou stanoveny dle plánu zálohování.

Cíl: 0x – zálohování je prováděno správně a není nutná žádná další akce
1x – bližší sledování situace, zda nedochází ke zhoršení
2x a více – kontaktování vedoucího ICT a přezkoumání příčiny chybně provedených záloh

Důkaz implementace: Hlášení o chybně provedených zálohách z logů. Hlášení stavu provedení záloh e-mailem ze zálohovacího serveru.

Četnost: Shromažďování dat: Týdně
Analýza: Měsíčně
Období měření: Roční

Odpovědné strany: Osoba odpovědná za metriku: Vedoucí ICT
Osoba shromažďující informace: IT administrátor
Osoba odpovědná za analýzu výsledků: IT administrátor specialista

Zdroj dat: Hlášení o chybně provedených záloh z logů. Hlášení stavu provedení záloh e-mailem ze zálohovacího serveru.

Formát podávání zpráv: Histogram znázorňující počty hlášených chybně provedených záloh v měřeném období.

8.4.3 Stav vytvořených plánů kontinuity

Na základě výsledků analýzy rizik, byla dle normy ISO/IEC 27001 vypracována Business Impact Analysis, zkráceně BIA, pro určení služeb nebo jiných aktiv, pro které by měly v podniku být vypracovány plány kontinuity. Na základě BIA bylo rozhodnuto o vypracování plánů pro všechny služby a aktiva s ohodnocením bezpečnostního atributu „Dostupnost“ hodnotnou „Kritická“.

Tuto metriku navrhuji pro pravidelné získávání přehledu, kolik plánů kontinuity podnik má vypracovaných na základě BIA a kolik plánů ještě vypracovaných není.

Jelikož dle normy ISO/IEC 27002 by měla být BIA pravidelně přezkoumávána, může podnik v budoucnu zjistit, že jsou nutné i jiné plány a počet potřebných plánů se tak může v čase měnit. Z tohoto důvodu tato metrika není plánována jednorázově, ale mělo by být provedeno pravidelné měření a na jeho základě by měla být situace řešena.

ID metriky: 008

Informační potřeba: Touto metrikou je měřen stav vytvořených plánů kontinuity dle hodnocení dopadů na kontinuitu klíčových služeb v podniku. Tedy kolik plánů kontinuity je vytvořeno pro služby ohodnocených bezpečnostním atributem Dostupnost jako „Kritická“.

Název metriky: Stav vytvořených plánů kontinuity

Vzorec/bodování: K1 – [Počet vytvořených plánů kontinuity pro služby s ohodnocením dostupnosti jako „Kritická“ / Počet služeb s ohodnocením bezpečnostního atributu Dostupnost jako „Kritická“] × 100. Výsledek je zaokrouhlen na jednotky, tedy bez uvádění desetinného místa.

Cíl: K1 > 90 % – není požadována žádná akce
90 % > K1 > 80 % – vyžadováno monitorování počtu provedených plánů, pokud se hodnoty nezlepšují, je zahájeno přezkoumání
K1 < 80 % – nahlášení neshody vedoucímu ICT, přezkoumání příčiny nevytváření plánů kontinuity u významných aktiv z hlediska dostupnosti. Musí být vytvořen dostačující počet plánů kontinuity.

Důkaz implementace: Vytvořené plány kontinuity.

Četnost: Shromažďování dat: Měsíčně

	Analýza: Ročně Období měření: Roční
Odpovědné strany:	Osoba odpovědná za metriku: Vedoucí ICT Osoba shromažďující informace: IT administrátor Osoba odpovědná za analýzu výsledků: IT administrátor specialista
Zdroj dat:	Vytvořené plány kontinuity, uložené na file serveru.
Formát podávání zpráv:	Histogram znázorňující procentuální stav vytvořených plánů kontinuity v měřením období.

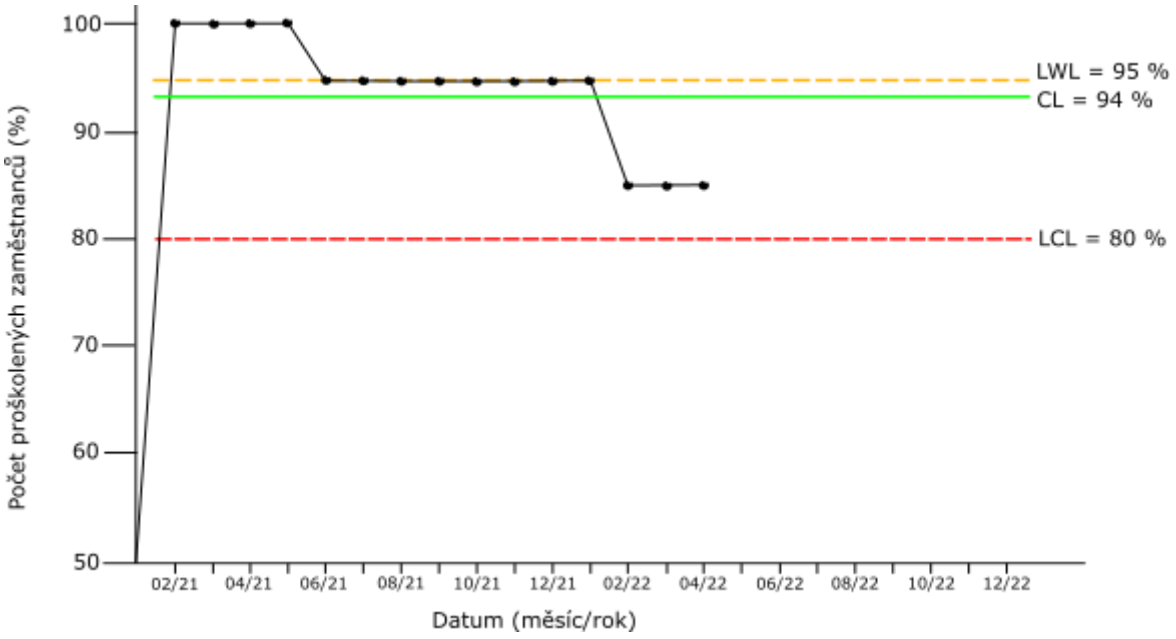
9 VYHODNOCENÍ VÝSLEDKŮ METRIK

V této kapitole jsou uvedeny výsledky metrik, získané při měření, které mi byly poskytnuty zaměstnanci podniku. V následujících kapitolách uvedu vyhodnocení výsledků na základě cílových hodnot metrik a při nesplnění cílů metriky navrhnu možné řešení. Dále jsem pro většinu metrik vytvořil grafický výstup pro znázornění, jak by měl vypadat výstup z metriky ve chvíli, kdy se bude předkládat vedení podniku. Vedení podniku by dle normy ISO/IEC 27001, měly být výsledky metrik předány k přezkoumání, aby vedení mohlo zhodnotit efektivnost metrik a při nesplnění cílů poskytnout patřičné zdroje pro navrhovaná opatření.

9.1 Vyhodnocení metriky Proškolení zaměstnanců v rámci bezpečnosti informací

Data pro tuto metriku byla shromážděna od února roku 2021, kdy proběhlo poslední školení o bezpečnosti informací. V dubnu roku 2022 byla provedena první analýza. Na níže uvedeném regulačním diagramu, který byl vytvořen pro lepší interpretaci výsledků metriky, lze vidět, že klesl počet proškolených zaměstnanců v dubnu roku 2021 o 5 % a následně v únoru roku 2022 o 10 %. Po přezkoumání příčiny bylo zjištěno, že toto snížení je způsobeno výměnou zaměstnanců. Jeden nový zaměstnanec nastoupil v dubnu 2021 a dva zaměstnanci nastoupili v únoru 2022.

Graf 1. Regulační diagram pro přehled proškolených zaměstnanců [zdroj: vlastní tvorba]



Jak je vidět z diagramu výše a z výstupu metriky, snižuje se procento proškolení zaměstnanců s každým novým zaměstnancem. Do doby, kdy proběhne po dvou letech nové školení, mohla by úroveň bezpečnostního povědomí zaměstnanců klesnout na neakceptovatelnou až rizikovou hranici pro podnik. Větší počet přijetí nových zaměstnanců zapříčiní náhlý skok v chování trendu a zapříčiní tak nestabilitu procesu.

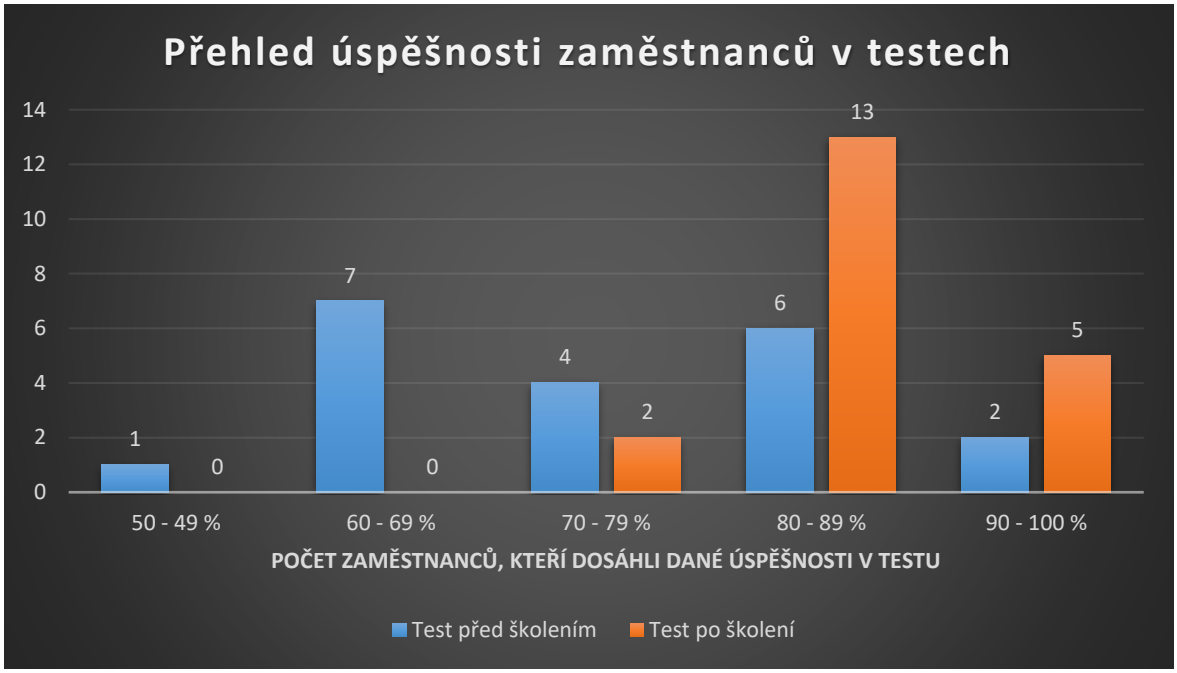
Doporučuji tedy provádět školení o bezpečnosti informací více frekventovaně, například jednou za půl roku, aby byli patřičně proškoleni i nastupující zaměstnanci. Další možností, dle mého názoru je, aby bylo školení všech nově nastupujících zaměstnanců individuálně v rámci zkušební doby.

9.2 Vyhodnocení metriky Porozumění zaměstnanců e-learningovému školení

Jak jsem zmínil v kapitole 8.1.3 v podniku bylo pro zaměstnance zrealizováno školení, zabývající se sociálním inženýrstvím. Pro zjištění bezpečnostního povědomí zaměstnanců jim byl předložen vědomostní test před proběhnutím školení a poté, co proběhlo školení, dostali znovu test s jinými otázkami. Jak lze vidět z grafu níže, před školením prošlo testem 8 zaměstnanců, zatímco při druhém testu mělo dostatečné bezpečnostní povědomí 18 zaměstnanců, což ukazuje na vysoké zlepšení. Z grafu 3 lze dokonce vidět, že žádný ze zaměstnanců se nepohyboval po provedení testu v hodnotách úspěšnosti 50 až 69 %.

Graf 2. Sloupcový graf pro určení poměru úspěšnosti v testu [zdroj: vlastní tvorba]

Graf 3. Sloupcový graf pro přehled úspěšnosti zaměstnanců dle jejich výsledků [zdroj: vlastní tvorba]

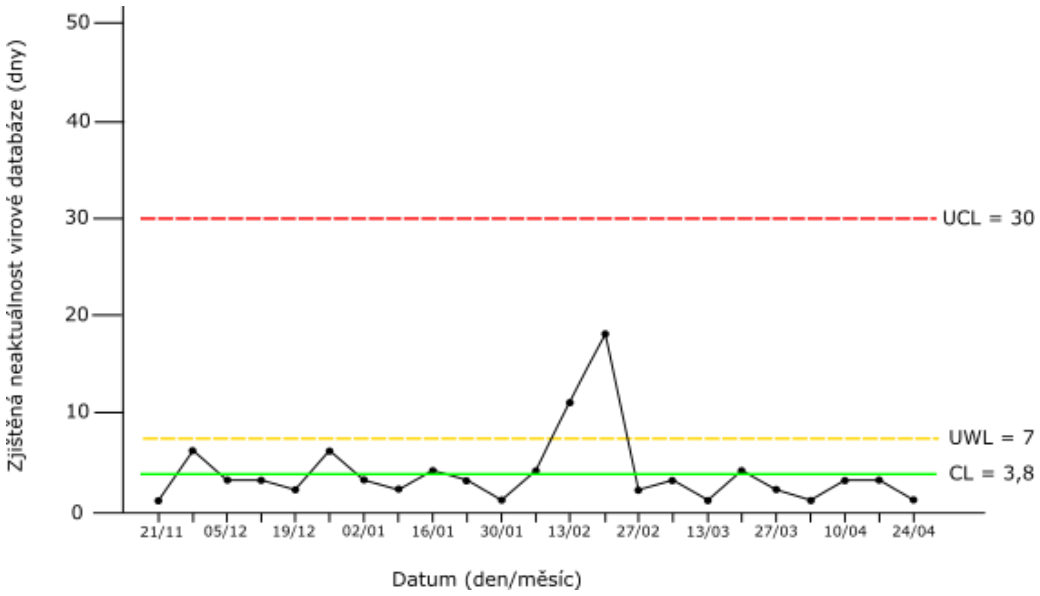


Podle vzorce metriky bylo vyhodnoceno, že počet zaměstnanců, kteří získali v testu více jak 80 % se zvýšil o 55 % díky e-learningovému školení. Na základě těchto výsledků byl splněn cíl metriky a e-learningové školení může být považováno za úspěšně a efektivní.

9.3 Vyhodnocení metriky Aktuálnost antivirové databáze

Pro interpretaci výsledků metriky byl vytvořen níže uvedený regulační digram, na kterém lze vidět, že UCL nebylo překročeno, pouze v průběhu února 2022 byla zvýšena neaktuálnost virové databáze na 17 dní. Na základě těchto hodnot byla dne 2.3.2022 provedena analýza a následné přezkoumání, při kterém bylo zjištěno, že příčinou byla deaktivace automatické činnosti aktualizace virové databáze. Toto deaktivování bylo zapříčiněno aktualizací celého systému ESET PROTECT. Poté byl problém odstraněn a aktualizace databáze byla nastavena tak, aby probíhala automaticky. Z následujících hodnot vyplývá, že počet dní, kdy je databáze neaktuální, je od té doby udržován konstantně na nízké úrovni.

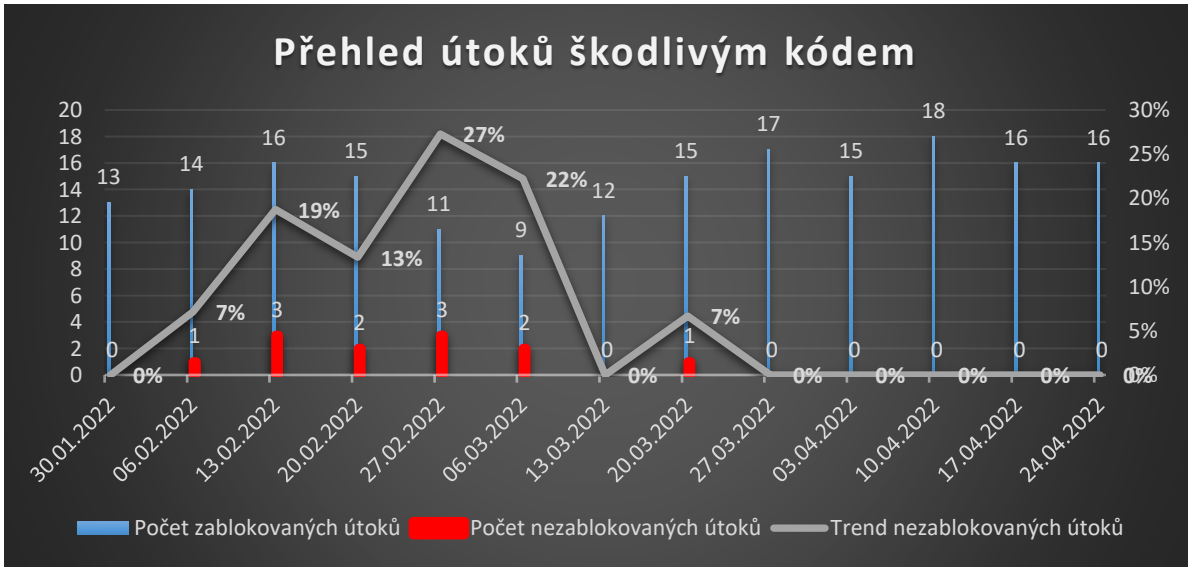
Graf 4. Regulační digram aktuálnosti virové databáze [zdroj: vlastní tvorba]



9.4 Vyhodnocení metriky Útoky škodlivým kódem s dopadem

Na základě metriky byla shromažďována data o zablokovaných a nezablokovaných útocích, zapříčiněných škodlivým kódem. Data byla shromážděna IT administrátorem od konce ledna roku 2022. Po provedení analýzy rizik byla zavedena bezpečnostní opatření pro snížení hrozeb, spojených se škodlivým kódem, v polovině března roku 2022. Od zavedení těchto bezpečnostních opatření lze z grafu vidět, že počet nezablokovaných útoků škodlivého kódu byl snižován a počet zablokovaných útoků se naopak zvyšoval. Z trendu označeným šedou barvou je patrné, že poměr nezablokovaných útoků má snižující se tendenci a proces spolu s bezpečnostními opatřeními je tedy efektivní.

Graf 5. Grafický přehled útoků škodlivým kódem [zdroj: vlastní tvorba]



9.5 Vyhodnocení metriky Počet incidentů u dodavatelů

Podnik má v současnosti se 4 dodavateli ve smluvních podmínkách podepsanou povinnost hlášení bezpečnostních incidentů. Hlášení od dodavatelů byla shromážděna za čtvrtý kvartál roku 2021 a první kvartál roku 2022. Dle metriky by měla analýza být provedena po čtyřech kvartálech, pro účely této práce byla však provedena dříve se současnými shromážděnými daty. Ohodnocení dodavatelů dle metriky je znázorněno v následující tabulce:

Tabulka 10. Hodnocení bezpečnostních incidentů u dodavatelů [zdroj: vlastní tvorba]

Popis dodavatele	**Vyhodnocovaný kvartál a rok vyhodnocení**	**U dodavatele za měřené období nenastal bezpečnostní incident ovlivňující bezpečnost informací.**	**U dodavatele za měřené období nastal bezpečnostní incident, neovlivňuje však smluvní vztah mezi podnikem a dodavatelem.**	**U dodavatele za měřené období nastal bezpečnostní incident, který ovlivňuje smluvní vztah mezi podnikem a dodavatelem. Pro podnik nevznikl žádný finanční nebo právní dopad.**	**U dodavatele za měřené období nastal bezpečnostní incident, který ovlivňuje smluvní vztah mezi podnikem a dodavatelem. Pro podnik vznikl v souvislosti s incidentem finanční nebo právní dopad.**	**Počet bodů:**
Dodavatel elektrického napájení	4Q/2021			**x**		**3**
	1Q/2022		**x**			**2**
Dodavatel kamerového systému	4Q/2021		**x**			**2**
	1Q/2022	**x**				**1**
Správa EZS	4Q/2021	**x**				**1**
	1Q/2022	**x**				**1**
Právnické služby	4Q/2021	**x**				**1**
	1Q/2022	**x**				**1**

Z tabulky ohodnocení dodavatelů vyplývá, že pouze jeden dodavatel byl ohodnocen 3 body. Dle metriky je tento dodavatelský vztah monitorován a pokud by nedošlo ke zlepšení, měl by podnik zauvažovat o změně dodavatele. Doplnění bezpečnostních požadavků do původní smlouvy není bohužel pravděpodobné, jelikož se jedná o velkou firmu, která ke změně podmínek nepřistupuje.

9.6 Vyhodnocení metriky Sjednání požadavků na bezpečnost informací ve smlouvách s dodavateli

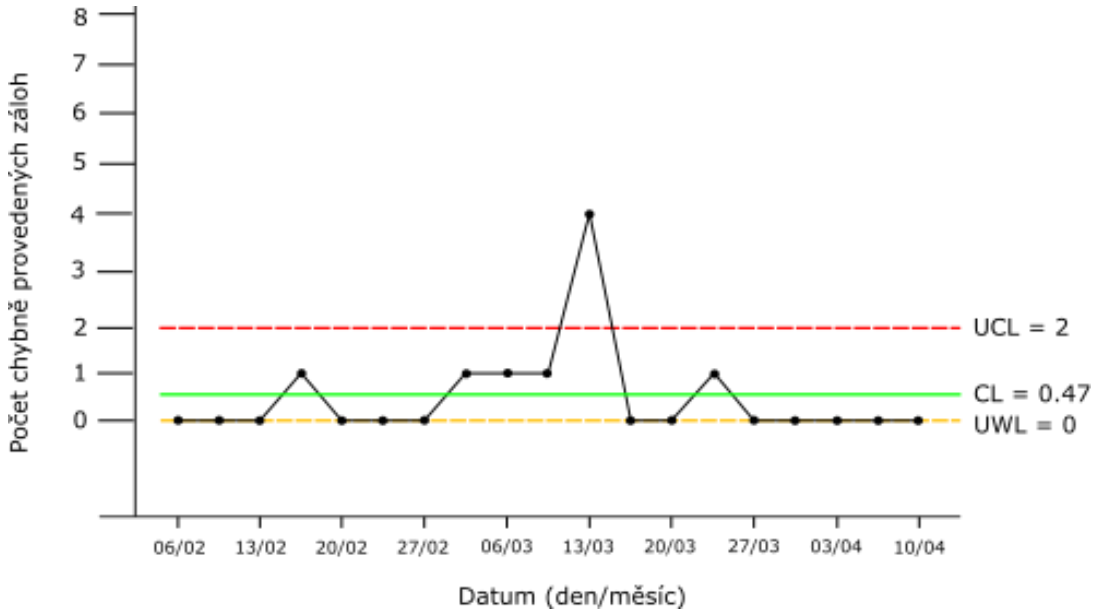
Při měření kritéria 1 bylo zjištěno, že poměr řešených bezpečnostních požadavků ve smlouvách s dodavateli je 63 %. Řešení bezpečnostních požadavků je tedy v podniku v současné době dostačující a následující kroky budou stanoveny až po další analýze za rok od současného měření.

Jelikož se jedná o první analýzu dle postupu metriky, neexistují data, která by bylo možné porovnat. Z toho důvodu v současné chvíli není možné posoudit kritérium 2, jehož cílem je stabilní nenarůstající trend.

9.7 Vyhodnocení metriky Správnost provádění záloh dat

Pro interpretaci výsledků metriky byl vytvořen níže uvedený regulační digram, ze kterého je zřejmé, že při měření bylo odhaleno překročení UCL v březnu roku 2022. Po provedení analýzy a následném přezkoumání, bylo zjištěno, že zálohy nejsou prováděny z důvodu plné kapacity zálohovacích disků. Tento problém byl odstraněn a z následujících hodnot lze vidět, že počet nesprávně provedených záloh je udržován konstantní na úrovni CL.

Graf 6. Regulační digram počtu nesprávně provedených záloh [zdroj: vlastní tvorba]



Na základě výsledků navrhuji doplnit novou metriku, která by monitorovala a měřila kapacitu zálohovacích disků na zálohovacím serveru, aby se předešlo podobným situacím a tím byla ještě více omezena možnost neprovedení zálohy dle plánu zálohování.

9.8 Vyhodnocení metriky Stav vytvořených plánů kontinuity

Dle postupu metriky bylo vyhodnoceno, kolik plánů kontinuity není v současné době vytvořených. Bylo zjištěno, že nejsou vytvořeny 2 plány kontinuity pro služby nebo aktiva, která jsou ohodnocena dostupností jako „Kritická“. Plány jsou vytvořeny tedy ze 77 %, čímž není splněn cíl metriky.

Nesplnění cíle bylo konzultováno s vedoucím ICT a bylo zjištěno, že plány nebyly vytvořeny z důvodu časové prodlevy při plnění úkolu. Navrhuji tedy těmto úkolům přiřadit vyšší prioritu, popřípadě využít externí společnost pro vytvoření plánů kontinuity.

Jelikož byla tato metrika vyhodnocena poprvé a plány kontinuity jsou vytvářeny teprve od konce minulého roku, nejsou k dispozici data, se kterými by mohla být data získaná při tomto měření porovnána. Z tohoto důvodu nebyly výstupy metriky interpretovány histogramem, ten bude vytvořen až při analýze následujícího měření.

ZÁVĚR

Diplomová práce byla zaměřena na malou, českou firmu, zabývající se vývojem softwaru, ICT službami a službami operátora sítě. Podnik se v průběhu práce připravoval na certifikaci podle normy ISO/IEC 27001 a ISO 9001.

S vedením podniku jsme se dohodli na návrhu metrik, jejímž používáním by mohl podnik stanovit efektivitu jeho procesů spojených se systémem řízení bezpečnosti informací. Definováním těchto metrik a jejich následným měřením a vyhodnocením výsledků podnik plní jeden z požadavků normy ISO/IEC 27001 a částečně požadavek normy ISO 9001.

K zajištění podkladů pro návrh metrik mi bylo umožněno být přítomen u pracovní činnosti zaměstnanců, projít si firemní prostory a konzultovat současný stav bezpečnosti informací přímo se zaměstnanci podniku. Dále byla, ve spolupráci s vedením, vytvořena analýza rizik, díky níž došlo ke zjištění, jaká rizika jsou nejvyšší a se kterými procesy souvisejí. Tímto bylo možné určit, které procesy jsou v podniku nejméně efektivní.

Při navrhování metrik jsem vycházel z postupu a doporučení normy ISO/IEC 27004, aby byl podnik v rámci měření informační bezpečnosti co nejlépe připraven na certifikaci. Dále jsem vycházel ze svých praktických zkušeností a navrhnul metriky tak, aby byly pro podnik co nejvíce ekonomicky výhodné a zároveň, aby se jim zaměstnanci mohli snadno přizpůsobit.

Procesy související s bezpečností informací byly stanoveny dle bezpečnostních opatření vyhlášky o kybernetické bezpečnosti tím způsobem, aby se podnik už při této přípravě co nejvíce připravil k možnému zavedení požadavků zákona o kybernetické bezpečnosti.

Dalším hlediskem při návrhu metrik bylo, aby odrážely efektivitu nejen procesů, ale i navržených bezpečnostních opatření, jejichž cílem bylo snížit zjištěná rizika z analýzy rizik. Tím se podařilo splnit jeden z dalších požadavků normy ISO/IEC 27001.

Pro metriky byl rovněž stanoveno, jak má probíhat postup měření a jak mají být výsledky metrik vyhodnoceny. Na základě výsledků jsem, ve spolupráci se zaměstnanci, metriky vyhodnotil a určil efektivitu procesů, spojených se systémem řízení bezpečnosti informací. Pokud při vyhodnocení byla zjištěna neefektivita, navrhl jsem adekvátní kroky ke zvýšení efektivity procesu.

V současné chvíli si dovoluji tvrdit, že podnik je připraven na certifikaci dle normy ISO/IEC 27001 z pohledu požadavku definovat monitorování a měření procesů či bezpečnostních opatření, spojených se systémem řízení bezpečnosti informací.

Dle mnou navrženého postupu může podnik v budoucnu rozšířit počet metrik dle aktuální situace a zvýšit tak rozsah měření efektivity zavedeného systému řízení bezpečnosti informací.

SEZNAM POUŽITÉ LITERATURY

[1] LESTYÁNSZKA ŠKŮRKOVÁ, Katarína, Marta KUČEROVÁ a Helena FIDLEROVÁ. Experience Of Implementing The Integrated Management System In Manufacturing Companies In Slovakia. Research Papers Faculty of Materials Science and Technology Slovak University of Technology [online]. 2015, 23(36), 179-186 [cit. 2022-04-21]. ISSN 1338-0532. Dostupné z: doi:10.1515/rput-2015-0021

[2] INTEGROVANÉ SYSTÉMY ŘÍZENÍ. TÜV SÜD CZECH [online]. [cit. 2022-04-21]. Dostupné z: https://www.tuvsud.com/cs-cz/cinnosti/audity-a-certifikace-systemu/integrovane-systemy-rizeni

[3] NOVÁK, Luděk a Josef POŽÁR. Systém řízení informační bezpečnosti [online]. In: . s. 10 [cit. 2022-04-21]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf

[4] GOGELA, Robert, CISA a CISM. Standardy a definice pojmů bezpečnosti informací [online]. In: . s. 5 [cit. 2022-04-21]. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf

[5] Zavedení systému řízení bezpečnosti – ISMS - 1.díl. GiTy [online]. [cit. 2022-04-21]. Dostupné z: https://www.chrantesidata.cz/cs/art/472-isms-serial-o-rizeni-bezpecnosti

[6] ISO 27002 - nejlepší bezpečnostní praktiky. Management Mania [online]. 2017 [cit. 2022-04-21]. Dostupné z: https://managementmania.com/cs/iso-27002-nejlepsi-bezpecnostni-praktiky

[7] GOLL, Jan. Zákon o kybernetické bezpečnosti versus ISO 27001: aneb jak vyhovět oběma normám [online]. [cit. 2022-05-21]. Dostupné z: https://www.systemonline.cz/sprava-it/zakon-o-kyberneticke-bezpecnosti-versus-iso-27001.htm

[8] BEDNÁŘOVÁ, Dagmar. Řízení kvality. V Českých Budějovicích: Jihočeská univerzita, Ekonomická fakulta, 2013. ISBN 978-80-7394-404-9.

[9] Management kvality. Publi.cz [online]. [cit. 2022-04-21]. Dostupné z: https://publi.cz/books/276/03.html

[10] Demingův cyklus PDCA: a norma ISO/IEC 20000-1:2011. Časopis IT Systems [online]. 2011(12) [cit. 2022-04-21]. Dostupné z: https://www.systemonline.cz/sprava-it/deminguv-cyklus-pdca.htm

[11] PDCA (Plan Do Check Act): Continually Improving, in a Methodical Way. Mind Tools [online]. [cit. 2022-04-21]. Dostupné z: https://www.mindtools.com/pages/article/newPPM_89.htm

[12] SPEJCHALOVÁ, Dana. Management kvality. Praha: Vysoká škola ekonomie a managementu, 2007. ISBN isbn978-80-86730-22-6.

[13] NÚKIB. BEZPEČNOSTNÍ ROLE: a jejich začlenění v organizaci. Govcert.cz [online]. [cit. 2022-04-21]. Dostupné z: https://www.govcert.cz/download/kii-vis/VKB/bezpe%C4%8Dnostn%C3%AD-role_v1.1.pdf

[14] Encyklopedie profesí: Manažer kvality. Prace.cz [online]. [cit. 2022-04-21]. Dostupné z: https://www.prace.cz/encyklopedie-profesi/m/manazer-kvality/

[15] MAŠÍN, Petr. Procesní management. [Praha]: Vysoká škola ekonomie a managementu, 2020. ISBN isbn:978-80-88330-07-3.

[16] URBÁNEK, Jiří. Teorie procesů - management environmentů. Brno: Akademické nakladatelství CERM, 2002. ISBN isbn80-7204-232-7.

[17] FIALA, Alois a Monika BECKOVÁ. Management procesů: průvodce manažera kvality. Praha: Dashöfer, 2006. ISSN 18021697.

[18] STŘELEC, Jiří. VLASTNÍK PROCESU. Vlastnicesta.cz [online]. 2012 [cit. 2022-04-21]. Dostupné z: https://www.vlastnicesta.cz/slovnik-pojmu/vlastnik-procesu/

[19] Zdroje (Business resources). Management Mania [online]. 2019 [cit. 2022-04-21]. Dostupné z: https://managementmania.com/cs/zdroje-podnikove-zdroje

[20] GRASSEOVÁ, Monika, Radek DUBEC a Roman HORÁK. Procesní řízení ve veřejném sektoru: teoretická východiska a praktické příklady. Brno: Computer Press, 2008. ISBN 978-80-251-1987-7.

[21] ŠEBEK, V. Řízení projektů a podnikových procesů [online]. [cit. 2022-04-21]. Dostupné z: https://slideplayer.cz/slide/3338832/

[22] Procesní analýza (Process analysis). Management Mania [online]. 2018 [cit. 2022-04-21]. Dostupné z: https://managementmania.com/cs/analyza-procesu-procesni-analyza

[23] WHEELER, Donald J. a David S. CHAMBER. Understanding Statistical Process Control. ISBN 978-0-945320-69-2.

[24] Interpretace naměřených dat. Lean Six Sigma [online]. [cit. 2022-04-21]. Dostupné z: https://lean6sigma.cz/interpretace-namerenych-dat/

[25] Histogram [online]. [cit. 2022-04-21]. Dostupné z: https://www.agenturapoznani.cz/userFiles/histogram.pdf

[26] DEBINSKA, Ewa a Joanna PAŁUBSKA. Property price dependence from noise level on example of local real estate market. Budownictwo i Architektura [online]. 2020, 18(3), 073-082 [cit. 2022-04-21]. ISSN 2544-3275. Dostupné z: doi:10.35784/bud-arch.815

[27] ČSN ISO/IEC 27004 Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Monitorování, měření, analýza a hodnocení. 2018.

[28] ČSN EN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací. 2014.

[29] Antivirový program. Antivirovecentrum.cz [online]. [cit. 2022-05-21]. Dostupné z: https://www.antivirovecentrum.cz/antiviry.aspx

[30] Firewall. ESET [online]. [cit. 2022-05-21]. Dostupné z: https://www.eset.com/cz/firewall/

[31] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN ISBN978-80-88168-32-4.

[32] Co je to proxy server. Správa Sítě [online]. [cit. 2022-05-21]. Dostupné z: https://www.sprava-site.eu/proxy-server/

[33] VÁLKA, Radek. Bezpečnost mobilních zařízení v malé společnosti. Brno, 2020. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Viktor Ondrák, Ph.D.

[34] VYMAZAL, Radek. MANAGEMENT LOGŮ A INSTALACE GRAYLOG. Connectica [online]. [cit. 2022-05-21]. Dostupné z: https://radekvymazal.cz/management-logu-a-instalace-graylog/

[35] Business Impact Analysis (BIA) Analýza dopadů. Dcit.cz [online]. [cit. 2022-05-21]. Dostupné z: https://www.dcit.cz/cs/bezpecnost/analyza-dopadu-BIA

[36] Co to je malware. Internetem bezpečně [online]. [cit. 2022-05-21]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/co-to-je-malware/

[37] Sociální inženýrství. ManagementMania.com [online]. [cit. 2022-05-22]. Dostupné z: https://managementmania.com/cs/socialni-inzenyrstvi

[38] Sociální inženýrství. Národní centrum kybernetické bezpečnosti [online]. [cit. 2022-05-21]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

[39] ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací. 2019.

[40] Security Tip (ST08-001): Using Caution with USB Drives. Cybersecurity and Infrastructure Security Agency [online]. [cit. 2022-05-21]. Dostupné z: https://www.cisa.gov/uscert/ncas/tips/ST08-001

[41] Zákon č. 563/1991 Sb.: Zákon o účetnictví. In: . ročník 1991. Dostupné také z: https://www.zakonyprolidi.cz/cs/1991-563

[42] Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: . ročník 2018. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BIA	Business Impact Analysis
BS	British Standard
CISA	Cybersecurity and Infrastructure Security Agency
CL	Central Line
CWQC	Company Wide Quality Control
ČSN	Českomoravské technické normy
EZS	Elektronická zabezpečovací signalizace
HW	Hardware
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IMS	Integrated Management System
IS	Information system
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information technology
LCL	Lower Control Line
LWL	Lower Warning Limit
MS	Microsoft
NAS	Network Attached Storage
NDA	Non-disclosure agreement
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PC	Personal computer
QMS	Quality Management System
SW	Software

TQM	Total Quality Management
UCL	Upper Control Line
UPS	Uninterruptible Power Supply/Source
USB	Universal Serial Bus
UWL	Upper Warning Limit
VPN	Virtual private network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

Příloha P1: Registr aktiv podniku

ID Aktiva	Název skupiny	Aktivum (název)	Popis aktiva	Garant aktiva
1	služby	**Síťové služby s vyšší prioritou**	Jedná se o síťová zařízení (switche) s vyšší prioritou pro podnik	Vedoucí ICT
2	služby	**Síťové služby s nižší prioritou, Optické převodníky, Wi-Fi**	Síťová zařízení jako switche, optické převodníky, Wi-Fi access pointy s nižší prioritou pro podnik	Vedoucí ICT
3	Hardware	**Kabeláž**	Rozvod kabeláže v areálu podniku	Vedoucí ICT
4	Hardware	**Úložiště on-line záloh**	Zařízení Synology NAS 2x pro zálohy dat	Vedoucí ICT
5	Hardware	**Úložiště off-line záloh**	Zařízení Synology NAS 1x, záloha dat	Vedoucí ICT
6	Hardware	**Datastore**	Zařízení Lenovo datastore – úložiště produkčních serverů	Vedoucí ICT
7	Hardware	**Produkční servery**	Fyzické produkční servery – Lenovo a IBM servery	Vedoucí ICT
8	Hardware	**Záložní a testovací servery**	Fyzické záložní a testovací servery IBM	Vedoucí ICT
9	Hardware	**Vývojářský server**	Fyzický server Lenovo	Ředitel odd. programování
10	Hardware	**Pracovní stanice ICT oddělení**	Notebooky a stolní počítače pracovníků ICT oddělení	Vedoucí ICT
11	Hardware	**Pracovní stanice programátorů**	Notebooky a stolní počítače pracovníků programátorského oddělení	Ředitel odd. programování
12	Hardware	**Pracovní stanice ostatních oddělení**	Notebooky a stolní počítače ostatních oddělení	Vedoucí ICT
13	Hardware	**Telefony, tablety**	Firemní telefony a tablety zaměstnanců	Vedoucí ICT
14	Hardware	**Kamerový systém**	Systém tvořený z kamer, kamerového servere v areálu podniku a obrazové záznamy na serveru	Vedoucí ICT
15	Hardware	**Tiskárny**	Tiskárny v areálu podniku	Předseda představenstva
16	Hardware	**EZS, docházkový systém a klíče**	EZS vč. čidel, docházkové čipy a klíče	Předseda představenstva
17	Hardware	**Agregáty a UPS**	Dieselové agregáty a napájecí zařízení UPS	Vedoucí ICT
18	služby	**Zabezpečené připojení do internetu a VPN**	Ochrana před škodlivými programy z internetu, kontrola příchozí pošty a poskytování služby VPN do firmy	Vedoucí ICT
19	Služby	**Služba pro přenos dat**	Služba přenosu dat poskytovaná našim zákazníkům	Ředitel odd. programování
20	služby	**Active directory**	Služba správy rolí – Active directory	Vedoucí ICT
21	služby	**Exchange**	Poštovní server	Vedoucí ICT
22	služby	**File server, Byznys**	File server a Byznys systém – ekonomický systém	Vedoucí ICT
23	služby	**Zálohovací a monitorovací server**	Server pro zálohování a monitoring HW serverů	Vedoucí ICT
24	služby	**Servery – EZS, Docházka, VCS, ostatní**	Služby EZS, zaznamenávání docházky, management vmware serveru a ostatních serverů	Předseda představenstva
25	služby	**OTRS ICT**	Tiketovací systém ICT oddělení	Vedoucí ICT
26	Software	**Serverové aplikace pro vývoj**	Redmine, GitLab, TeamCity, OTRS, Wiki, Terminálový server, AD, serverové OS	Ředitel odd. programování
27	Software	**Testovací aplikační servery**	Hosting testovacích verzí námi vyvíjeného SW	Ředitel odd. programování

28	Software	**Testovací databázové servery**	Spravované testovací data vyvíjeného SW	Ředitel odd. programování
29	Software	**IS Target**	Systém pro správu informací o zaměstnancích a dodavatelích	Personalistka
30	Software	**Software pro přenos dat**	Námi vyvinutý SW zajišťující provoz služby a přenos dat mezi zákazníky	Ředitel odd. programování
31	Informace/data	**Konfigurace a data active directory**	Konfigurace a data ze systému active directory	Vedoucí ICT
32	Informace/data	**Konfigurace a data Exchange**	Konfigurace a data ze systému Exchange	Vedoucí ICT
33	Informace/data	**Data na file serveru, Byznysu**	Data na file serveru a vy systému Byznys	Vedoucí ICT
34	Informace/data	**Zálohy na NAS zařízeních**	Zálohovaná data na NAS zařízeních (2x on-line, 1x off-line)	Vedoucí ICT
35	Informace/data	**Konfigurace a data v EZS, Docházce, VCS, ostatní**	Konfigurace a data v EZS, systému Docházka, data z managementu serveru vmware a ostatních servery	Předseda představenstva
36	Informace/data	**Data v OTRS ICT**	Data v tiketovacím systému ICT oddělení	Vedoucí ICT
37	Informace/data	**Dokumentace zákazníků ICT**	Dokumentace zákazníků uložená na file serveru	Vedoucí ICT
38	Informace/data	**Přístupová hesla zákazníků ICT**	Přístupová hesla zákazníků uložená na file serveru	Vedoucí ICT
39	Informace/data	**Zdrojové kódy**	Uložené zdrojové kódy, včetně jejich historie, build skriptů a konfigurace	Ředitel odd. programování
40	Informace/data	**Kamerové záznamy**	Záznamy z kamer uložené na serveru pro kamery	Vedoucí ICT
41	Informace/data	**Projektová dokumentace**	Smlouvy, objednávky, analýzy, zápisy z jednání, požadavky zadavatele na vývoj, údržbu a technickou podporu k vyvíjenému SW	Ředitel odd. programování
42	Informace/data	**Testovací data**	Data vytvořená při vývoji SW, data poskytnutá zadavatelem	Ředitel odd. programování
43	Informace/data	**Provozní informace**	Licenční soubory/klíče k vývojářským nástrojům a knihovnám, instalátory uložené na file serveru, programátorská wiki, pracovní deníky, off-line dokumentace k používaným nástrojům a knihovnám, telefonní seznam	Ředitel odd. programování
44	Informace/data	**Dokumenty zákazníka**	Archiv zpráv zasílaných prostřednictvím služby pro přenos dat	Ředitel odd. programování
45	Software	**Antivirový program**	ESET POTECT – antivirový SW na koncových zařízeních, produkčních serverech	Vedoucí ICT
46	Software	**SW – servery a aplikace**	SW – MS Windows server, Exchange, Veeam, Byznys, vmware, Sophos a ostatní SW	Vedoucí ICT
47	Software	**SW – Stanice a aplikace**	SW – MS Windows, MS Office a ostatní SW	Vedoucí ICT
48	Dodavatelé	**Správa EZS**	Dodavatel zodpovědný za chod EZS	Vedoucí ICT
49	Dodavatelé	**Právnické služby**	Firma poskytující právnické služby	Předseda představenstva
50	Dodavatelé	**Klíčové služby – internet**	Dodavatel konektivity k internetu	Vedoucí ICT
51	Dodavatelé	**Klíčové služby – vytápění**	Dodavatel vytápění	Předseda představenstva
52	Dodavatelé	**Klíčové služby – elektřina**	Dodavatel elektrického proudu	Předseda představenstva

53	Dodavatelé	**Kamerový systém**	Firma spravující kamerový systém a mající vzdálený přístup do kamerového systému	Vedoucí ICT
54	Prostory	**Veřejné prostory**	Venkovní areál podniku	Předseda představenstva
55	Prostory	**Zabezpečené prostory - kancelářské**	Kancelářské prostory, ve kterých se nachází citlivé údaje	Předseda představenstva
56	Prostory	**Zabezpečené prostory - technické**	Prostory s technickou infrastrukturou (např. komunikační místnosti s aktivními prvky, serverovna)	Vedoucí ICT
57	Prostory	**Red Zone**	Zabezpečená a zamřížovaná místnost s bytelnými dveřmi a samostatnými čipy umožňujícími vstup	Ředitel odd. programování
58	Prostory	**Nezabezpečené prostory**	Oblasti budovy, kde se nenachází citlivé údaje (jídelna, toalety,...)	Předseda představenstva
59	Zaměstnanci	**Management**	Členové představenstva	Předseda představenstva
60	Zaměstnanci	**Vedoucí pracovníci**	Vedoucí pracovníci jednotlivých oddělení	Předseda představenstva
61	Zaměstnanci	**Uživatelé s omezenými oprávněními**	Zaměstnanci s neprivilegovanými právy	Předseda představenstva
62	Zaměstnanci	**Uživatelé s privilegovanými oprávněními**	Zaměstnanci s privilegovanými právy - administrátoři	Předseda představenstva

Příloha P2: Ohodnocení aktiv z pohledu důvěrnosti, integrity a dostupnosti

Aktivum (název)	Klasifikace		
	Důvěrnost	**Integrita**	**Dostupnost**
Síťové služby s vyšší prioritou	Střední	N/A[2]	Kritická
Síťové služby s nižší prioritou, Optické převodníky, Wi-Fi	Střední	N/A	Střední
Kabeláž	Nízká	N/A	Střední
Úložiště on-line záloh	Vysoká	Vysoká	Střední
Úložiště off-line záloh	Vysoká	Vysoká	Nízká
Datastore	Vysoká	Vysoká	Kritická
Produkční servery	Vysoká	Vysoká	Kritická
Záložní a testovací servery	Nízká	Nízká	Nízká
Vývojářský server	Střední	Kritická	Střední
Pracovní stanice ICT oddělení	Vysoká	Nízká	Střední
Pracovní stanice programátorů	Vysoká	Kritická	Střední
Pracovní stanice ostatních oddělení	Vysoká	Nízká	Nízká
Telefony, tablety	Vysoká	Nízká	Nízká
Kamerový systém	Vysoká	Nízká	Střední
Tiskárny	Nízká	N/A	Střední
EZS, docházkový systém a klíče	Vysoká	Střední	Vysoká
Agregáty a UPS	Střední	Střední	Vysoká
Zabezpečené připojení do internetu a VPN	Střední	N/A	Vysoká
Služba pro přenos dat	Vysoká	Střední	Kritická
Active directory	Nízká	Vysoká	Vysoká
Exchange	Nízká	Vysoká	Vysoká
File server, Byznys	Nízká	Vysoká	Vysoká
Zálohovací a monitorovací server	Nízká	Vysoká	Vysoká
Servery – EZS, Docházka, VCS, ostatní	Střední	Střední	Střední
OTRS ICT	Nízká	Nízká	Vysoká
Serverové aplikace pro vývoj	Nízká	Střední	Střední
Testovací aplikační servery	Nízká	Nízká	Nízká
Testovací databázové servery	Nízká	Nízká	Střední
IS Target	Vysoká	Vysoká	Střední
Software pro přenos dat	Střední	Nízká	Kritická
Konfigurace a data active directory	Vysoká	Vysoká	Kritická
Konfigurace a data Exchange	Vysoká	Vysoká	Kritická
Data na file serveru, Byznysu	Vysoká	Vysoká	Střední
Zálohy na NAS zařízeních	Vysoká	Vysoká	Střední
Konfigurace a data v EZS, Docházce, VCS, ostatní	Střední	Střední	Střední
Data v OTRS ICT	Vysoká	Nízká	Nízká

[2] N/A – daný bezpečnostní atribut nelze klasifikovat z pohledu vybraného bezpečnostního atributu

Dokumentace zákazníků ICT	Vysoká	Střední	Střední
Přístupová hesla zákazníků ICT	Vysoká	Vysoká	Střední
Zdrojové kódy	Střední	Kritická	Střední
Kamerové záznamy	Vysoká	Střední	Střední
Projektová dokumentace	Střední	Střední	Nízká
Testovací data	Vysoká	Nízká	Nízká
Provozní informace	Střední	Nízká	Nízká
Dokumenty zákazníka	Vysoká	Vysoká	Kritická
Antivirový program	Kritická	Vysoká	Vysoká
SW – servery a aplikace	Nízká	Nízká	Nízká
SW – Stanice a aplikace	Nízká	Nízká	Nízká
Správa EZS	Střední	Vysoká	Střední
Právnické služby	Kritická	Střední	Nízká
Klíčové služby – internet	Střední	Vysoká	Kritická
Klíčové služby – vytápění	N/A	N/A	Střední
Klíčové služby – elektřina	N/A	N/A	Vysoká
Kamerový systém	Střední	Nízká	Vysoká
Veřejné prostory	Nízká	N/A	N/A
Zabezpečené prostory – kancelářské	Vysoká	N/A	Střední
Zabezpečené prostory – technické	Vysoká	N/A	Střední
Red Zone	Vysoká	N/A	Střední
Nezabezpečené prostory	Nízká	N/A	Nízká
Management	N/A	N/A	Vysoká
Vedoucí pracovníci	N/A	N/A	Střední
Uživatelé s omezenými oprávněními	N/A	N/A	Nízká
Uživatelé s privilegovanými oprávněními	N/A	N/A	Vysoká

Příloha P3: Analýza rizik ve kterých byla identifikována neakceptovatelná rizika

Název analýzy	Analýza služeb ICT oddělení			
Zahrnutá aktiva	**Zaměstnanci:** Uživatelé s omezenými oprávněními, Uživatelé s privilegovanými oprávněními			
	Služby: Síťové služby s vyšší prioritou, Síťové služby s nižší prioritou, Optické převodníky, Wi-Fi, Kabeláž, Active directory, Exchange, File server, Byznys, OTRS ICT			
	Hardware: Datastore, Produkční servery, Pracovní stanice ICT oddělení			
	Informace/data: Active directory, Exchange, Konfigurace a data active directory, Konfigurace a data Exchange, Dokumentace zákazníků ICT, Přístupová hesla zákazníků ICT, OTRS ICT, Data v OTRS ICT			
	Software: SW – servery a aplikace			
	Prostory: Zabezpečené prostory – technické, kancelářské			
Hodnota skupiny aktiv	**4**			
Název hrozby	**Název zranitelnosti**	**H** Pravděpodobnost	**Z** Snadnost zneužití	**Riziko**
Poškození nebo selhání technického anebo programového vybavení	Nedostatečná údržba informačního a komunikačního systému	3	2	24
	Zastaralost informačního a komunikačního systému	3	2	24
	Nedostatečná ochrana aktiv	3	1	12
Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	3	36
	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	3	2	24
	Nedostatečná míra nezávislé kontroly	3	2	24
Užívání programového vybavení v rozporu s licenčními podmínkami	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	2	1	8
	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	2	2	16
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	1	8
	Zastaralost informačního a komunikačního systému	3	3	36

Škodlivý kód (například viry, spyware, trojské koně)	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	2	24
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	3	36
	Neschopnost včasného odhalení pochybení ze strany zaměstnanců	3	2	24
Ztráta, odcizení nebo poškození aktiva	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	2	24
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	3	36
	Nedostatečná ochrana aktiv	3	2	24
Zneužití nebo neoprávněná modifikace údajů	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	2	2	16
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	2	16
	Nedostatečná míra nezávislé kontroly	2	3	24
	Neschopnost včasného odhalení pochybení ze strany zaměstnanců	2	3	24
Pochybení ze strany zaměstnanců	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	2	24
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	2	24
Zneužití vnitřních prostředků, sabotáž	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	1	2	8
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	1	2	8
	Nedostatečná míra nezávislé kontroly	1	3	12
Zneužití vyměnitelných technických nosičů dat	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	2	2	16
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	2	16
	Nedostatečná míra nezávislé kontroly	2	2	16

	Neschopnost včasného odhalení pochybení ze strany zaměstnanců	2	2	16
Zneužití identity	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	2	24
	Nevhodné nastavení přístupových oprávnění	3	1	12
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	2	24
Narušení fyzické bezpečnosti	Nedostatečná ochrana vnějšího perimetru	2	2	16
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	1	8
	Nedostatečná ochrana aktiv	2	1	8
Nedostatek zaměstnanců s potřebnou odbornou úrovní	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	3	36
	Nevhodná bezpečnostní architektura	3	1	12
Napadení elektronické komunikace (odposlech, modifikace)	Zastaralost informačního a komunikačního systému	2	2	16
	Nevhodné nastavení přístupových oprávnění	2	2	16
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	2	16
	Nevhodná bezpečnostní architektura	2	1	8
Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Nedostatečná ochrana aktiv	3	2	24
	Nevhodná bezpečnostní architektura	3	2	24
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	3	36
Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	Nedostatečná ochrana aktiv	2	2	16
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	2	16
	Nevhodná bezpečnostní architektura	2	2	16

Název analýzy	Analýza koncových zařízení (PC, notebooky)			
Zahrnutá aktiva	**Zaměstnanci:** Uživatelé s omezenými oprávněními, Uživatelé s privilegovanými oprávněními			
	Služby: OTRS ICT, File server, Byznys, Exchange, Active directory			
	Hardware: Pracovní stanice ICT oddělení, Pracovní stanice programátorů, Pracovní stanice ostatních oddělení			
	Informace/data: Data na file serveru, Byznysu, Data v OTRS ICT, Dokumentace zákazníků ICT, Projektová dokumentace, Provozní informace, Dokumenty zákazníka			
	Software: SW – Stanice a aplikace			
Hodnota skupiny aktiv	**4**			
Název hrozby	**Název zranitelnosti**	**H** Pravděpodobnost	**Z** Snadnost zneužití	**Riziko**
Poškození nebo selhání technického anebo programového vybavení	Nedostatečná údržba informačního a komunikačního systému	2	2	16
	Zastaralost informačního a komunikačního systému	2	2	16
	Nedostatečná ochrana aktiv	2	1	8
Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	4	3	48
	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	4	2	32
	Nedostatečná míra nezávislé kontroly	4	2	32
Užívání programového vybavení v rozporu s licenčními podmínkami	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	2	24
	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	3	2	24
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	2	24
Škodlivý kód (například viry, spyware, trojské koně)	Zastaralost informačního a komunikačního systému	4	2	32
	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	4	3	48

	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	4	3	48
	Neschopnost včasného odhalení pochybení ze strany zaměstnanců	4	2	32
Ztráta, odcizení nebo poškození aktiva	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	3	36
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	2	24
	Nedostatečná ochrana aktiv	3	2	24
Zneužití nebo neoprávněná modifikace údajů	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	2	2	16
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	2	16
	Nedostatečná míra nezávislé kontroly	2	3	24
	Neschopnost včasného odhalení pochybení ze strany zaměstnanců	2	2	16
Pochybení ze strany zaměstnanců	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	3	36
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	2	24
Zneužití vnitřních prostředků, sabotáž	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	2	1	8
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	2	16
	Nedostatečná míra nezávislé kontroly	2	2	16
Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	4	3	48
	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	4	2	32

	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	4	2	32
	Neschopnost včasného odhalení pochybení ze strany zaměstnanců	4	2	32
Zneužití vyměnitelných technických nosičů dat	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	3	36
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	2	24
	Nedostatečná míra nezávislé kontroly	3	2	24
	Neschopnost včasného odhalení pochybení ze strany zaměstnanců	3	1	12
Zneužití identity	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	2	24
	Nevhodné nastavení přístupových oprávnění	3	2	24
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	2	24

Název analýzy	Analýza dodavatele kamerového systému			
Zahrnutá aktiva	**Dodavatelé:** Kamerový systém			
	Služby: Síťové služby s vyšší prioritou, Zálohovací a monitorovací server			
	Hardware: Kabeláž, Kamerový systém, Záložní a testovací servery			
	Informace/data: Kamerové záznamy			
Hodnota skupiny aktiv	**4**			
Název hrozby	**Název zranitelnosti**	**H** Pravděpodobnost	**Z** Snadnost zneužití	**Riziko**
Poškození nebo selhání technického anebo programového vybavení	Nedostatečná údržba informačního a komunikačního systému	3	2	24
	Zastaralost informačního a komunikačního systému	3	2	24
	Nevhodná bezpečnostní architektura	3	1	12
Škodlivý kód (například viry, spyware, trojské koně)	Zastaralost informačního a komunikačního systému	2	2	16
	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	2	3	24
	Nevhodné nastavení přístupových oprávnění	2	3	24
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	3	24
Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Nedostatečná ochrana aktiv	2	1	8
	Nevhodná bezpečnostní architektura	2	2	16
Zneužití nebo neoprávněná modifikace údajů	Nevhodné nastavení přístupových oprávnění	3	2	24
	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	3	2	24
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	3	36
Nedodržení smluvního závazku ze strany dodavatele	Nevhodné nastavení přístupových oprávnění	4	2	32
	Nedostatečná míra nezávislé kontroly	4	2	32

	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	4	3	48
Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	Nedostatečná ochrana aktiv	2	1	8
	Nevhodná bezpečnostní architektura	2	2	16
Napadení elektronické komunikace (odposlech, modifikace)	Zastaralost informačního a komunikačního systému	2	2	16
	Nevhodné nastavení přístupových oprávnění	2	3	24
	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2	3	24
	Nevhodná bezpečnostní architektura	2	2	16
Zneužití identity	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	3	3	36
	Nevhodné nastavení přístupových oprávnění	3	2	24
	Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	3	2	24