VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

INFORMAČNÍ BEZPEČNOST JAKO JEDEN Z UKAZATELŮ HODNOCENÍ VÝKONNOSTI V ENERGETICKÉ SPOLEČNOSTI

INFORMATION SECURITY AS ONE OF THE PERFORMANCE INDICATORS IN ENERGY COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. Lukáš Kubík
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Petr Sodomka, Ph.D., MBA
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Lukáš Kubík**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**doc. Ing. Petr Sodomka, Ph.D., MBA**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Informační bezpečnost jako jeden z ukazatelů hodnocení výkonnosti v energetické společnosti

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Diplomová práce se zaměřuje na problematiku hodnocení zavádění systému informační bezpečnosti v energetické společnosti a vytvoření souboru ukazatelů pro určení rozsahu působnosti bezpečnosti informací na podnikovou výkonnost.

Základní literární prameny:

MOLNÁR, Z. Efektivnost informačních systémů. Praha: Grada Publishing, 2000. ISBN 80-7169-410-X.

POUR, J., L. GÁLA a Z. ŠEDIVÁ. Podniková informatika. 2. přepracované a aktualizované vydání. Praha: Grada Publishing, 2009. ISBN 978-80-247-2615-1.

SODOMKA, P. a H. KLČOVÁ. Informační systémy v podnikové praxi. 2. aktualizované a rozšířené vydání. Praha: Computer Press, 2010. ISBN 978-80-251-2878-7.

TVRDÍKOVÁ, M. Zavádění a inovace IS ve firmách. Praha: Grada Publishing, 2001. ISBN 80-716--703-6.

UČEŇ, P. Zvyšování výkonnosti firmy na bázi potenciálu zlepšení. Praha: Grada Publishing, 2008. ISBN 978-80-247-2472-0.

VOŘÍŠEK, J. Strategické řízení informačního systému a systémová integrace. Praha: Management Press, 2006. ISBN 978-80-85943-40-9.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17

V Brně dne 28.2.2017

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práce se zabývá hodnocením stavu informační bezpečnosti a jeho využitím jako ukazatele podnikové výkonnosti v energetické společnosti. Kapitola analýza problému a současné situace předkládá poznatky o stavu bezpečnosti informací a etapě zavádění ISMS. Praktická část se zaměřuje na analýzu rizik a hodnocení úrovně zralosti procesů, na jejichž základě jsou navržena bezpečnostní opatření a doporučení. Zároveň jsou navrženy metriky pro posouzení úrovně bezpečnosti informací.

Abstract

Master thesis is concerned with assessing the state of information security and its use as an indicator of corporate performance in energy company. Chapter analysis of the problem and current situation presents findings on the state of information security and implementation stage of ISMS. The practical part is focused on risk analysis and assessment the maturity level of processes, which are submitted as the basis for the proposed security measures and recommendations. There are also designed metrics to measure level of information security.

Klíčová slova

Bezpečnost informací, Systém řízení informační bezpečnosti, ISMS, Kybernetická bezpečnost, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, Podniková výkonnost, Řízení rizik, Metrika, Model zralosti

Key words

Information Security, Information Security Management System, ISMS, Cyber Security, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, Corporate Performance, Risk Management, Measure, Maturity Model

Bibliografická citace

KUBÍK, L. *Informační bezpečnost jako jeden z ukazatelů hodnocení výkonnosti v energetické společnosti*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 113 s. Vedoucí diplomové práce doc. Ing. Petr Sodomka, Ph.D., MBA.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 22. května 2017

.....

Podpis

Poděkování

Chtěl bych poděkovat doc. Ing. Petru Sodomkovi, Ph.D., MBA za odborné vedení diplomové práce a Ing. Petru Sedlákovi za cenné rady při zpracování této práce. Děkuji zaměstnancům energetické společnosti za jejich ochotu, se kterou se podělili o informace a jejich postřehy při řešení dané problematiky.

OBSAH

ÚVOD

Využívání výpočetní techniky proniklo do všech oblastí společnosti a podstatně přispívá ke zlepšování životní úrovně populace po celém světě. Na druhé straně se s technologickým pokrokem zvětšuje prostor pro ilegální aktivity. Neustále přibývá kybernetických útoků a škodlivého softwaru s cílem omezit poskytované služby nebo odcizit citlivé údaje za účelem jejich prodeje či zneužití získaných informací. Největší riziko představuje prostředí internetu, a proto je důležité zvyšovat povědomí o možných hrozbách a základních bezpečnostních principech a tím předejít incidentům způsobených nezodpovědným jednáním uživatelů.

Zpracovávání informací se s rozvojem informačních a komunikačních technologií stává nedílnou a klíčovou součástí činnosti firem napříč všemi odvětvími. Následné využívání získaných znalostí lze považovat nejen za konkurenční výhodu, ale může představovat i efektivní nástroj k dosahování podnikových cílů. Postupně dochází ke značnému růstu objemu uchovávaných dat v informačních systémech, které zpracovávají informace o dodavatelích, odběratelích či uživatelích. Případný únik informací může způsobit ztrátu zákazníků či dobrého jména a v nejhorším případě dokonce zánik společnosti. Průmyslové podniky patřící do kritické infrastruktury musí navíc zabezpečit i fyzickou ochranu prvků a procesů, neboť jejich narušení by mohlo mít za následek závažný dopad na zajištění základních životních potřeb obyvatelstva či na fungování státu.

Odpovídající odezvou na zmíněné hrozby je vybudování a neustálé zlepšování systému bezpečnosti informací. Následné přínosy jeho zavedení lze posuzovat z několika hledisek. Vedle podpory firemních cílů, zlepšení důvěryhodnosti a konkurenceschopnosti může společnost na základě míry rizika určit výši potencionální finanční ztráty a investovat do bezpečnostních opatření ve vysoce rizikových oblastech pro zlepšení stability a spolehlivosti svých aktiv. Úroveň informační bezpečnosti lze použít jako jeden z ukazatelů pro hodnocení výkonnosti společnosti, čímž se zabývá tato diplomová práce.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Diplomová práce se zaměřuje na problematiku hodnocení zavádění systému řízení bezpečnosti informací v energetické společnosti a vytvoření souboru ukazatelů pro určení rozsahu působnosti bezpečnosti informací na výkonnost společnosti.

Hlavním cílem práce je stanovení metodiky pro posouzení účinnosti a monitorování ISMS prostřednictvím přezkoumávání bezpečnostních opatření a ukazatelů výkonnosti, které budou sledovat důležité činitele v oblasti bezpečnosti informací, s jejich následnou implementací ve společnosti.

Dílčím cílem práce je ve vymezeném rozsahu přehodnocení provedení analýzy rizik a sestavení zralostního modelu pro hodnocení úrovně jednotlivých opatření uvedených v normě ISO/IEC 27002. Na základě zjištěných nedostatků bude navržen akční plán ISMS a vytvořen soubor ukazatelů pro stanovení efektivity a efektivnosti zavedeného systému řízení bezpečnosti informací.

Výstupem diplomové práce bude systematický přístup pro sledování výkonnosti ISMS pomocí navrženého souboru ukazatelů, sestaveného zralostního modelu pro posuzování bezpečnostních opatření a stanovení priorit následných kroků rozvoje ISMS.

Teoretická východiska práce objasní pojmy a normy související s bezpečností a zároveň uvedou vybrané metody používané při hodnocení podnikové výkonnosti. Kapitola analýza problému a současné situace předloží poznatky o stavu bezpečnosti informací, etapě zavádění a příležitostech vylepšení současného ISMS ve společnosti. Návrh vlastního řešení se zaměří na vytvoření bezpečnostního reportu, který bude obsahovat výsledná zjištění analýzy rizik, hodnocení úrovně zralosti procesů, akční plán pro ISMS a metriky pro měření výkonnosti v oblasti bezpečnosti informací.

1 TEORETICKÁ VÝCHODISKA PRÁCE

Teoretická část práce obsahuje východiska, na kterých se zakládají tvrzení v analýze současného stavu a jsou použity jako znalostní báze při tvorbě vlastních návrhů řešení. Kapitola vysvětluje pojmy, metody a postupy použité v ostatních částech práce.

1.1 Základní pojmy a názvosloví informační bezpečnosti

Na úvod jsou uvedeny základní pojmy a názvosloví informační bezpečnosti, které jsou důležité pro pochopení zpracovávané problematiky.

Data

Data jsou nositeli zaznamenaných skutečností a vytváří opakovaně interpretovatelnou a formalizovanou podobu informace, jež je vhodná pro komunikaci, vyhodnocování nebo pro potřeby následného zpracování (1).

Aktivum

Aktivum lze definovat jako veškerý hmotný a nehmotný majetek mající pro vlastníka význam vyjádřený cenou a důležitostí, respektive je použita kombinace obou způsobů hodnocení. V obecné rovině může být aktivem proces, děj, událost, jejich synchronizace, a dokonce i přímo samotný subjekt. Základními charakteristikami každého aktiva jsou jeho **hodnota** a **zranitelnost** (2).

Informace

Informace popisuje reálné prostředí, jeho stav a procesy v něm probíhající ve formě údajů, přičemž její rostoucí množství snižuje míru entropie před a po obdržení zprávy. V reálném světě se informace vyskytuje v různých formách, může být vytištěna nebo napsána na papíře, ukládána v elektronické podobě, posílána poštou nebo elektronickou cestou či vyřčena při konverzaci. V oboru informatiky vystupuje v podobě kódovaných dat prostřednictvím fyzikální interpretace v úložném zařízení nebo na přenosovém médiu. Informace pro organizace všech druhů a velikostí představují významné aktivum, čímž vzniká požadavek na jejich přiměřenou ochranu. Informační a komunikační technologie představují důležitý nástroj nejen pro jejich vytváření, zpracování, ukládání a přenos, ale i zabezpečení (1, 3).

Informační systém

Minimálně z důvodu rozmanitosti terminologie neexistuje přesná definice informačního systému, avšak lze jej chápat jako soustavu vzájemně propojených informací a procesů, které s těmito informacemi pracují (1).

Dostupnost

Dostupnost představuje zajištění přístupnosti a použitelnosti informace jen oprávněnému uživateli v požadovaný okamžik (3).

Důvěrnost

Důvěrnost je vlastností zaručující přístup nebo poskytnutí informace výhradně oprávněné osobě, entitě nebo procesu (3).

Integrita

Pojem integrita vymezuje správnost a úplnost informace, kterou není možné modifikovat nebo poškodit při neautorizovaném přístupu (3).

Zranitelnost

Zranitelností se rozumí slabé místo aktiva nebo opatření, které může být zneužito jednou nebo více hrozbami (3).

Hrozba

Hrozba označuje potenciální příčinu nežádoucího incidentu, který vzniká zneužitím zranitelnosti aktiva a může mít za následek poškození systému nebo organizace. Hlavní charakteristikou hrozby je její úroveň, která je obvykle klasifikována na základě schopnosti způsobit škodu, možnosti působení na aktivum nebo zájmu o naplnění hrozby. **Dopad hrozby** vymezuje vznik škody v důsledku působení hrozby (2).

Opatření

Postup, proces, fyzický prostředek, služba či cokoliv, co bylo navrženo a je určeno pro zmírnění nebo úplné vyloučení zranitelnosti, dopadu či působení hrozby se nazývá opatření. Jeho rozsah představuje **úroveň opatření** a dle typu se člení na preventivní, podpůrné, detekční a reaktivní. Míra plnění účelu v reálném procesu se označuje jako **účinnost opatření** (2).

Riziko

Riziko vzniká působením hrozby na aktiva a vyjadřuje míru jejich ohrožení. Představuje odlišný a nežádoucí vývoj od předpokládaného s nebezpečím vzniku škody, poškození, ztráty či zničení. Riziko vytváří stav nejistoty, který se zpravidla vyjadřuje pomocí pravděpodobnosti v rozmezí hodnot 0 a 1. Existence rizika souvisí s neurčitostí výsledku, přičemž v množině variant vývoje se vyskytuje alespoň jedna nežádoucí varianta (2).

Bezpečnostní událost

Bezpečnostní událost určuje identifikovaný stav systému, služby nebo sítě ukazující na možnost porušení bezpečnostní politiky nebo selhání bezpečnostních opatření. Může se jednat i o jinou dříve nenastalou situaci, která je důležitá z pohledu bezpečnosti informací (4).

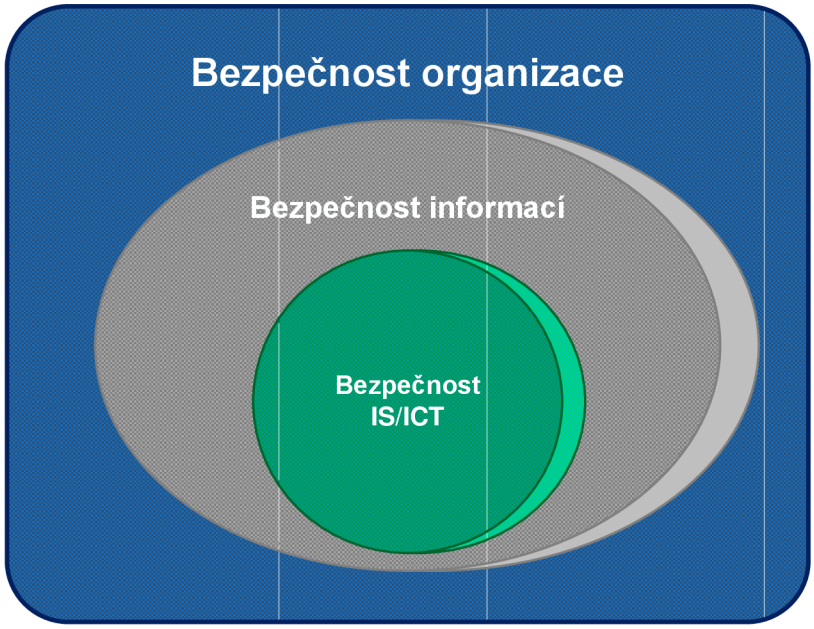
Bezpečnostní incident

Pojem bezpečnostní incident představuje jednu nebo více nežádoucích bezpečnostních událostí, u nichž existuje vysoká pravděpodobnost kompromitace činnosti organizace a ohrožení bezpečnosti informací (4).

Bezpečnost informací

Bezpečnost informací je tvořena třemi hlavními dimenzemi, kterými jsou **důvěrnost**, **dostupnost** a **integrita**. Zahrnuje implementaci a správu bezpečnostních opatření zaměřených na širokou škálu hrozeb a zajišťuje tak zmírňování dopadů bezpečnostních incidentů, kontinuitu činností organizace, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí. Informační bezpečnosti je dosaženo při provádění souboru kontrol vybraných v rámci procesu řízení rizik a spravovaných pomocí ISMS, včetně politik, procesů, postupů, softwaru a hardwaru pro ochranu informačních aktiv (3).

Informační bezpečnost je ve vzájemném vztahu s pojmy bezpečnost organizace a bezpečnost IS/ICT. **Bezpečnost organizace**, jejímž záměrem je ochrana majetku společnosti, je postavena nejvýše a obsahuje bezpečnost IS/ICT a bezpečnost informací. **Bezpečnost informací** obsahuje bezpečnost IS/ICT a práci s informacemi v nedigitální formě. **Bezpečnost IS/ICT** chrání pouze aktiva informačního systému podporovaná informačními a komunikačními technologiemi (1).



Obrázek 1: Vzájemné vztahy bezpečností v organizaci (Upraveno dle: 1)

1.2 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací neboli ISMS (Information Security Management System) je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození. Nejprve jsou určena aktiva, která se mají chránit, poté jsou zvolena a řízena možná rizika bezpečnosti informací a zavedena opatření s požadovanou úrovní záruk a následnou kontrolou. Z důvodu zajištění dostatečné efektivity bezpečnosti informací se musí jednat o řízený proces vyvážený ve všech oblastech, který má podporu vedení a respektuje kulturu organizace. Ekonomické hledisko ISMS vyžaduje dosažení informační bezpečnosti za akceptovatelné náklady (1).

ISMS tvoří část celkového systému řízení organizace, založeného na přístupu k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací. ISMS zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, praktiky, postupy, procesy a zdroje. Rozsah zavedení systému řízení bezpečnosti informací je strategickým rozhodnutím společnosti a může obsahovat organizační složku, informační systém nebo jeho část, případně celou organizaci. Na všechny procesy v ISMS lze aplikovat model PDCA, jehož původním autorem byl Walter A. Shewart. Celý koncept následně ve svých pracích rozpracoval a formuloval W. Edwards Deming (1, 4).

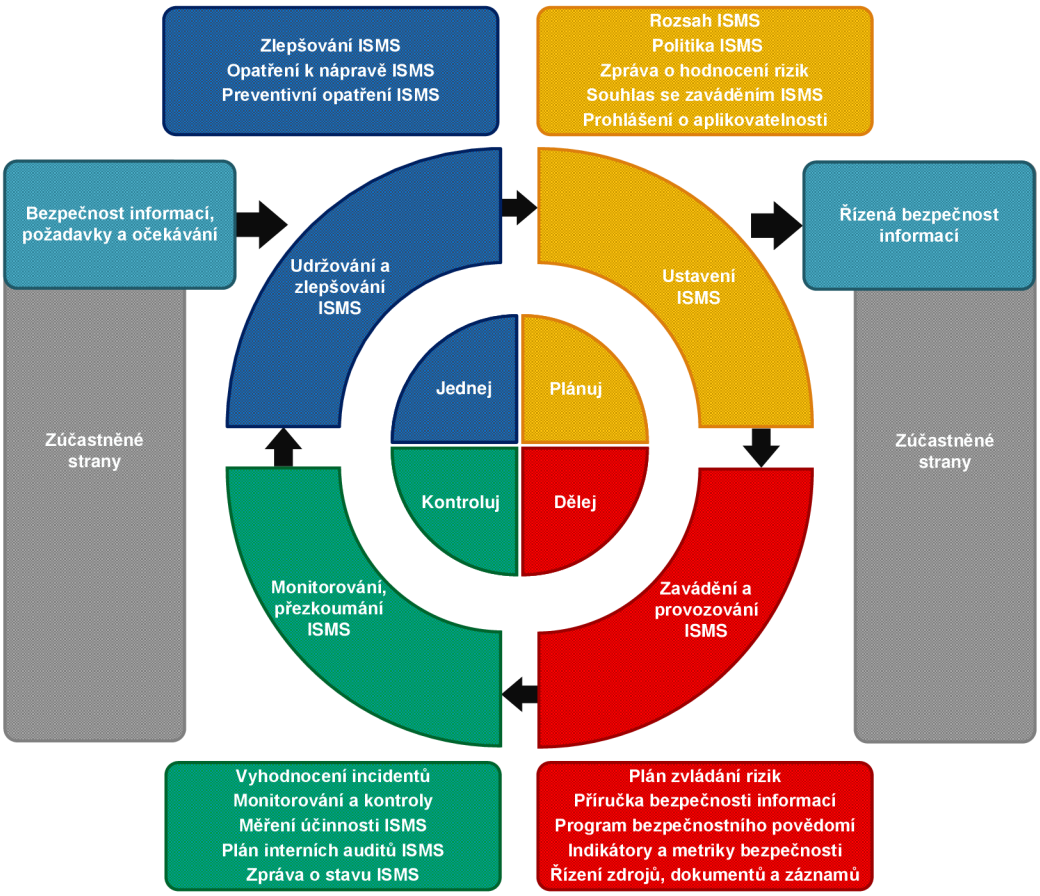
1.2.1 Model PDCA a ISMS

Model PDCA neboli Demingův cyklus představuje iterativní metodu postupného zlepšování formou opakovaného provádění změn ve čtyřech etapách, kterými jsou (1):

- **Plan (plánuj)** – naplánování zamýšleného zlepšení,
- **Do (dělej)** – realizace plánu,
- **Check (kontroluj)** – ověření výsledku realizace oproti původnímu záměru,
- **Act (jednej)** – úpravy záměru a implementace zlepšení do praxe (1).

Systém řízení bezpečnosti informací je založen na využití PDCA cyklu, který bývá označován jako **životní cyklus ISMS**, jehož jednotlivé fáze tvoří (1):

- **Ustavení ISMS** – určení rozsahu a odpovědnosti,
- **Zavádění a provoz ISMS** – prosazení vybraných bezpečnostních opatření,
- **Monitorování a přezkoumání ISMS** – zajištění zpětné vazby a hodnocení řízení,
- **Údržba a zlepšování** – odstraňování slabin a soustavné zlepšování (1).



Obrázek 2: Model PDCA aplikovaný na procesy ISMS (Upraveno dle: 1, 5)

1.2.2 Životní cyklus ISMS

V průběhu životního cyklu ISMS by měla organizace provést následující kroky (3):

- Identifikovat informační aktiva a s nimi spojené bezpečnostní požadavky,
- Posoudit rizika bezpečnosti informací a ošetřit rizika bezpečnosti informací,
- Vybrat a implementovat opatření k zvládnutí neakceptovatelných rizik,
- Monitorovat, udržovat a zvyšovat efektivnost příslušných opatření (3).

Pro zajištění trvalé ochrany informačních aktiv a efektivnosti ISMS je nezbytné opakovaně provádět výše uvedené kroky. Obsah jednotlivých fází životního cyklu ISMS je stanoven normami ISO/IEC 27001 a ISO/IEC 27002 (3).

a) Ustavení ISMS

První etapou budování ISMS je jeho ustavení, při kterém je vymezena forma řešení bezpečnosti informací. Kromě definice rozsahu a odsouhlasení dokumentu **Prohlášení o aplikovatelnosti** patří mezi kritické činnosti provedení analýzy rizik a výběr vhodných bezpečnostních opatření pro snížení vlivu existujících rizik. Ustavení ISMS má zásadní dopady na fungování ISMS během jeho celého životního cyklu, protože definuje základy celého systému řízení bezpečnosti informací a její výsledky se promítají v následujících etapách (5).

Ustavení ISMS je možné rozdělit do následujících skupin činností (5):

- Definice rozsahu, hranic a vazeb ISMS,
- Definice a odsouhlasení Prohlášení o politice ISMS,
- Analýza a zvládání rizik,
- Příprava Prohlášení o aplikovatelnosti (5).

Budování systému informační bezpečnosti je zahájeno vymezením kontextu organizace a určením hranice ISMS. Při stanovení rozsahu se zvažují **externí** a **interní aspekty**, které jsou významné pro záměry organizace a mají vliv na dosažení zamýšleného výstupu systému řízení informační bezpečnosti. Zároveň je nezbytné porozumět potřebám a očekáváním zainteresovaných stran, jejichž požadavky mohou zahrnovat zákonné, předpisové a smluvní povinnosti. **Rozsah ISMS** musí být dostupný jako dokumentovaná informace (4).

Vrcholové vedení je povinno s ohledem na systém řízení informační bezpečnosti demonstrovat vůdčí roli tím, že stanoví politiku a cíle bezpečnosti informací v souladu se strategickým směřováním organizace. Současně musí být vyhrazeny potřebné zdroje s přiřazením odpovědností a pravomocí pro zajištění shody s normami a podávání zpráv o výkonnosti ISMS vedení společnosti. Zaměstnanci by měly být informováni o politice bezpečnosti informací a důsledcích při nepřizpůsobení se jejím požadavkům (4).

Klíčovou součástí etapy ustavení ISMS je proces řízení rizik. Míra schopnosti organizace vyhovět potřebám ISMS je dána riziky s nimiž je možné pracovat následujícími způsoby. Riziku se lze vyhnout, čímž se mění potřeby ISMS snížením dopadů dané hrozby či pravděpodobnosti jejich výskytu. Při přenesení rizika se mění rozsah, protože musí být doplněn subjekt, na který bylo riziko přeneseno. Nejčastější formou zvládání rizika je aplikace vhodného bezpečnostního opatření, což má vliv na snižování zranitelnosti daného informačního aktiva. Poslední možností zvládání je akceptace zbytkových rizik, jež by měly být zaznamenány. Procesem řízení rizik se podrobně zabývá kapitola 1.4 (5).

Poslední kroky plánování vedou k zajištění formálního souhlasu vedení organizace s výběrem opatření a se zbytkovými riziky. Bezpečnostní manažer na tomto základě může zpracovat **prohlášení o aplikovatelnosti** obsahující vybraná opatření a jejich cíle (5).

b) Zavádění a provozování ISMS

Během této etapy zavádění ISMS je nezbytné provést následující aktivity (5):

- Formulovat a zavést dokument **plán zvládání rizik**,
- Zavést bezpečnostní opatření a formulovat **příručku bezpečnosti informací**, upřesňující pravidla a postupy aplikovaných opatření v definovaných oblastech,
- Definovat program **budování bezpečnostního povědomí** a zaškolit uživatele,
- Určit způsob měření účinnosti opatření a sledovat stanovené ukazatele,
- Zavést postup a další opatření pro rychlou reakci na bezpečnostní incidenty,
- Řídit zdroje, dokumentaci a záznamy ISMS (5).

Plán zvládání rizik vymezuje řídicí činnosti, odpovědnosti a priority pro správu rizik bezpečnosti informací. Na základě tohoto dokumentu probíhá další zavádění ISMS v organizaci (5).

Etapa zavádění a provozování ISMS se soustředí na prosazování bezpečnostních opatření, která byla vybrána během ustavení ISMS a jsou uvedena v **příručce bezpečnosti informací** (5).

Měření účinnosti aplikovaných bezpečnostních opatření je součástí všech etap životního cyklu ISMS. K efektivnímu řízení bezpečnosti je potřeba sledovat zvolené ukazatele v pravidelných intervalech. Na základě získaných informací je možné provádět důležitá rozhodnutí (1).

Jedním z nejdůležitějších prvků při prosazování ISMS je **budování bezpečnostního povědomí**, které představuje rozhodující faktor skutečné efektivity celého systému řízení bezpečnosti informací. Všechny vedoucí pracovníky a uživatele organizace je nutné seznámit s bezpečnostními principy, politikami, směrnicemi a provádět pravidelně se opakující školení, protože správně poučený uživatel znamená mnohem menší riziko. Základní návod definující chování uživatele při práci s výpočetní technikou a informačními systémy představuje dokument **minimální bezpečnostní pravidla pro uživatele**, ze kterého by měla logicky vycházet veškerá základní školení (1, 5).

c) Monitorování a přezkoumání ISMS

Hlavním úkolem etapy monitorování a přezkoumání ISMS je zajištění zpětné vazby. V souvislosti s tímto požadavkem dochází k prověření aplikovaných bezpečnostních opatření a jejich důsledků pro systém řízení bezpečnosti informací. Samotné ověření začíná u přímé kontroly odpovědných osob ze strany jejich nadřízených či bezpečnostním manažerem. Důležitou úlohu sehrává nezávislé posouzení fungování a účinnosti ISMS pomocí interních auditů. Obecným cílem všech použitých zpětných vazeb je připravit dostatek podkladů o skutečně dosažené úrovni fungování ISMS, které budou předloženy vedení za účelem následného přezkoumání, zda je realizace ISMS v souladu s obecnými potřebami organizace (5).

Během této etapy životního cyklu ISMS je nutné vykonat následující aktivity (5):

- Monitorovat a ověřit účinnost bezpečnostních opatření,
- Vykonávat interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS,
- Připravit zprávu o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni vedení organizace včetně revize zbytkových a akceptovaných rizik (5).

d) Udržování a zlepšování ISMS

Poslední etapou životního cyklu ISMS je jeho udržování a zlepšování. V této fázi by mělo docházet ke sběru podnětů ke zlepšení ISMS a k nápravě všech nedostatků a nesplněných požadavků neboli **neshod**, které se v ISMS objevují. Veškeré činnosti související s nápravou a preventivní činností musí být zdokumentovány (5).

V průběhu této části zavádění ISMS je potřebné realizovat následující činnosti (5):

- Zavádět identifikované možnosti zlepšení ISMS,
- Provádět opatření k nápravě a preventivní opatření pro odstranění nedostatků (5).

1.2.3 Řada norem ISMS

Před uvedením nejdůležitějších norem zabývajících se problematikou ISMS je vysvětlen rozdíl mezi pojmy standard a norma a jsou představeny některé normalizační instituce zabývající se standardizací bezpečnosti informačních technologií na různých úrovních.

Standard

Standard představuje dokumentovanou úmluvu obsahující technické specifikace nebo přesně stanovená kritéria důsledně používaná jako pravidla. Standard může sloužit jako definice charakteristických vlastností, které zabezpečí požadovanou kvalitu materiálu, výrobku, procesu a služby (1).

Norma

Norma je doporučení pro daný standard k realizaci požadovaného kompatibilního řešení. Zatímco normy jsou velmi často výsledkem těžce dosaženého kompromisu, standardy bývají zdrojem k dynamickému prosazení technické politiky a následného pokroku (1).

ISO

Posláním mezinárodní organizace ISO je podporování rozvoje standardizačních a s tím spojených aktivit zaměřujících se na usnadnění mezinárodních směn zboží a služeb a na spolupráci ve sféře intelektuální, vědecké, technologické a ekonomické (1).

IEC

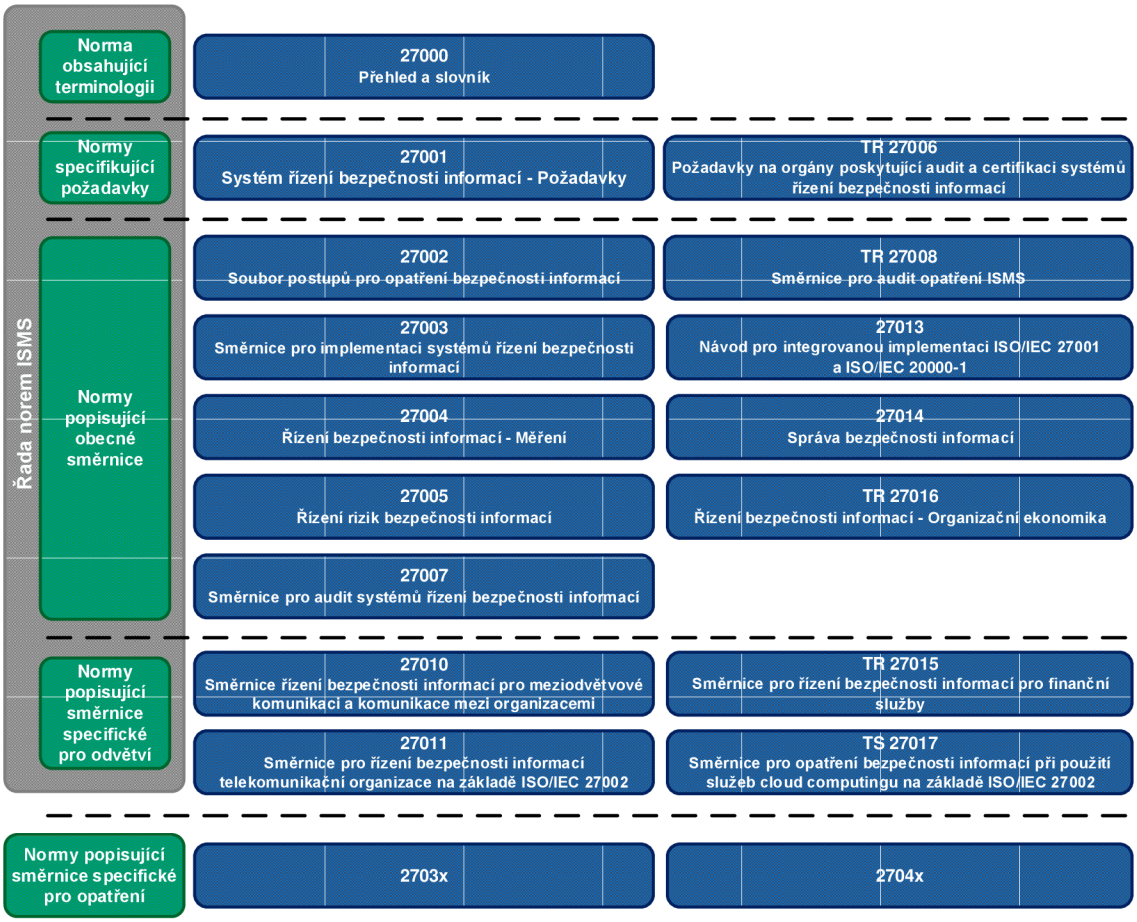
Organizace IEC připravuje a vydává mezinárodní normy z oblasti elektrotechnických, elektronických a jim příbuzných oborech (1).

ČSN

Česká technická norma (ČSN) vzniká dvojím způsobem. Do soustavy českých technických norem jsou přejímány evropské a mezinárodní normy formou ČSN EN nebo jsou vytvořeny původní ČSN vyplývající z národních potřeb a z hledisek zachování funkčnosti fondu ČSN (1).

Řada norem ISMS

Řada norem ISMS obsahuje několik mezinárodních norem, které mají společný název Informační technologie – Bezpečnostní techniky. Skládá se ze vzájemně souvisejících norem, které obsahují významné strukturální komponenty zaměřující se na technické **normy popisující požadavky** na ISMS (ISO/IEC 27001) a na organizace certifikující shodu s ISO/IEC 27001 (ISO/IEC 27006). Další technické normy poskytují návod pro různé stránky implementace ISMS a zabývají se **obecnými směrnicemi ve vztahu k opatření** či **specifickými návody podle odvětví** (3).



Obrázek 3: Vztahy mezi normami řady ISMS (Upraveno dle: 3)

a) Normy obsahující přehled a terminologii

Norma **ISO/IEC 27000** popisuje základní principy systému řízení bezpečnosti informací, podává přehled o řadě norem ISMS a definuje používané termíny a pojmy v ISMS (3).

b) Normy specifikující požadavky

Specifikace nároků na ustavení, provozování, monitorování, přezkoumávání, udržování a zlepšování systémů řízení bezpečnosti informací v kontextu celkových rizik organizace je uvedena v normě **ISO/IEC 27001**. Norma vymezuje požadavek implementace bezpečnostních opatření upravených podle potřeb organizace nebo její části. Jednotlivá opatření a jejich cíle jsou obsaženy v příloze A (3).

Norma **ISO/IEC 27006** poskytuje doporučení pro organizace provádějící audit a certifikaci ISMS. Primárně je určená k podpoře procesu akreditace certifikačních orgánů a doplňuje požadavky obsažené v normách ISO/IEC 17021 a ISO/IEC 27001 (1).

c) Normy popisující obecné směrnice

Seznam obecných opatření a jejich cílů pro doporučené postupy, které lze použít při výběru, implementaci a provádění opatření, definuje norma **ISO/IEC 27002**. Norma je rozčleněna na 14 kapitol obsahujících 35 kategorií bezpečnosti a 114 opatření (3).

Tabulka 1: Přehled kapitol bezpečnosti informací dle ISO/IEC 27002:2013 (Upraveno dle: 4)

Označení	Kapitola	Počet kategorií	Počet opatření
A.5	Politiky bezpečnosti informací	1	2
A.6	Organizace bezpečnosti informací	2	7
A.7	Bezpečnost lidských zdrojů	3	6
A.8	Řízení aktiv	3	10
A.9	Řízení přístupu	4	14
A.10	Kryptografie	1	2
A.11	Fyzická bezpečnost a bezpečnost prostředí	2	15
A.12	Bezpečnost provozu	7	14
A.13	Bezpečnost komunikací	2	7
A.14	Akvizice, vývoj a údržba systému	3	13
A.15	Vztahy s dodavateli	2	5
A.16	Řízení incidentů bezpečnosti informací	1	7
A.17	Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	2	4
A.18	Soulad s požadavky	2	8

ISO/IEC 27003 představuje praktický návod pro implementaci ISMS. Norma rovněž obsahuje informace pro ustavení, provozování, monitorování, přezkoumávání, udržování a zlepšování ISMS podle ISO/IEC 27001 (3).

Doporučení pro používání metrik a měření účinnosti zavedeného ISMS jsou uvedeny v normě **ISO/IEC 27004**. Implementace těchto doporučení je předmětem programu měření bezpečnosti informací, který zahrnuje proces rozvoje metrik, provádění měření, analýzy dat, hlášení výsledků měření a proces vyhodnocení a zlepšování programu měření bezpečnosti informací. V příloze normy jsou uvedeny příklady konceptů měření pro určitá opatření nebo procesy ISMS (1).

ISO/IEC 27005 obsahuje pokyny pro řízení rizik bezpečnosti informací v rámci organizace a podporuje obecný koncept specifikovaný normou ISO/IEC 27001. Struktura normy dostatečně podporuje implementaci informační bezpečnosti založenou na přístupu řízení rizik, ale nenabízí konkrétní metodiku pro řízení rizik bezpečnosti informací a záleží tak jen na zvoleném pojetí řízení rizik organizací (1).

Návod na provádění auditů ISMS podle ISO/IEC 27001 s popisem kompetencí auditorů systému řízení bezpečnosti informací předkládá norma **ISO/IEC 27007** (3).

ISO/IEC 27008 se zaměřuje na přezkoumání opatření bezpečnosti informací včetně kontroly technické shody s normou na implementaci bezpečnosti informací, kterou organizace ustavila (3).

Návod vztahující se k principům a procesům pro správu bezpečnosti informací, pomocí něhož může organizace hodnotit, usměrňovat a monitorovat řízení bezpečnosti informací, poskytuje norma **ISO/IEC 27014** (3).

d) Normy popisující směrnice specifické pro jednotlivá odvětví

Směrnice pro implementaci ISMS ve zdravotnictví má označení **ISO/IEC 27799**. Zdravotnickým organizacím poskytuje úpravu směrnice ISO/IEC 27002 výhradně pro jejich odvětví. **ISO/IEC 27011** se zaměřuje na směrnice podporující zavedení systému řízení bezpečnosti informací v telekomunikačních organizacích (3).

Technická zpráva **ISO/IEC TR 27019** předkládá směrnice vycházející z normy ISO/IEC 27002 pro použití na systémy řízení procesů v energetickém průmyslu. Cílem ISO/IEC TR 27019 je rozšířit soubor norem ISO/IEC 27000 na oblast procesních řídicích systémů a automatizační techniky, což umožňuje v energetickém rozvodném průmyslu implementovat standardizovaný systém řízení informační bezpečnosti se záběrem až na úroveň řízení procesů. Rozsah normy se vztahuje na systémy řízení procesů používané v energetice pro řízení a monitorování výroby, přenosu, skladování a distribuci elektrické energie, plynu a tepla v kombinaci s kontrolou podpůrných procesů. Do působnosti ISO/IEC TR 27019 nespadají energetické systémy řízení technologických procesů v domácnostech a jim srovnatelných obytných budovách, konvenční či klasická ovládací zařízení, která jsou postavena na analogovém nebo elektromechanickém principu (6).

ISO/IEC TR 27019 se vztahuje na následující systémy, aplikace a komponenty (6):

- Informační technologie podporující centrální a distribuované řízení procesů, monitorování a automatizační techniky,
- Číslicové regulátory a automatizační komponenty,
- Všechny další podpůrné systémy používané v oblasti řízení procesů,
- Digitální ochranu a bezpečnostní systémy,
- Distribuované komponenty v prostředí inteligentních sítí,
- Software, firmware a aplikace nainstalované ve výše zmíněných systémech (6).

1.3 Vybrané zákony a evropské směrnice pro bezpečnost informací

Obsahem této kapitoly jsou vybrané zákony a nařízení Evropské unie, které se vztahují k bezpečnosti informací a ovlivňují systém řízení bezpečnosti informací.

1.3.1 Zákon o ochraně osobních údajů

Obecným právním předpisem ochrany osobních údajů je **Zákon č. 101/2000 Sb.**, o ochraně osobních údajů a o změně některých zákonů. Zákon upravuje zpracovávání osobních údajů, ke kterému může docházet automatizovaně nebo jinými prostředky, státními orgány, orgány územní samosprávy, jinými orgány veřejné moci, ale i fyzickými a právnickými osobami. Působnost zákona se nevztahuje na nahodilé shromažďování osobních údajů, jež nejsou dále zpracovávány, ani na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu (7).

Za **osobní údaj** je dle zákona považována jakákoliv informace, jestliže na jejím základě lze subjekt údajů přímo nebo nepřímo identifikovat na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. Zákon rozlišuje osoby, které zpracovávají osobní údaje, na **správce** a **zpracovatele osobních údajů**. Osoby, jejichž osobní údaje se zpracovávají, představují dle zákona **subjekty údajů**. Správcům a zpracovatelům jsou při ochraně osobních údajů ukládány povinnosti, zatímco subjektům údajů jsou dána práva (7).

1.3.2 Směrnice GDPR

Směrnice Evropské unie nazvaná **Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation – GDPR)** již vstoupila v platnost a v roce 2018 bude transponována do českého legislativního prostředí. Nařízení GDPR bude přímo aplikovatelné pro každou organizaci nabízející zboží či služby v rámci členských států Evropské unie a manipulující s osobními údaji subjektů. Ochrana osobních údajů by měla být zahrnuta do všech firemních procesů a systémů. V rámci nové legislativy bude celý dodavatelský řetězec, od výrobce až po dodavatele a zákazníky, zodpovědný za ochranu dat a nebude možné převádět odpovědnost za zabezpečení dat (8).

Nařízení přináší subjektům údajů posílení stávajících práv prostřednictvím výrazně větší kontroly nad vlastními osobními údaji. Ustanovení GDPR poskytne fyzickým osobám snazší přístup k jejich datům, neboť správci a zpracovatelé dat je budou muset důkladněji informovat o způsobu zpracovávání informací, který je dostupný ve srozumitelné podobě. Fyzické osoby budou nově disponovat právem na přenositelnost osobních údajů mezi poskytovateli služeb, právem být informován o zneužití vlastních dat a právem být zapomenut pro vymazání osobních údajů (8).

Obecnou povinností správce osobních údajů je závazek zavést vhodná technická a organizační opatření s cílem splnit požadavky nařízení GDPR při zpracování dat a zaručit ochranu práv subjektů údajů. Další povinnosti správce dle GDPR zahrnují (8):

- Povinnost provádět posouzení dopadu na ochranu osobních údajů,
- Povinnost vést záznamy o zpracováních osobních údajů,
- Povinnost ohlašovat případy narušení bezpečnosti osobních údajů,
- Povinnost jmenovat inspektora ochrany údajů (8).

1.3.3 Zákon o kybernetické bezpečnosti

Kybernetický zákon z části vychází z procesních požadavků normy ISO/IEC 27000 a zaměřuje se na zvýšení bezpečnosti kritické infrastruktury. Dohled nad kybernetickou bezpečností provádí Národní bezpečnostní úřad. Národní centrum kybernetické bezpečnosti působí jako prvotní zdroj bezpečnostních informací. Prvky kritické infrastruktury jsou určovány na základě průřezových a odvětvových kritérií (9).

Kybernetickou bezpečnost upravují následující zákonné pilíře (9):

- **Zákon č. 181/2014 Sb.**, o kybernetické bezpečnosti,
- **Vyhláška č. 316/2014 Sb.** o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti,
- Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvků kritické infrastruktury ve znění **novely č. 315/2014 Sb.,**
- **Vyhláška č. 317/2014 Sb.** o významných informačních systémech a jejich určujících kritériích (9).

Povinnosti vyplývající ze zákona o kybernetické bezpečnosti jsou technické a organizační povahy. Mezi organizační opatření patří především zavedení systému řízení bezpečnosti informací, zřízení bezpečnostních rolí v organizaci, řízení rizik, zvládání a hlášení bezpečnostních incidentů. Součástí technických opatření je například fyzické zabezpečení, ochrana komunikační sítě, ověřování identity uživatelů a ochrana před škodlivými kódy. Prvky kritické infrastruktury musí být pod nepřetržitým dohledem a jejich provozovatel je povinen nasadit nástroje pro detekci, sběr a vyhodnocení kybernetických bezpečnostních událostí (9, 10).

Subjekty s uloženými povinnostmi v oblasti kybernetické bezpečnosti jsou (10):

- Poskytovatelé služeb elektronických komunikací a subjekty zajišťující síť elektronických komunikací,
- Orgány nebo osoby zajišťující významnou síť,
- Správci komunikačního systému kritické informační infrastruktury,
- Správci informačního systému kritické informační infrastruktury,
- Správci významného informačního systému (10).

Zákon o kybernetické bezpečnosti vymezuje **kritickou informační infrastrukturu** jako prvek nebo systém prvků kritické infrastruktury v odvětví komunikačních a informačních systémů ve znění krizového zákona v oblasti kybernetické bezpečnosti. **Významným informačním systémem** je informační systém spravovaný orgánem veřejné moci, u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. Významný informační systém není kritickou informační infrastrukturou. **Významnou sítí** se dle zákona o kybernetické bezpečnosti rozumí síť elektronických komunikací dle zákona o elektronických komunikacích zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo poskytující připojení ke kritické informační infrastruktuře (10).

Kybernetická bezpečnostní událost představuje dle zákona o kybernetické bezpečnosti událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. **Kybernetický bezpečnostní incident** je narušení bezpečnosti informací v kritické infrastruktuře v důsledku kybernetické bezpečnostní události (10).

1.3.4 Směrnice NIS

Na půdě Evropské unie vznikla **směrnice NIS (Network Information Security)** jako ucelený dokument, jehož cílem je zajistit vysokou míru bezpečnosti sítí a informačních systémů napříč všemi členskými státy. Směrnice NIS byla publikována a vstoupila v platnost v srpnu 2016, přičemž členské státy mají povinnost implementovat směrnici do svých národních legislativ v průběhu 21 měsíců. Účelem směrnice NIS je harmonizace opatření pro kybernetickou bezpečnost v rámci Evropské unie (11).

Jedna část povinností vyplývajících ze směrnice má organizační a legislativní charakter, druhá část se vztahuje na okruhy povinných subjektů, které směrnice definuje. Mezi povinnosti organizačního a legislativního charakteru patří (11):

- Povinnost každého členského státu mít národní strategii pro bezpečnost sítí a informačních systémů obsahující strategické cíle a konkrétní opatření,
- Zřízení centrálního orgánu na řízení kybernetické bezpečnosti,
- Povinnost zřídit CSIRT týmy, které se v českém překladu směrnice nazývají Skupinami pro reakci na incidenty v oblasti počítačové bezpečnosti (11).

Směrnice NIS definuje dvě skupiny povinných subjektů, kterými jsou provozovatelé základních služeb a provozovatelé elektronických služeb. Skupina **provozovatelů základních služeb** bude tvořena organizacemi, jež spadají do odvětví jako energetika, doprava, bankovnictví, digitální infrastruktura, zdravotnictví, dodávky a rozvody pitné vody. Do digitální infrastruktury jsou zařazeny výměnné internetové uzly, poskytovatelé služeb systému doménových jmen a rejstříky internetových domén nejvyšší úrovně. Za identifikaci subjektů základních služeb bude odpovědný stát. **Národní bezpečnostní úřad** bude dle směrnice NIS centrálním orgánem pro oblast kybernetické bezpečnosti. Národní bezpečnostní úřad bude zároveň nadále provozovat vládní bezpečnostní tým a působit jako kontaktní místo pro hlášení incidentů od subjektů základních služeb (11).

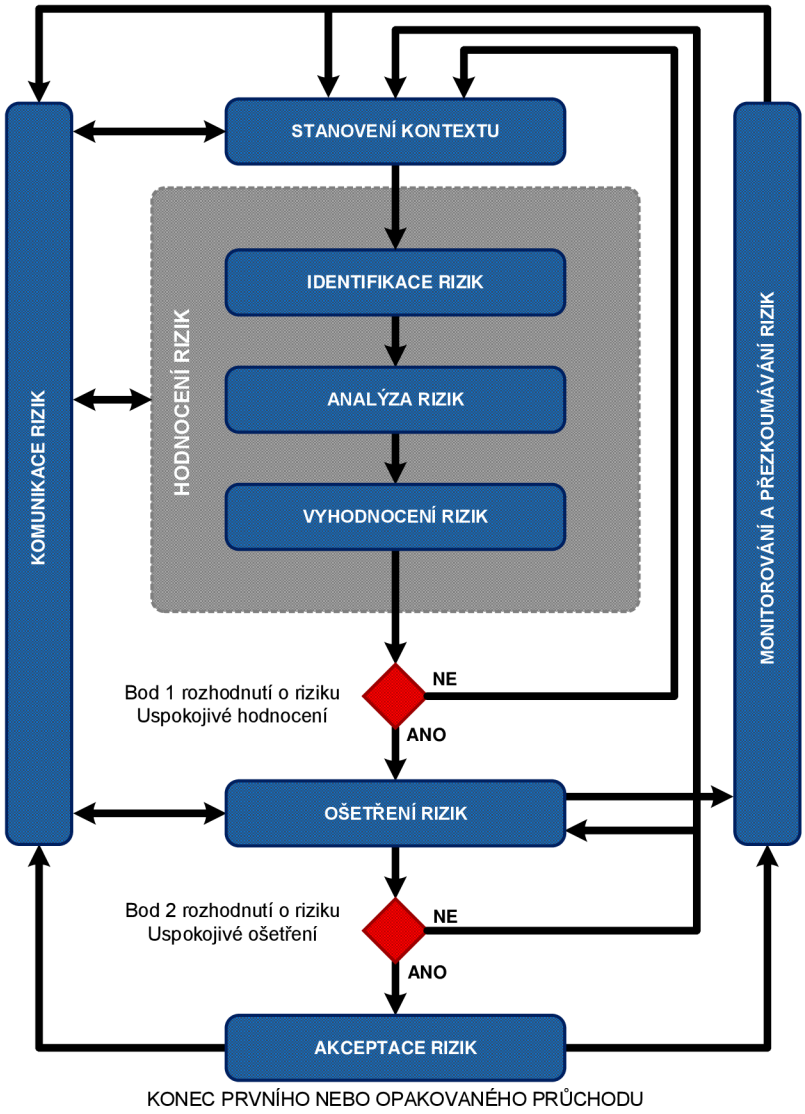
Mezi **provozovatele elektronických služeb** patří online tržiště, poskytovatelé Cloud Computingu a internetové vyhledávače. Z povinných subjektů jsou však automaticky vyřazeny mikropodniky a malé podniky. Subjekty elektronických služeb budou spadat pod působnost národního CSIRT týmu, který je provozován sdružením CZ.NIC. Kontrolu plnění požadavků povinných subjektů bude vykonávat Národní bezpečnostní úřad (11).

1.4 Proces řízení rizik bezpečnosti informací

K identifikaci potřeb organizace vyplývajících z řízení rizik a vytvoření účinného systému řízení bezpečnosti informací je nutný **systematický přístup k řízení rizik bezpečnosti informací**, který tvoří nedílnou součást činností řízení bezpečnosti všech informací a je používán k zavedení i pro další provozování ISMS. Řízení rizik významně ovlivňuje efektivitu fungování celého ISMS a představuje základ každého systému řízení bezpečnosti informací. Proces řízení rizik bezpečnosti informací lze použít pro organizaci jako celek, jakoukoliv samostatnou část organizace, jakýkoliv informační systém nebo plánované aspekty opatření (12).

Norma ISO/IEC 27001 specifikuje nutnost založit přijatá opatření v rámci systému řízení informační bezpečnosti na riziku a použitím procesu řízení rizik bezpečnosti informací lze tento požadavek splnit. Během celého procesu řízení rizik je důležité **zapojení zainteresovaných stran a jejich informování** o identifikovaných rizicích a charakteru přijatých opatření ke zmírnění rizika. Podrobné výsledky každé činnosti procesu řízení rizik bezpečnosti informací by měly být zdokumentovány (12).

Norma ISO/IEC 27005 aplikuje proces řízení rizik bezpečnosti informací, jenž zahrnuje stanovení kontextu, posouzení rizik, ošetření rizik, akceptace rizik, monitorování a přezkoumávání rizik. Jedná se o **cyklický proces**, v němž je na začátku **stanoven kontext** pro realizaci posouzení rizik. Po etapě **hodnocení rizik** a shromáždění dostatku informací k efektivnímu určení akcí, které jsou nutné pro modifikaci rizik na přijatelnou úroveň, následuje **ošetření rizik**. Jestliže jsou získané informace nedostatečné, provádí se opakování hodnocení rizik s revidovaným kontextem. Činnosti **akceptace rizik** musí zajistit, aby vedoucí pracovníci organizace explicitně přijali zbytková rizika zejména v situaci, kdy zavedení opatření bylo odloženo nebo opomenuto. Na následujícím obrázku je zobrazen proces řízení rizik vymezený normou ISO/IEC 27005 (12).



Obrázek 4: Proces řízení rizik bezpečnosti informací dle ISO/IEC 27005 (Upraveno dle: 12)

Řízení rizik informační bezpečnosti je propojeno s procesy systému řízení informační bezpečnosti. Následující tabulka shrnuje činnosti řízení rizik bezpečnosti informací a jejich vztah čtyřem fázím procesu ISMS (12).

Tabulka 2: Propojení ISMS a procesu řízení rizik bezpečnosti informací (Upraveno dle: 12)

Proces ISMS	Proces řízení rizik bezpečnosti informací
Plánuj	Stanovení kontextu Posouzení rizik Příprava plánu ošetření rizik Akceptace rizik
Dělej	Implementace plánu ošetření rizik
Kontroluj	Kontinuální monitorování a přezkoumání rizik
Jednej	Udržování a zlepšování procesu řízení rizik informační bezpečnosti

1.4.1 Stanovení kontextu

Organizace by měla stanovit kontext pro řízení rizik bezpečnosti informací, který zahrnuje určení kritérií pro řízení rizik bezpečnosti informací, definuje rozsah a hranice a stanoví příslušnou organizační strukturu pro řízení rizik bezpečnosti informací. Nejdůležitějším aspektem je určit **účel řízení rizik bezpečnosti informací**, jímž může být podpora ISMS, právní shoda a důkaz povinné péče, příprava plánu kontinuity činností organizace, příprava plánu reakce na incidenty, popis požadavků na bezpečnost informací u produktu, služby nebo bezpečnostního mechanismu (12).

1.4.2 Posouzení rizik bezpečnosti informací

Posouzení rizik kvantifikuje nebo kvalitativně popisuje riziko a umožňuje určit prioritu rizik podle jejich vnímané důležitosti nebo jiných stanovených kritérií. Posouzení rizik stanovuje hodnotu informačních aktiv, identifikuje možné a existující hrozby a zranitelnosti, určuje stávající opatření a jejich účinek na riziko, determinuje potencionální dopady a ustanovuje prioritu určených rizik. Postup posouzení rizik tvoří (12):

- Identifikace rizik,
- Analýza rizik,
- Hodnocení rizik (12).

V následujících odstavcích je uveden postup posouzení rizik bezpečnosti informací.

a) Identifikace rizik

Účelem identifikace rizik je určit příčiny vzniku potencionální ztráty a porozumět všem okolnostem, při nichž může dojít ke ztrátě. V následujících odstavcích jsou popsány kroky ke shromáždění vstupních dat pro činnost posouzení rizik (12).

Identifikace a hodnocení aktiv

Aktivum představuje veškerý hmotný a nehmotný majetek, jenž má pro organizaci hodnotu a vyžaduje ochranu. Pro ohodnocení aktiv je nezbytné nejprve identifikovat aktiva. Identifikace aktiv se provádí na vhodném stupni podrobnosti, který poskytuje pro posouzení rizik dostatek informací. Stupeň podrobnosti lze zpřesnit v dalším opakování posouzení rizik. V této etapě se doporučuje **seskupit všechna aktiva, která k sobě logicky patří**. Seznam identifikovaných aktiv musí obsahovat **vlastníka aktiva**, kterým se rozumí pověřená osoba odpovědná za jeho produkci, vývoj, údržbu, používání a bezpečnost. Vlastník aktiva je nejvhodnější osobou pro následné **určení hodnoty** aktiva pro organizaci (1, 12).

Po vytvoření seznamu aktiv je potřeba k **ohodnocení aktiv** stanovit stupnici a hodnotící kritéria. Stupnice může být vyjádřena finančními částkami či kvalitativními hodnotami a obě varianty lze kombinovat. Peněžní stupnice vyjadřuje v místní měně hodnotu určitého aktiva, zatímco kvalitativní stupnice reprezentuje hodnotu pomocí termínů například od velmi nízká až po kritická. Důležité je vhodné barevné odlišení k jednodušší orientaci v rozsáhlých tabulkách s hodnocením aktiv. Rozsah a výběr termínů si může organizace zvolit v závislosti na bezpečnostních potřebách nebo své velikosti. Příklad tabulky s termíny pro kvalitativní hodnocení v případě napadení aktiva je uveden v následující tabulce (1).

Tabulka 3: Příklad tabulky s termíny pro kvalitativní hodnocení aktiv (Upraveno dle: 1)

Hodnota	Hodnocení dopadu
1	Žádný dopad na organizaci
2	Zanedbatelný dopad na organizaci
3	Potíže nebo finanční ztráty
4	Vážné potíže či podstatné finanční ztráty
5	Existenční potíže

Hlavním principem při ohodnocení aktiv jsou náklady vzniklé v důsledku porušení důvěrnosti, integrity a dostupnosti. Pro **výpočet hodnoty aktiva** je možné použít různé postupy, avšak nejjednodušším a nejpoužívanějším způsobem určení hodnoty aktiva je tzv. **součtový algoritmus**, jenž je stanoven vzorcem (1):

$$\frac{Dostupnost + Důvěrnost + Integrita}{3}$$

Identifikace a posouzení hrozeb

Hrozba má potencionální schopnost poškodit aktiva jako jsou informace, procesy a systémy, a tím i samotnou organizaci. Dle původu lze hrozby rozdělit na **přírodní** nebo způsobené **lidským faktorem**. Podle úmyslu se hrozby rozlišují na **náhodné** a **úmyslné**. Z hlediska bezpečnosti je žádoucí, aby náhodné a úmyslné hrozby byly identifikovány společně s odhadem jejich úrovně a pravděpodobnosti. Hrozby by se měly identifikovat podle typu či v případě potřeby určit jednotlivé hrozby v rámci obecné třídy. V praxi je doporučeno seskupení hrozeb podle aktiv, na něž působí (12).

Posouzení hrozeb se provádí z pohledu možného narušení autentičnosti, dostupnosti, důvěrnosti, integrity, individuální odpovědnosti a spolehlivosti aktiv. Při posuzování se nesmí zapomenout na tzv. **následné efekty hrozby** a vždy je potřeba promyslet možné dopady hrozeb do nejmenších podrobností. Například výpadek elektrické energie neznamená jen nedostupnost dat, ale může vést při dlouhodobém výpadku k ohrožení činnosti organizace, případně i ohrožení fyzické integrity člověka (1).

Identifikace stávajících opatření bezpečnosti opatření

Identifikace stávajících opatření se provádí z důvodu předcházení zbytečné práci nebo nákladům, například při duplikaci opatření. Norma ISO/IEC 27005 rovněž doporučuje provedení kontroly správné funkčnosti opatření. Pokud opatření nefunguje podle předpokladů, může způsobit zranitelnost aktiva, a proto je vhodné učinit rozhodnutí o ponechání, odstranění nebo nahrazení příslušného opatření. Mezi činnosti, které mohou pomoci identifikovat stávající opatření, patří přezkoumání dokumentů s informacemi o opatřeních, provedení kontrol s odpovědnými pracovníky a fyzické přezkoumání (12).

b) Analýza rizik

Analýza rizik se provádí v různých stupních podrobnosti v závislosti na kritičnosti aktiv, rozsahu známé zranitelnosti a předchozích incidentech zasahujících organizaci za účelem identifikace zranitelných míst a působících hrozeb. Cílem analýzy rizik je **snížení velikosti rizika** na přijatelnou úroveň, respektive **přijetí zbytkových rizik**, u nichž je minimalizace rizik neefektivní. Forma analýzy rizik by měla být v souladu s vytvořenými kritérii hodnocení rizik jako součást stanovení kontextu (1, 12).

Metodiky analýzy rizik

Analýza rizik může být kvalitativní nebo kvantitativní, ale v závislosti na okolnostech je možné použít kombinaci obou metodik. Kvalitativní analýza je obvykle méně složitá a nákladná než kvantitativní analýza. V praxi se často používá nejprve kvalitativní analýza k získání obecné indikace úrovně rizika a k odhalení větších rizik, přičemž později může být nutné provést více konkrétní nebo kvantitativní analýzu k upřesnění rizik (12).

Kvalitativní analýza rizik používá k popisu velikosti následků a pravděpodobnosti **škálu kvalifikačních atributů**, kterou lze přizpůsobit podle okolností a pro různá rizika lze použít různé popisy. Výhodou kvalitativní metody rizik je snadné použití a její nevýhodou je závislost na subjektivním výběru škály. Kvalitativní analýza rizik může být použita v případě, kdy jsou zdroje číselných údajů nevhodné nebo při počátečním určení rizik, které vyžadují podrobnější analýzu (12).

Kvantitativní analýza rizik používá pro velikost následků a pravděpodobnosti **stupnici s číselnými hodnotami**. Kvalita analýzy závisí na přesnosti a úplnosti číselných hodnot a platnosti použitých modelů. Při kvantitativní analýze rizik lze vycházet z historických dat incidentů a její výhodou je souvislost s cíli bezpečnosti informací a zájmy organizace. Nevýhodou kvantitativního přístupu je nedostatek dat u nových rizik a o slabých místech v bezpečnosti nebo nedostupnost konkrétních a kontrolovaných dat, což vytváří mylný dojem o významu a přesnosti posouzení rizik (12).

Způsob vyjádření následků a pravděpodobnosti poskytující úroveň rizika, se bude měnit podle typu a účelu, pro který má být výstup posouzení rizik použit. V analýze by měla být zohledněna a účinně sdělena nejistota a nestálost následků a pravděpodobnosti (12).

Metody pro výpočet míry rizika

Míru rizika je možné stanovit pomocí **maticové metody analýzy rizik**, která využívá matici aktiv, hrozeb a zranitelností a probíhá ve čtyřech fázích. První krok obsahuje vytvoření **matice zranitelnosti** spojením tabulky hodnocení aktiv s tabulkou hrozeb a zranitelností. V následující fázi je **posouzena zranitelnost aktiv** a získané údaje jsou doplněny do matice. Třetí krok zahrnuje **výpočet míry rizika** pomocí vztahu (1):

$$\boldsymbol{R = T \cdot A \cdot V},$$

kde použité symboly mají následující význam:

R – míra rizika,

T – pravděpodobnost vzniku hrozby,

A – hodnota aktiva,

V – zranitelnost aktiva (1).

Na závěr jsou stanoveny **hranice rizika**. Rozsah a výběr termínů si může organizace zvolit v závislosti na bezpečnostních potřebách nebo její velikosti (1).

Druhým přístupem je **analýza rizik vyhodnocující pravděpodobnost incidentu a jeho dopad**. Tato metoda využívá dva parametry, kterými jsou pravděpodobnost a dopad incidentu a skládá se ze čtyř etap. Prvním krokem je **doplnění existujících opatření** do tabulky hrozeb a zranitelností. Následně je proveden **odhad pravděpodobnosti incidentu**. Na závěr je vypočtena **míra rizika** pomocí vztahu (1):

$$\boldsymbol{R = PI \cdot D},$$

kde použité symboly mají následující význam:

R – míra rizika,

PI – pravděpodobnost incidentu,

D – dopad (1).

c) Hodnocení rizik

Výstupem analýzy rizik je **seznam rizik** s přidělenou prioritou podle kritérií hodnocení rizik v souvislosti se scénáři incidentů, jež k těmto rizikům vedou. K hodnocení rizik by organizace měla porovnat odhadnutá rizika s kritérii hodnocení rizik definovaných během stanovení kontextu (12).

1.4.3 Ošetření rizik bezpečnosti informací

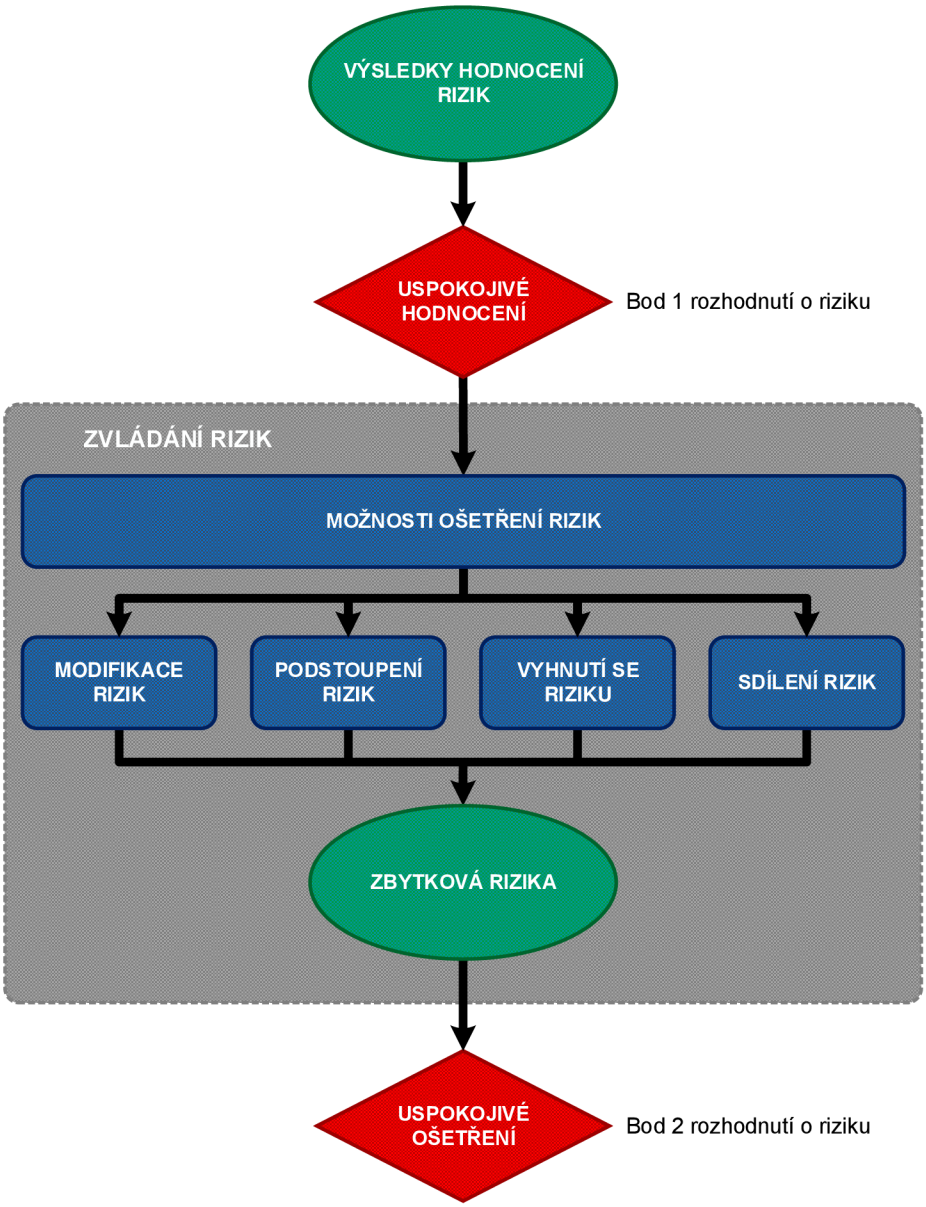
Na základě seznamu rizik a stanovené priority podle kritérií hodnocení rizik jsou s ohledem na kritéria pro akceptaci rizik, legislativní a smluvní požadavky vybrána opatření pro ošetření rizik z důvodu **minimalizace případných rizik**. Primárně by měla být uplatněna možnost zajištění **velkého snížení rizika při poměrně nízkých nákladech**. Další možnosti pro zlepšení mohou být neekonomické, proto je zapotřebí posoudit, zda jsou obhajitelné. Cílem ošetření rizik je snížit nepříznivé následky rizik na nejnižší přiměřeně dosažitelnou míru bez ohledu na jakákoliv absolutní kritéria (12).

Mezi způsoby ošetření rizik patří (12):

- **Modifikace rizika** – úroveň rizika by měla být řízena zavedením, odstraněním nebo změnou opatření, aby bylo zbytkové riziko přehodnoceno na **přijatelné**,
- **Podstoupení rizika** – jestliže úroveň rizik splňuje kritéria **akceptace rizik**, není zapotřebí přijímat další opatření a riziko lze **podstoupit**,
- **Vyhnutí se riziku** – organizace může přijmout rozhodnutí o celkovém vyhnutí se riziku změnou podmínek plánované nebo existující činnosti, pokud jsou identifikovaná rizika považována za příliš **vysoká** nebo **náklady na ošetření rizik převyšují přínosy**,
- **Sdílení rizika** – sdílení rizik zahrnuje rozhodnutí sdílet určitá rizika s externími stranami, přičemž mohou vznikat **nová rizika** nebo se **měnit existující** rizika, a proto může být nutné další ošetření rizik. Odpovědnost za zvládnutí rizika je možné sdílet, ale odpovědnost za dopad obvykle sdílet nelze (12).

Podrobné informace o opatřeních poskytuje norma ISO/IEC 27002. Jednotlivé způsoby ošetření rizik se vybírají na základě výstupu z posouzení rizik, očekávaných nákladů na implementaci a očekávaných přínosů, přičemž se jednotlivé způsoby ošetření rizik vzájemně nevylučují a jejich kombinací lze získat podstatnou výhodu. Některé způsoby ošetření rizik mohou účinně řešit více než jedno riziko (12).

Norma ISO/IEC doporučuje definovat plán ošetření rizik, který obsahuje identifikaci pořadí priorit, jednotlivé způsoby ošetření rizik a časový harmonogram. Po vytvoření plánu ošetření rizik jsou určena **zbytková rizika** na základě aktualizace nebo opakování posouzení rizik (12).



Obrázek 5: Ošetření rizik dle ISO/IEC 27005 (Upraveno dle: 12)

1.4.4 Akceptace rizik bezpečnosti informací

Plány ošetření rizik popisují způsob ošetření hodnocených rizik, aby splňovala kritéria pro akceptaci rizik. Odpovědní vedoucí pracovníci přezkoumávají a schvalují plány ošetření rizik a výsledná zbytková rizika. **Akceptovaná rizika** a **odpovědnosti** za toto rozhodnutí musí být formálně zaznamenána. V některých případech nemusí úroveň zbytkového rizika vyhovovat kritériím akceptace rizik, protože uplatňovaná kritéria neberou v úvahu převažující okolnosti naznačující nepřiměřenost kritérií akceptace rizik, která by měla být revidována (12).

1.4.5 Komunikace rizik bezpečnosti informací

Důležitá je účinná komunikace a výměna informací o rizicích mezi zainteresovanými stranami, neboť může mít podstatný vliv na rozhodnutí, které je nutné učinit. Efektivní obousměrná komunikace zajišťuje srozumitelnost podkladů, vnímání rizika a přínosů zainteresovanými stranami a zdůvodnění uskutečnění konkrétní akce (12).

1.4.6 Monitorování a přezkoumání rizik bezpečnosti informací

Rizika, faktory ovlivňující pravděpodobnost a následky hrozeb a faktory ovlivňující vhodnost nebo náklady způsobů ošetření rizik se mohou změnit. Z tohoto důvodu je nezbytné zajistit jejich pravidelné **monitorování a přezkoumávání** pro zajištění souladu a přiměřenosti kontextu, výstupu z posouzení a ošetření rizik vzhledem k okolnostem. Zároveň by měl být monitorován, přezkoumáván a zlepšován proces řízení rizik (12).

1.5 Řízení a měření výkonnosti

Řízení výkonnosti lze definovat jako kombinaci řízení, metodik a metrik podporovanou aplikacemi, nástroji a infrastrukturou, která umožňuje uživatelům definovat, monitorovat a optimalizovat výsledky a výstupy k dosažení strategických cílů stanovených organizací na různých úrovních řízení. Řízení výkonosti se aplikuje na všech úrovních řízení společnosti. Stanovené celopodnikové cíle a metriky musí být zapracovány do systémů řízení výkonnosti na detailnějších úrovních řízení (13).

S výkonností souvisí pojmy efektivita a účinnost. **Efektivita** je vymezena jako účinnost prostředků vložených do nějaké činnosti hodnocené z hlediska užitečného výsledku této činnosti. **Účinnost** představuje porovnání skutečně dosažených výsledků s tím, co by mohlo být vytvořeno se stejným rozsahem využití zdrojů. Hlavním zástupcem systémů řízení výkonnosti je **Corporate Performance Management (CPM)**, který reprezentují následující segmenty (13):

- Komplex manažerských metod,
- Podnikové procesy,
- Metriky,
- Systémy potřebné k měření a řízení výkonnosti organizace (13).

Manažerské metody tvoří metodologický a logický základ řízení společnosti a jejich principy jsou respektovány i v ostatních segmentech. Mezi manažerské metody patří například Balanced Scorecard (BSC), Six Sigma, Activity Based Costing (ABC) a Value Based Management (VBM). Na manažerské metody navazují plánovací, analytické a monitorovací **podnikové procesy**, které vytvářejí ve svém komplexu procedurální logiku podnikového řízení. Podstatnou charakteristikou **metrik** je jejich přiřazení k podnikovým procesům a vazba na specifikované manažerské metody. Metriky se v rámci CPM člení na následující skupiny (13):

- **Klíčové indikátory výsledků (KRI)** sledující náklady, výnosy a spokojenost zákazníků,
- **Klíčové indikátory výkonnosti (KPI)** hodnotící výkonnost interních procesů lidských a jiných zdrojů,
- **Ostatní indikátory výkonnosti (PI)** vybraných procesů, zdrojů či pracovních týmů (13).

1.5.1 Balanced Scorecard

Metoda **Balanced Scorecard (BSC)** byla vytvořena autory Kaplanem a Nortonem. Balanced Scorecard je pro svoji jednoduchost a strukturovanost značně rozšířeným přístupem při řízení firem. Jedná se o metodu, která převádí misi a vizi do cílů a metrik způsobem, který vyjadřuje kauzální vztahy příčina-důsledek, a tím vystihne jednotlivé oblasti společnosti a všechny oblasti základních předpokladů. (13, 14).

Mezi doporučená hlediska, z nichž se Balanced Scorecard skládá, patří perspektivy **finanční**, **zákaznická**, **procesní** a **učení a růstu**. Každá z perspektiv obsahuje tři součásti, kterými jsou **mise**, **cíle** a **ukazatele**. Strategický Balanced Scorecard se může dále rozpadat na Balanced Scorecard pro jednotlivá oddělení podniku (13).

Základní principy Balanced Scorecard

Finanční perspektiva obsahuje hlavní finanční cíle z pohledu vedení, představenstva a vlastníků organizace. U finančních cílů by měl být proveden provázaný rozpad do ostatních perspektiv BSC. Balanced Scorecard lze použít pro tvorbu finanční strategie a nasazení finančních cílů a ukazatelů pro jejich naplňování (14).

Zákaznická perspektiva definuje, jak lze dosáhnout cílů finanční perspektivy pomocí zákazníků, jejich vnímáním společnosti a naplňováním cílů a vize společnosti. Cíle a metriky zákaznické perspektivy se zaměřují na měření a hodnocení tržních podílů, tržní orientace firmy, nabízených produktů z hlediska vlastností významných pro zákazníka, úrovně vztahu se zákazníkem a image firmy (13).

Procesní a organizační perspektiva představuje infrastrukturu zajišťující propojení zákaznické perspektivy s perspektivou učení a růstu. Proces lze definovat jako posloupnost činností, které slouží k transformaci vstupů do přidané hodnoty výstupů. Proces je spouštěn a ukončen určitou událostí, má stanoveny cíle, metriky těchto cílů, vlastníka a interního či externího zákazníka. Procesní perspektiva se zaměřuje na hodnocení zralosti, efektivnosti, výkonnosti a spolehlivosti procesů (13, 14).

Perspektiva učení a růstu zajišťuje kvalifikační a kapacitní východisko předchozích perspektiv. Zohledňuje připravenost na budoucí změny hodnocení, lidských zdrojů, řízení znalostí a spokojenosti zaměstnanců. Pro perspektivu učení a růstu jsou definovány tři hlavní směry. **Motivace** představuje dynamicky uspořádaný soubor vnitřních faktorů, které ve formě určitých pobídek podněcují a usměrňují pracovní výkony. **Kvalifikace** reprezentuje zvyšování kvality intelektuálního kapitálu. **Kvalitou a funkčností systému řízení** lze dosáhnout efektivní vnitřní komunikace (14).

Pro vyjádření **kauzálních vztahů příčina a důsledek** jsou v návaznosti na finanční cíle stanoveny cíle v zákaznické perspektivě. Firemní procesy jsou nástrojem pro dosahování stanovených cílů ve finanční a zákaznické perspektivě. Zaměření a infrastruktura těchto procesů jsou plně podřízeny cílům v předchozích dvou perspektivách. Firemní procesy a jejich zdroje je tedy nutné nastavit tak, aby bylo dosaženo cílů v perspektivě zákaznické a tím v perspektivě finanční (14).

Proces vytváření hodnoty prostřednictvím řady příčinných vazeb mezi cíli v rámci čtyř perspektiv systému Balanced Scorecard popisuje **mapa strategie**. Mapy strategie a Balanced Scorecard představují mechanismy, které pomáhají vedení společnosti vyladovat větší počet organizačních jednotek v zájmu vytváření hodnoty. Vytvořená mapa celofiremní strategie může být ke koordinaci hodnototvorných činností přenesena na nižší úrovně divizí, podnikatelských a podpůrných jednotek a oddělení (15).

1.5.2 Metriky

Pojem metrika je používán v souvislosti s hodnocením a měřením výkonnosti podniku a lze jej vymezit jako konkrétně specifikovanou metodu měření s definovaným rozsahem. Metrika slouží jako nástroj měření efektivnosti a výkonnosti orientující se zejména na cíle, kritické faktory úspěchu, procesy, aktivity a výkonnost zdrojů a pracovníků (14).

Metrika je definována následujícími atributy (14):

- Název a identifikace,
- Algoritmus nebo vzorec výpočtu tvrdých metrik,
- Definice měkkých metrik,
- Vlastník metriky,
- Dimenze určující měrnou jednotku, organizační jednotku či časové období aj.,
- Výchozí a požadovaná hodnota,
- Zdroj dat pro měření,
- Postup, způsob, periodicita, odpovědnost a vykazování výsledků měření,
- Postup, způsob, periodicita, odpovědnost a vykazování výsledků ověřování správnosti měření (14).

Základní členění metrik

Metriky se dle **objektu měření** dělí na tvrdé a měkké. **Tvrdé metriky** jsou objektivně měřitelné ukazatele, které sledují vývoj podnikových cílů a zaměřují se na výkonnost podnikových procesů, klíčových aktivit nebo přímo na zákazníka. **Měkké metriky** slouží k měření a hodnocení úrovně výkonnosti procesů externím či auditním způsobem. Tvrdými metrikami jsou mimo ukazatelů také **indikátory**, u nichž jsou stanoveny žádoucí meze. Pokud reálná hodnota vykáže odchylku od mezí, jedná se o odchylku od žádoucího stavu. Jestliže metrika není indikátorem, musí mít definován **žádoucí stav** s nímž je poté skutečná hodnota ukazatele srovnána a hodnocena (14).

Metriky lze podle **opakovatelnosti** členit na **kontinuální,** u nichž měření probíhá opakovaně v definované periodicitě, a **diskrétní**, jež jsou aplikovány v časově omezeném rozsahu s nízkým počet počtem opakovaných měření (14).

Metriky v členění pro **hodnocení efektů z inovace IS/ICT** se rozlišují na interní a externí metriky**. Interní metriky** jsou definovány samotným podnikem a jejich prostřednictvím lze identifikovat skutečný efekt inovace IS/ICT, hodnotit efektivnost vynaložených prostředků, podpořit motivační systém pro management a zaměstnance či hodnotit interní úroveň poskytovaných služeb. **Externí metriky** jsou vymezeny uživatelským podnikem a dodavatelem projektu inovace IS/ICT. Jejich smyslem je zainteresovat dodavatele na dosažení přínosů z inovace IS/ICT a vytvořit účinné platformy pro sjednocení cílů týmů dodavatele a odběratelského podniku (14).

Pro základní vlastnosti metrik platí (14):

- Musí být odvozeny ze struktury podnikových cílů, z cílů procesů a zdrojů, které jsou dekomponovány z podnikové strategie,
- Respektují priority určené firemní strategií,
- Je uplatněn vyvážený poměr tvrdých a měkkých metrik,
- Jsou objektivně měřitelné,
- Měření je opakovatelné,
- Zachování konzistence v čase,
- Musí být dostupné a srozumitelné pracovníkům, kteří s nimi pracují
- Metriky jsou objektivně interpretovatelné (14).

1.6 Teoretická východiska metodiky práce

Existuje mnoho norem či osvědčených postupů, které mohou být za určitých podmínek použity k posouzení bezpečnostní situace v organizaci. Normy obsahují ujednání ohledně procesů, ale neposkytují hodnotící kritéria a doporučení pro efektivní řízení a měření bezpečnost informací. Sledování účinnosti bezpečnostních opatření vyžaduje definici integrovaného přístupu pro rozhodování o investicích za účelem určení výše prostředků odpovídající hodnotě aktiv a potencionálním rizikům. Investice do bezpečnosti informací by měly být v souladu s cíli a záměry organizace (16).

Bezpečnostní report pro vedení organizace by měl minimálně obsahovat (16):

- Vysvětlení bezpečnostní strategie a programu,
- Informace o operativní efektivnosti,
- Náklady na bezpečnostní opatření (16).

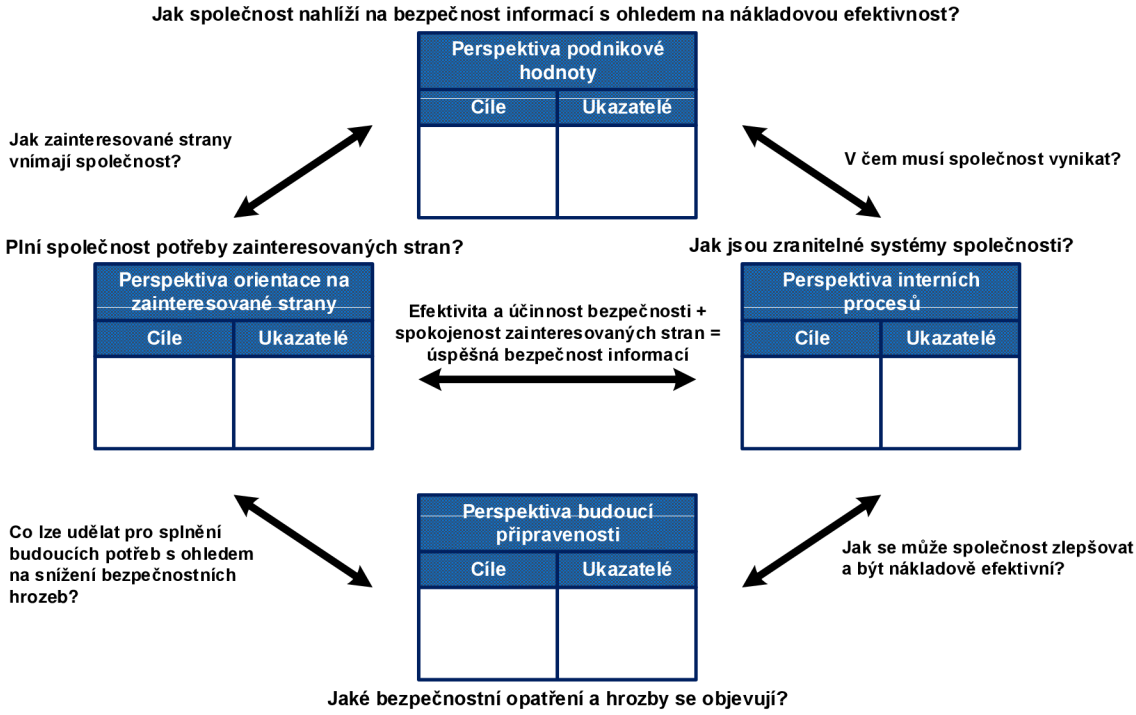
Mezi požadované výstupy při řízení bezpečnosti informací patří (17):

- **Soulad se strategií** – informační bezpečnost by měla být v souladu s podnikovou strategií a tím podporovat dosahování cílů organizace,
- **Řízení rizik** – efektivní řízení a snižování rizik, která implementací nákladově efektivních opatření minimalizují potenciální dopady na přijatelnou úroveň,
- **Řízení zdrojů** – účinné řízení infrastruktury a znalostí o bezpečnosti informací,
- **Měření výkonnosti** – měření, monitorování a podávání zpráv o všech činnostech v oblasti bezpečnosti informací a tím přispívat k naplňování cílů organizace,
- **Poskytování hodnoty** – optimalizace investic do bezpečnosti informací (17).

Hlavním problémem při určování hodnoty bezpečnosti informací je kvantifikace přínosů. Efekty z investice se mohou projevit v dlouhodobém časovém horizontu a stanovení výše ztráty a pravděpodobnosti výskytu incidentu je založeno na odhadu. Přesný způsob výpočtu by vyžadoval statistické informace shromážděné v průběhu několika let s přesnými údaji o incidentech, jejich povaze a očekávané ztrátě. Bezpečnostní strategii je potřeba zaměřit na zmírnění dopadů ve vysoce rizikových oblastech a zlepšení procesů či opatření s nízkou úrovní zralosti. Mezi nástroje, které lze použít k prokázání hodnoty bezpečnostního programu, patří **Balanced Scorecard**, **řízení rizik**, **zralostní model** nebo **diagnostické metody** (16).

1.6.1 Bezpečnostní Balanced Scorecard

Kromě minimalizace a řízení rizik na základě nákladově efektivního a účinného způsobu je doporučeno vytvoření měřitelné bezpečnostní strategie, která je založena na srovnávání a průběžném monitorování výkonnosti. Do budoucna by ke sledování cílů organizace při řízení rizik, řízení zdrojů, poskytování hodnoty a řízení bezpečnosti informací bylo možné použít model bezpečnostního Balanced Scorecard. Sestavení Balanced Scorecard pro bezpečnost informací se provádí na základě informační strategie, jež je odvozena z podnikové strategie. Na následujícím obrázku je uveden navrhovaný Balanced Scorecard pro bezpečnost informací (17).



Obrázek 6: Navrhovaný bezpečnostní Balanced Scorecard (Upraveno dle: 17)

Perspektiva podnikové hodnoty

Bezpečnost informací se vztahuje k ochraně dat před ztrátou, nevhodným zveřejněním nebo poškozením během ukládání, přenosu nebo zpracování. S rozvojem technologií se objevují nové možnosti pro zlepšení podnikové výkonnosti. Přidanou hodnotu lze spatřovat i v bezpečnosti informací a mezi příklady přidané hodnoty bezpečnosti informací patří zlepšení pověsti a důvěryhodnosti organizace, budování užších vztahů se zákazníky, nové a jednoduché způsoby zpracování elektronických transakcí (17).

Perspektiva orientace na zainteresované strany

Bezpečnostní manažeři musí vzít v úvahu potřeby mnoha různých typů uživatelů, ale i zainteresovaných stran. Z pohledu zákazníka musí být dostatečně zajištěny organizační postupy. Chování zaměstnanců je nedílnou součástí bezpečnosti informací. Přijetí a náležité používání bezpečnostních postupů zaměstnanci je ovlivněno jejich vnímáním rizika, prostředím v organizaci, jakož i dostupností zdrojů. Manažeři si musí být vědomi těchto ovlivňujících faktorů, které zlepšují postupy bezpečnosti informací (17).

Perspektiva interních procesů

Interní procesy zahrnují plánování, pořízení, nasazení a údržbu produktů a služeb, správu uživatelských požadavků, nákladově efektivní řízení provozu či pravidelná školení koncových uživatelů. Měření a vyhodnocování interních procesů může být provedeno z pohledu plánování a určení priority bezpečnostních aktivit, nasazení bezpečnostních služeb a produktů, provozu a údržby stávajících bezpečnostních služeb (17).

Perspektiva budoucí připravenosti

Jedním z hledisek perspektivy budoucí připravenosti je pravidelné odborné školení zaměstnanců zabývajících se správou informačních a komunikačních technologií a bezpečností informací na různé typy hrozeb a způsoby, jak se jim účinně vyhnout. Bezpečnostní pracovníci by měli aktivně přemýšlet o budoucích hrozbách, které mohou mít vliv na systémy, a pokusit se navrhnout vhodná opatření (17).

1.6.2 Zralostní model

Proces řízení rizik poskytuje informace o potencionálních hrozbách, ale nepředkládá informace o připravenosti a bezpečnostní situaci v organizaci. Na základě vyhodnocení zralosti procesů a opatření bezpečnosti informací je možné upřednostnit aktivity, které se zaměřují na řešení nedostatků v oblasti bezpečnosti informací. Zralostní model může být založen na řadě norem ISO/IEC 27000, které doporučují použití nejlepších praktik, ale nestanovují žádná kritéria pro posouzení jejich úrovně. Pro efektivní využití standardů v procesu posouzení úrovně zralosti pro bezpečnost informací musí být vytvořena hodnotící kritéria pro každý z bodů zvoleného standardu. Za tímto účelem je možné použít normu ISO/IEC 15504, která definuje standardní kritéria, na jejichž základě se určují hodnotící kritéria pro každé opatření standardu ISO/IEC 27002 (16).

Každý model zralosti pokrývá všechny kapitoly jednoho nebo více standardů či rámců, kterými jsou například ISO 27000, COBIT nebo NIST, případně lze navrhnout vlastní katalog opatření. **Současná úroveň** zralosti pro každou kapitolu normy by měla být posouzena v souladu s kritérii a porovnána s **požadovanou úrovní**. Výslednou hodnotu úrovně zralosti každé části standardu nebo jiného seskupení lze určit pomocí průměrné hodnoty či váženého průměru a získané výsledky posouzení pomocí modelu zralosti je vhodné pro přehlednost a srozumitelnost graficky zobrazit (16).

Rozsah posouzení může být omezen na část organizace, podmnožinu činností organizace či na vybrané domény modelu. Po dokončení hodnocení úrovně zralosti bezpečnosti informací by měly vzniknout akční plány, které jsou v každém novém cyklu hodnocení revidovány společně s přehodnocením bezpečnostních opatření (16).

1.6.3 Model řízení bezpečnosti informací

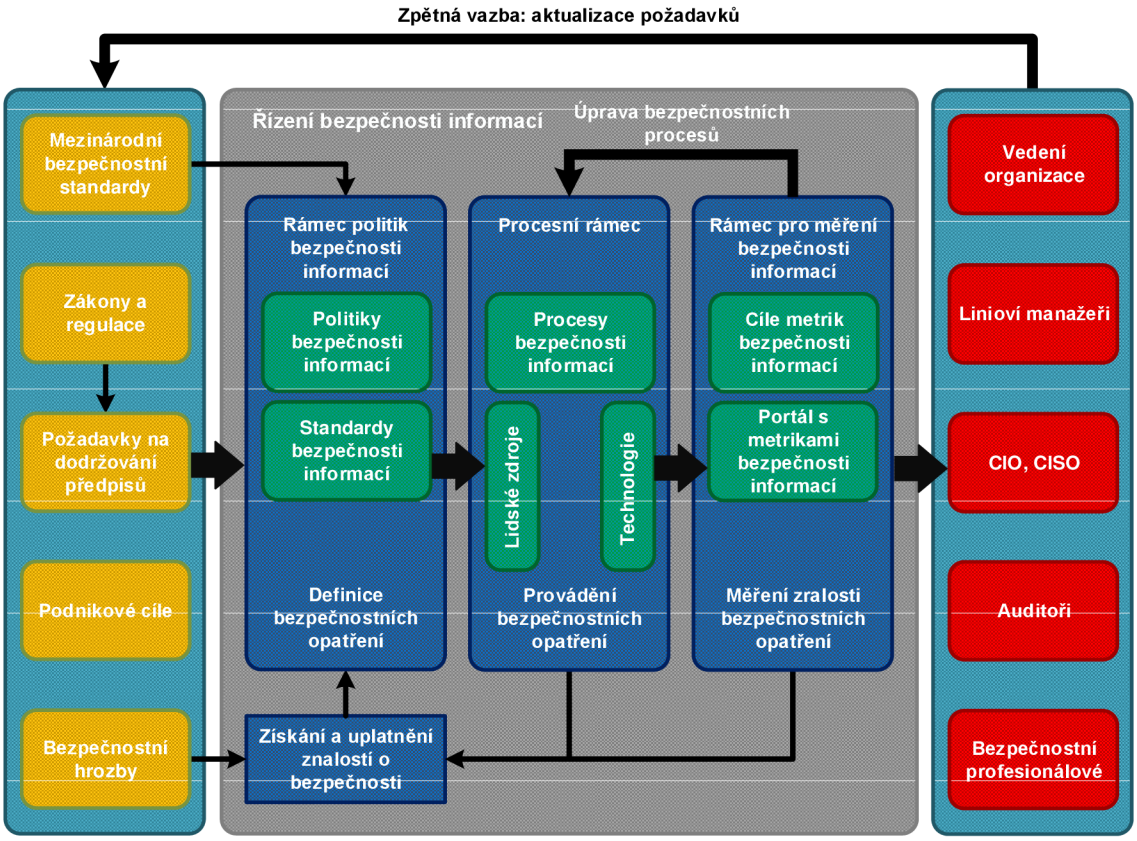
Mezi významné faktory pro zavedení systému řízení bezpečnosti informací patří zákony a regulace, podnikové cíle a bezpečnostní hrozby. Zajištěním souladu s legislativními požadavky předchází organizace žalobám nebo pokutám za nedodržování předpisů. Bezpečnost informací chrání významná aktiva společnosti, čímž se podílí na dosažení podnikových cílů a zisku. Bezpečnostní hrozby pochází z vnějšího a vnitřního prostředí organizace a jejich realizací dochází ke ztrátě informací či omezení obchodních procesů. Pro dosažení podnikových cílů a splnění legislativních požadavků musí společnost reagovat na bezpečnostní hrozby (18).

První část řízení bezpečnosti v modelu představují politiky bezpečnosti informací zahrnující jednotlivé politiky, standardy a příručky s definicí dostupných bezpečnostních opatření, jež je možné implementovat. Při výběru vhodných bezpečnostních opatření lze použít mezinárodní bezpečnostní standardy (18).

K implementaci opatření dochází dle navrhovaného modelu v procesním rámci. Bezpečnostní opatření uvedené v politikách nebo standardech představují proces, který je podporován lidskými a technologickými zdroji. Ke sledování investic do bezpečnosti informací musí mezi technologiemi, procesy, bezpečnostními opatřeními a podnikovými cíli existovat vazba. Každé opatření musí být spojeno s jedním nebo více bezpečnostními cíli a každý proces musí mít svého vlastníka a být zlepšován na základě monitorování a provedeného měření (18).

Organizace by měla být schopna měřit stav bezpečnostních opatření, dodržování bezpečnostních politik a efektivitu bezpečnostních procesů. Rámec definovaných metrik poskytuje zpětnou vazbu a informace ke sledování průběhu bezpečnostních procesů podle plánu. Na základě výsledků měření lze vyhodnotit dosahování stanovených cílů, prokázat hodnotu bezpečnosti informací pro společnost a zainteresované strany (18).

Při určovaní potřeb měření je vhodné do procesu stanovení metrik začlenit požadavky zainteresovaných stran. Propojení podnikatelských a bezpečnostních cílů lze realizovat pomocí analýzy rizik podnikových procesů, na jejímž základě je možné určit směrování bezpečnosti informací. Měření bezpečnosti informací zahrnuje základní provozní metriky pro sledování funkčnosti procesů a zjištění úrovně zralosti bezpečnostních procesů (18).



Obrázek 7: Model řízení informační bezpečnosti (Upraveno dle: 18)

2 ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE

Kapitola se zabývá charakteristikou odvětví a představením energetické společnosti, její podnikové, informační a bezpečnostní strategie, včetně infrastruktury a zejména analýzou současného stavu systému řízení bezpečnosti informací. V závěru je současný stav shrnut a jsou předloženy požadavky na změnu. Součástí je i popis praktického použití metodiky práce a myšlenková mapa řešené problematiky.

2.1 Praktické použití metodiky práce

Rozhodování v oblasti bezpečnosti informací by mělo být založeno na identifikovaných rizicích. V rámci procesu řízení rizik se následně určí adekvátní opatření ke zjištěné míře rizik za přiměřené výše nákladů na zavedení opatření.

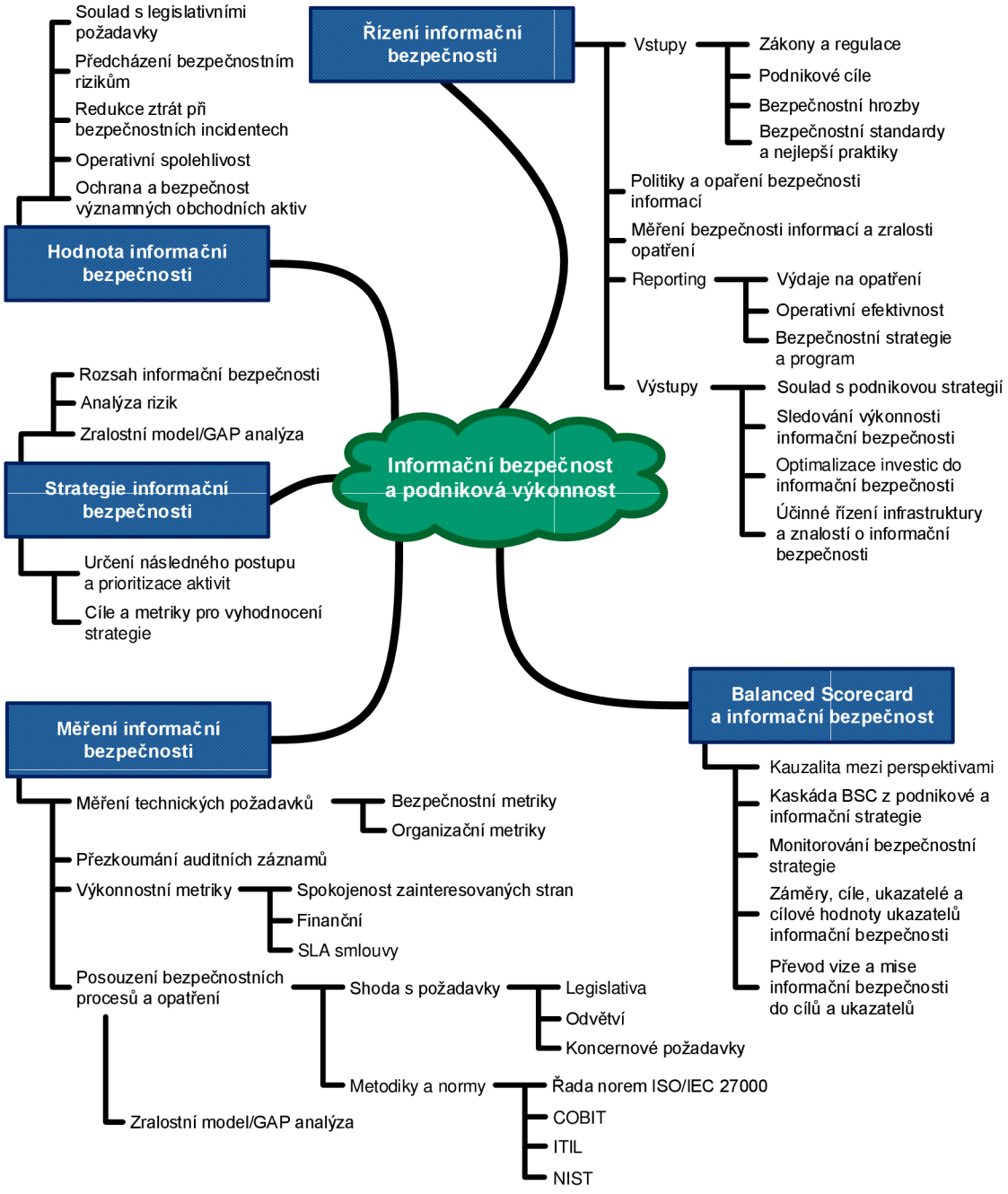
Pro hodnocení míry zdokonalování jednotlivých bezpečnostních procesů a opatření, které je relativně rychlé, objektivní a opakované, je vhodné použít zralostní model. Opatření definovaná normou ISO/IEC 27002 lze využít jako referenční model pro přehodnocení současného stavu ISMS pomocí zralostního modelu. Pro vyjádření způsobilosti procesů je možné aplikovat stupnici z normy ISO/IEC 15504, která pro vymezení zvláštního aspektu způsobilosti stanovuje množinu atributů na definované škále.

Zralostní model je založen na porovnání definovaného cílového stavu se stávajícím a musí být sestaven z množiny indikátorů, které explicitně určují účely a výsledky opatření podle jejich vymezení ve vybraném referenčním modelu. Indikátory nadále prokazují dosažení atributů v rámci rozsahu úrovně způsobilosti. Mapování indikátorů se provádí v atributech a s vyšší vyzrálostí opatření dochází ke zvýšení jeho efektivnosti a systém řízení bezpečnosti informací je možné lépe řídit a plánovat. K odstranění zjištěných nedostatků se navrhují opatření pro dosažení cílové úrovně.

Kromě přehodnocení ISMS pomocí analýzy rizik a zralostního modelu je vhodné stanovit soubor metrik za účelem hodnocení účinnosti ISMS. Na základě výsledků měření se určují procesy či opatření, které vyžadují změnu nebo zlepšení. Při definici metrik lze vycházet z doporučení normy ISO/IEC 27004.

Výsledky analýzy rizik a posouzení stavu ISMS pomocí zralostního modelu a metrik umožňují definovat bezpečnostní strategii, která se zaměřuje na zmírnění dopadů ve vysoce rizikových oblastech a zlepšení procesů či opatření s nízkou úrovní zralosti.

Problematiku působnosti informační bezpečnosti na podnikovou výkonnost zachycuje následující obrázek pomocí myšlenkové mapy.



Obrázek 8: Myšlenková mapa informační bezpečnosti a podnikové výkonnosti (Zpracování vlastní)

2.2 Charakteristika odvětví energetiky

Struktura energetického trhu v České republice je tvořena sektory elektroenergetiky, plynárenství a teplárenství. Obchodními činnostmi se v energetických odvětvích rozumí:

- Výroba, přenos, distribuce a obchod s elektrickou energií,
- Výroba, přeprava, distribuce, uskladňování a obchod s plynem,
- Výroba a rozvod tepelné energie,
- Činnosti operátora trhu.

Následující podkapitoly obsahují charakteristiku odvětví energetiky v České republice se zaměřením na elektroenergetiku, významné zákony a regulaci subjektů na trhu. Uvedené poznatky vychází z energetického zákona.

2.2.1 Organizační struktura v odvětví elektroenergetiky

Účastníky na trhu s elektrickou energií jsou výrobci elektřiny, provozovatel přenosové soustavy, provozovatelé distribučních soustav, operátor trhu, obchodníci s elektřinou a zákazníci.

Podnikat v odvětví energetiky na území České republiky mohou fyzické nebo právnické osoby na základě licence udělené Energetickým regulačním úřadem. Mezi podmínky pro udělení licence fyzické osobě patří dosažení plnoletosti, právní způsobilost, trestní bezúhonnost a odborná způsobilost. Právnické osoby jsou povinny ustanovit odpovědného zástupce a uvedené požadavky na fyzickou osobu musí splňovat členové statutárního orgánu (19).

Operátor trhu

Operátorem trhu je akciová společnost, jejímž zakladatelem a jediným akcionářem je stát Česká republika. Výkon akcionářských práv provádí Ministerstvo průmyslu a obchodu. Předmět činnosti operátora trhu vychází z energetického zákona, přičemž mezi jeho hlavní funkce patří organizování krátkodobého trhu s elektrickou energií a plynem, zprostředkování obchodu s elektrickou energií, vydávání záruk původu elektřiny z obnovitelných zdrojů, evidence výroben elektřiny, zpracování obchodních podmínek operátora trhu pro elektroenergetiku a pro plynárenství či tvorba zpráv o trhu s elektrickou energií a plynem (19).

Výrobce elektřiny

Výrobce elektrické energie musí pro připojení zařízení k elektrizační soustavě splňovat technické požadavky na provozování přenosové nebo distribuční soustavy. Podmínkou pro výrobce elektřiny je získání licence a registrace u operátora trhu, navíc výstavba výrobny elektřiny o celkovém instalovaném minimálním elektrickém výkonu 100 kW je možná pouze na základě udělené státní autorizace (19).

Provozovatel přenosové soustavy

Přenosová soustava je propojena s evropskými elektrizačními soustavami a slouží pro zajištění přenosu elektřiny od výrobce k distributorovi na celém území České republiky. Výhradním provozovatelem přenosové soustavy je společnost ČEPS, a.s. s jediným akcionářem, jímž je stát Česká republika. Práva akcionáře ve společnosti vykonává Ministerstvo průmyslu a obchodu. Provozovatel přenosové soustavy dle energetického zákona musí být z hlediska své společnické struktury nezávislý na výrobě a obchodu s elektřinou a plynem a mít přidělen certifikát nezávislosti (19).

Provozovatelé distribučních soustav

Distribuční soustavu tvoří soubor zařízení pro rozvod elektřiny z přenosové soustavy nebo ze zdrojů do nich zapojených ke koncovým uživatelům. Součástí distribuční soustavy jsou i její řídící, ochranné, zabezpečovací a informační systémy. Provozovatel distribuční soustavy zajišťuje spolehlivé provozování, obnovu a rozvoj distribuční soustavy na území vymezeném licencí. Provozovatel distribuční soustavy s více než 90 000 odběrnými místy nesmí být současně držitelem licence na výrobu elektřiny, přenos elektřiny, obchod s elektřinou či s plynem (19).

Obchodník s elektřinou

Obchodník představuje fyzickou či právnickou osobu, která nakupuje elektřinu za účelem jejího prodeje. Obchodník s elektřinou má právo na poskytnutí přenosu nebo distribuce elektřiny, nakupovat elektřinu od držitelů licence na výrobu či obchod elektrické energie nebo z jiných států a prodávat ji ostatním účastníkům trhu. Obchodník s elektřinou je povinen od energetického regulačního úřadu získat licenci s platností na pět let (19).

Zákazníci

Zákazníkem se rozumí osoba, která nakupuje elektřinu pro své vlastní konečné užití v odběrném místě. Všichni zákazníci přitom mají na energetickém trhu stejná práva a povinnosti, jejichž garantem je Energetický regulační úřad (19).

2.2.2 Legislativa a regulace v odvětví elektroenergetiky

Legislativním základem energetického trhu je **energetický zákon** 458/2000 Sb., Zákon o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů, který je doplněn řadou prováděcích vyhlášek. Mezi nejdůležitější legislativu v odvětví patří:

- Cenová rozhodnutí Energetického regulačního úřadu,
- Prováděcí vyhlášky k energetickému zákonu,
- Vyhlášky Ministerstva průmyslu a obchodu,
- Zákon o hospodaření energií,
- Nařízení vlády,
- Vyhlášky Ministerstva pro místní rozvoj.

Kromě legislativně stanovených práv a povinností jako je ochrana spotřebitele, daňová legislativa aj. je energetické odvětví ovlivňováno cenovou regulací a kontrolami vstupu do odvětví prostřednictvím udělování licencí pro výkon činnosti na základě státního souhlasu. Podstatná je i vazba na ochranu životního prostředí, jejíž součástí jsou nařízení na snížení emisí skleníkových plynů, zvýšení energetické účinnosti a zvýšení podílu obnovitelných zdrojů energie na celkové spotřebě. Hlavními orgány státní správy pro oblast regulace jsou Energetický regulační úřad a Ministerstvo průmyslu a obchodu.

Ministerstvo průmyslu a obchodu

Ministerstvo průmyslu a obchodu v odvětví energetiky vedle vydávání vyhlášek poskytuje státní autorizace na výstavbu výroben elektřiny a plynových zařízení, vypracovává státní energetickou koncepci a Národní akční plán pro energii z obnovitelných zdrojů, zpracovává analýzy zavedení inteligentních měřicích systémů v oblasti elektroenergetiky a plynárenství, zabezpečuje plnění závazků vyplývajících z mezinárodních smluv nebo z členství v mezinárodních organizacích (19).

Energetický regulační úřad

Energetický regulační úřad působí jako správní úřad pro výkon regulace v energetice. Mezi hlavní oblasti působnosti náleží regulace cen, vykonávání dohledu nad trhy v energetických odvětvích, monitorování a vyhodnocování dodržování kvality dodávek a služeb v elektroenergetice a plynárenství, rozhodování o potřebných licencích a certifikátech nezávislosti (19).

Regulace ceny v energetice

Mezi významné položky určující cenu patří platba za distribuci elektřiny distributorovi, platba za odebrané množství a příspěvek na obnovitelné zdroje. Platba za odebrané množství elektřiny a pevná cena za měsíc představují položky z celkové ceny za elektřinu, které jsou stanoveny trhem.

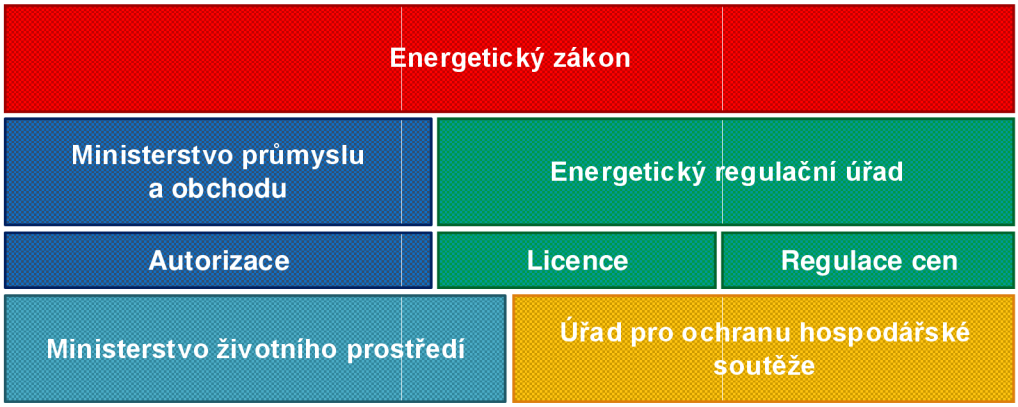
Cena za distribuci se skládá z platby za odebrané množství a pevné platby za přípojné místo, jejíž výše je závislá na velikosti hlavního jističe. Platba za distribuci, poplatek za systémové služby, poplatek operátorovy trhu a příspěvek na obnovitelné zdroje energie podléhají regulaci a jejich výši stanovuje vyhláška Energetického regulačního úřadu.

Oddělení distribučních a přenosových soustav

Provozovatel přenosové soustavy a provozovatel distribuční soustavy, který je součástí vertikálně integrovaného podniku, musí být nezávislý na jiných činnostech, jež se netýkají jeho hlavního předmětu podnikání z hlediska právní formy a rozhodování. V podmínkách České republiky platí povinnost oddělení provozovatelů distribučních soustav pro společnosti, které mají více než 90 000 připojených odběrných míst (19).

Mezi hlavní faktory regulace v odvětví energetiky tedy patří:

- Tvorba cen elektrické energie v rámci distribučního řetězce,
- Vysoké náklady na budování infrastruktury distribuční a přenosové soustavy,
- Ekologické limity na výrobu elektrické energie,
- Výroba elektřiny z obnovitelných zdrojů,
- Majetkové propojení společností,
- Míra a forma zdanění činností.



Obrázek 9: Hlavní subjekty a nástroje regulace v odvětví energetiky (Zpracování vlastní)

2.3 Základní charakteristika společnosti

Energetická společnost (dále jako ES) je součástí mezinárodního energetického koncernu působícího v mnoha zemích Evropy, ale i v Rusku a Severní Americe. Aktivity ES jsou na území České republiky usměrňovány a řízeny holdingovou společností, pod níž náleží skupina právně samostatných subjektů s oddělenými pravomocemi. Organizační uspořádání jasně vymezuje role a odpovědnosti individuálních společností, jejichž spolupráce je založena na základě uzavřených smluv o poskytovaných službách.

Do kompetencí jednotlivých společností patří:

- Realizace strategických rozhodnutí a podpora operativních činností obchodní a distribuční společnosti,
- Obchodování s elektrickou energií a plynem, výroba elektrické a tepelné energie,
- Provoz, rozvoj a údržba elektrické a plynové distribuční soustavy,
- Servisní služby v oblasti distribuce elektřiny a plynu,
- Poskytování IT a telekomunikačních služeb ve skupině.

Hodnotový řetězec

ES působí zejména v sektorech elektroenergetiky a plynárenství. Hodnotový řetězec společnosti zahrnuje výrobu, přenos, velkoobchod, distribuci a prodej elektřiny a plynu zákazníkům. Politická rozhodnutí a regulační instituce ovlivňují problematiku řízení sítí v energetice. Obnovitelné zdroje energie, decentralizovaná produkce a energetická účinnost způsobují rozpad tradičního hodnotového řetězce v energetice do stále většího počtu samostatných segmentů trhu.

Pro odvětví energetiky je charakteristická duální infrastruktura. Kromě infrastruktury pro přenos energie musí být spravována a řízena i informační infrastruktura, která podporuje centrální a distribuované řízení procesů, monitorování a řízení výroby, přenos, skladování a distribuci energie. Transformací energetické soustavy a její digitalizací jsou získávány přesnější informace o výrobě a spotřebě energie v téměř reálném čase. Informační infrastruktura je nedílnou součástí spolehlivosti elektrizační soustavy a hodnotový řetězec obsahuje nejen toky energie, ale i informací.

Obrázek 10: Hodnotový řetězec společnosti (Zpracování vlastní)

2.3.1 Strategie společnosti

Posláním ES v České republice je zajistit spolehlivý provoz, optimalizaci procesů a modernizaci infrastruktury. Aktivity ES jsou na českém trhu směřovány k dosažení vedoucího postavení v oblastech zákaznické orientace a energeticky efektivních řešení. Společnost k uspokojení potřeb zákazníků vyvíjí nové modely dodávky energie a nabízí poradenství, vzdělávání či nabídku finančně výhodných produktů a služeb.

Společnost na českém trhu usiluje o pozici nejvyhledávanějšího partnera pro energetická a zákaznická řešení. Strategie reflektuje základní tržní trendy v energetickém odvětví, mezi které patří decentralizace produkce elektrické energie, vývoj energetických sítí do podoby platformy řešení výroby energie spojené s distribucí, měnící se potřeby zákazníků a globální poptávka po obnovitelných zdrojích energie. ES usiluje o vytvoření přidané hodnoty ve všech těchto podnikatelských činnostech zajištěním vynikající výkonnosti v klíčových oblastech, jež zahrnují neustálé inovace technologií, trvalou udržitelnost řešení, vymezení pozice značky a udržování vztahů se zákazníky, obchodními partnery a ostatními zainteresovanými stranami. Záležitost společenské odpovědnosti je zahrnuta do strategie energetické skupiny v České republice.

Společenská odpovědnost

Společenská odpovědnost tvoří součást podnikatelské činnosti a představuje dobrovolný závazek podniku chovat se ohleduplně k prostředí a společnosti v místě své působnosti, a to ve spolupráci se zainteresovanými stranami. Odpovědné chování pro ES znamená jednat v souladu s neustálým vývojem společenského a přírodního prostředí. Společenská odpovědnost ES je postavena na pěti pilířích, které odráží zaměření aktivit a uplatňování těchto zásad umožňuje ES dosahovat spokojenosti zákazníků, zaměstnávat vzdělané a schopné odborníky a rozvíjet dobré vztahy a spolupráci s místními organizacemi.

Jednotlivé pilíře společenské odpovědnosti ES dodržují následující zásady:

- **Odpovědné vedení společnosti:** platnost přijatého etického kodexu v rámci celého koncernu, využívat výstupy z Risk Managementu pro přímé řízení,
- **Trh:** pozice čestného partnera a zákaznická orientace představují nezbytnou podmínkou úspěchu ES,
- **Životní prostředí:** minimalizace negativních dopadů na životní prostředí,
- **Pracovní místo:** profesionální růst, vzdělávání, zvyšování kvalifikace a kvalitní pracovní podmínky pro zaměstnance,
- **Region**: vystupovat jako významný zaměstnavatel a investor, angažovanost v oblastech rozvoje dětí a mládeže, vzdělávání a ekologie.

Obrázek 11: Pilíře společenské odpovědnosti společnosti (Upraveno dle interních materiálů)

2.3.2 Infrastruktura společnosti

Infrastruktura ES se z hlediska účelu, požadavků na bezpečnost a odpovědností za správu a provoz člení na komerční a procesní. Komerční a procesní infrastruktura by měla být na základě koncernových požadavků oddělena do samostatných síťových segmentů. Pro komerční infrastrukturu vyplývá z koncernových dokumentů povinnost zavést ISMS s ohledem na lokální legislativu a normy řady ISO/IEC 27000. Na procesní infrastrukturu se vztahuje kybernetický zákon, především v rámci distribuční sítě.

Komerční infrastruktura (dále jako CIT) zahrnuje ICT systémy, které slouží k provozu komerčních aplikací jako je informační systém SAP, kancelářské aplikace Microsoft Office a elektronická pošta. Komerční infrastruktura je podle lokalizace ICT zdrojů klasifikována na centralizovanou a decentralizovanou. Centralizovaná CIT obsahuje servery a zařízení pro ukládání dat používaných současně více uživateli. Systémy patřící k centralizované CIT jsou zpravidla umístěny v datových a servisních centrech obsluhující všechny společnosti v rámci koncernu. Decentralizovanou CIT se rozumí počítače na pracovišti, mobilní výpočetní technika a multifunkční zařízení. Počítače na pracovišti jsou přidělovány konkrétnímu zaměstnanci nebo funkční roli a nacházejí se především v administrativních budovách. Mobilní výpočetní technika a zařízení podléhají stejným standardům jako nepřenosná zařízení. Multifunkční zařízení mají rozhraní LAN pro možnost centrálního monitorování a řízení a jsou používána pro kopírování, skenování, tisk či jako fax. CIT je řízena centrálně v rámci celého koncernu a provozní odpovědnost za komerční infrastrukturu, datové a hlasové sítě má v celé mezinárodní skupině divize informačních technologií.

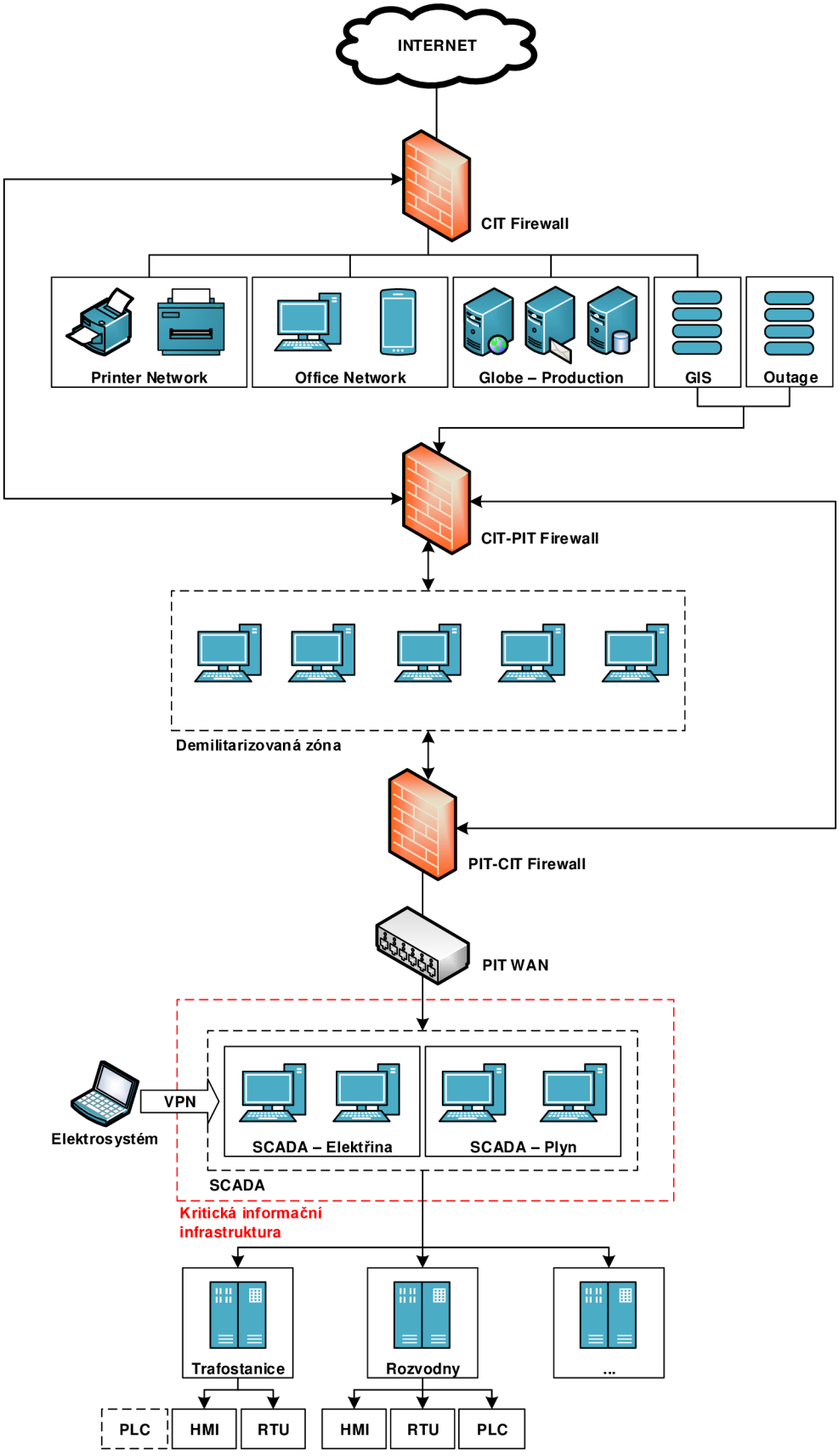
Procesní infrastruktura (dále jako PIT) obsahuje telekomunikační a informační technologie potřebné pro fungování technických procesů. Součástí PIT jsou řídící komponenty, síťové komponenty a aplikační systémy pro kontrolu a řízení výroby elektrické energie, jejího přenosu a distribuce. Na PIT jsou kladeny specifické požadavky na ochranu prvků z hlediska ověření dostupnosti či přípustných okolních a provozních podmínek z důvodu zajištění spolehlivé a nepřetržité dodávky energie v souladu s platnou legislativou.

Správa a provoz PIT je řešena lokálně s ohledem na koncernové požadavky a lokální legislativu, přičemž primární odpovědnost je přidělena distribuční společnosti. U PIT je z pohledu bezpečnosti vyžadována ochrana výrobních procesů se zajištěním maximální dostupnosti prvků s nezbytnou redundancí infrastruktury a zařízení, neboť se přípustná doba výpadku zařízení pohybuje v rámci hodin. Většina zařízení pro PIT jsou vyvíjena externími subjekty a následný servis obstarává na základě smluvních ujednání samotný dodavatel. Společnost provádí jen parametrizaci a nastavení zařízení a softwaru.

Informační systém pro dispečerské řízení a sběr dat z procesů se používá SCADA, jenž představuje centralizovaný systém s distribuovanou architekturou používaný v oblasti monitorování distribuce elektrické energie. Mezi řídící komponenty vyskytující se v PIT patří zařízení PQM (Power Quality Monitoring) pro řízení kvality elektrické sítě, hromadné dálkové ovládání (HDO) k regulaci odběru elektrické energie na dálku, RTU (Remote Terminal Unit) představující telemetrickou datovou jednotku určenou k podpoře SCADA, PLC (Programmable Logic Controller) ke správě elektrických komponent ve výrobních procesech a pro monitorování procesů v grafické podobě se používá HMI (Human Machine Interface).

Síťové prvky PIT zahrnují výrobní a řídící síť, komunikační router, firewall, modem, telefonní systém, sítě LAN a WAN. Výrobní síť slouží k napojení senzorů a ostatních výrobních zařízení k PLC a řídící síť propojuje dohledovou úroveň s kontrolními moduly. Sítě LAN a WAN jsou propojeny přes komunikační router a používají se pro komunikaci ve SCADA systémech. Firewall se používá se k ochraně sítě, filtrování paketů podle nastavených politik a oddělení sítí do bezpečnostních zón.

Některé prvky v rámci PIT jsou součástí kritické informační infrastruktury (dále jako KII) a vztahuje se na ně kybernetický zákon. Do KII jsou zahrnuty technické dispečinky provozovatele distribuční soustavy elektřiny a plynu, centrální systém SCADA, fyzické trasy komunikačního systému a podpůrná zařízení prvků informačního a komunikačního systému.



Obrázek 12: Infrastruktura ve společnosti (Upraveno dle interních materiálů)

2.3.3 Informační strategie

Přístup k řízení informačních a komunikačních technologií je charakteristický centrálním plánováním a integrací informační a podnikatelské strategie. ES se zaměřuje na využívání nejnovějších technologií pro vývoj nových produktů a služeb, neboť škálovatelná a agilní řešení spolu s konzistentní správou portfolia přispívají k jejich přidané hodnotě. Rostoucí význam informačních technologií ve společnosti je způsoben orientací na inovace a digitalizaci. Klíčovou roli zastávají mobilní technologie, sociální média, nástroje Big Data, řešení Smart Grid, inteligentní měřící přístroje a interaktivní prodej s cílem umožnit společnosti vytvářet nové obchodní modely.

Divize informačních technologií tvoří postupy a technická řešení zejména pro komerční infrastrukturu, dohlíží na poskytovatele síťových služeb a spolupracuje s jednotlivými obchodními jednotkami k poskytování služeb splňujících obchodní a bezpečnostní požadavky. Roli dodavatele IT služeb, systémového integrátora, správce hardwaru a softwaru vykonává pro komerční infrastrukturu celé skupiny v České republice dceřiná společnost, která je součástí nadnárodní skupiny pro poskytování IT služeb.

2.3.4 Bezpečnostní strategie

Posláním bezpečnosti informací v ES je splnění právních, regulatorních či koncernových požadavků a zajištění přiměřené ochrany aktiv, která jsou z obchodního hlediska důležitá. Hodnota informační bezpečnosti je vnímána ve smyslu minimalizace rizik, zamezení vzniku finančních ztrát, zajištění operativní spolehlivosti a zabezpečení zákaznických dat, komunikačních sítí či infrastruktury. Aktivity v oblasti bezpečnosti informací jsou realizovány v návaznosti na poslání a obchodní činnosti společnosti, neboť v souvislosti s postupem digitálních technologií se v rámci PIT i CIT zvyšují nároky na informační a fyzickou bezpečnost provozních systémů a za nesplnění legislativních požadavků hrozí společnosti sankce.

Pro identifikaci bezpečnostních požadavků se používají následující zdroje:

- Výsledky hodnocení rizik zohledňující podnikovou strategii a cíle,
- Požadavky vyplývající ze smluv, právních předpisů a vyhlášek,
- Zásady a obchodní požadavky na zpracování informací vyvinuté organizací pro podporu provozu.

Mezi faktory podněcující vytvoření ISMS v ES patří:

- Bezpečná a spolehlivá dodávka energie zákazníkům,
- Legislativní a regulatorní požadavky,
- Koncernové požadavky na ISMS,
- Využívání kybernetického prostoru,
- Integrace informační bezpečnosti do inteligentních sítí,
- Ochrana obchodních zájmů a dodržování právních předpisů.

Obecný rámec definující základní organizaci systému řízení bezpečnosti informací pro řízení a monitorování rizik vztahujících se k důvěrnosti, dostupnosti a integritě informací je vymezen politikou *Information Security* s účinností v celém koncernu. Holistický přístup s podrobnějším popisem základních činností v ISMS je stanoven směrnicemi s označením *GP3-19*, které vycházejí z principů řady norem ISO/IEC 27000 a zavazují jednotlivé společnosti ES k implementaci ISMS. Cílem nařízení je poskytnout definici minimálních požadavků na bezpečnost informací nejen pomocí obecných pravidel, ale i specifických postupů pro průmyslové řídící systémy (dále jako ICS).

Pro implementaci systému řízení bezpečnosti informací s působností až na úroveň řízení procesů v energetickém rozvodném průmyslu jsou používány i principy vycházející z technické zprávy ISO/IEC TR 27019, která se vztahuje na systémy řízení procesů používaných v energetice.

Aktivity společnosti jsou omezeny zákonnými povinnostmi a regulacemi v odvětví. Kromě energetického zákona, souvisejících vyhlášek a vládních nařízení se především na distribuční síť vztahuje kybernetický zákon. ES má vytvořen návrh strategie kybernetické bezpečnosti, který shrnuje výchozí podmínky pro kybernetickou bezpečnost v distribuční společnosti, současný stav činností a navrhuje opatření pro oblast PIT a CIT. Strategie pro kybernetickou bezpečnost je implementována do informační strategie distribuční společnosti a stanovuje rámec fungování technologií, procesů a personálu zajišťujícího provoz distribuční sítě. Implementace strategie je členěna do dvou etap. První fáze zahrnuje zavedení bezpečnostních opatření pro prvky KII a v následující etapě je posouzeno rozšíření systému kybernetické bezpečnosti o další významná aktiva vyskytující se v distribuční síti.

Kybernetická bezpečnost v distribuční společnosti je realizována formou projektu, jehož cílem je:

- Dosažení shody se zákonem o kybernetické bezpečnosti,
- Implementaci ISMS a případně i jeho certifikace,
- Implementace požadavků GP3-19,
- Uplatnění přístupu založeném na rizicích spočívající ve vyhodnocení vhodnosti ochrany aktiv a vynaložených nákladů vůči riziku,
- Měření a včasnou reakci na kybernetické incidenty.

Tabulka 4: Přehled odpovědností za rozhodnutí pro IS/ICT a ISMS (Zpracování vlastní)

Typ rozhodnutí	CIT	PIT
Priorita rozvoje IS/ICT	Centrálně divize IT	Distribuční společnost
Investice do IS/ICT	Vedení koncernu	Distribuční společnost
Architektura a standardy IS/ICT	Vedení koncernu	Vedení koncernu, distribuční společnost
Sourcing IS/ICT služeb a zdrojů	Vedení koncernu	Distribuční společnost
Operativní správa a provoz IS/ICT	Lokální divize IT	Distribuční společnost
Investice a rozvoj ISMS	Vedení koncernu, centrální divize IT	Distribuční společnost
Standardy pro ISMS	Vedení koncernu	Vedení koncernu, legislativa

2.4 Současný stav bezpečnosti informací ve společnosti

Popis současného stavu bezpečnosti informací se zabývá procesní infrastrukturou. Uvedené informace vycházejí z osobních sdělení a provedeného auditu pro zhodnocení souladu systému kybernetické bezpečnosti, jehož výsledky představují východiska pro posouzení systému bezpečnosti informací ve společnosti. Následující odstavce obsahují implementovaná opatření v jednotlivých oblastech dle normy ISO/IEC 27001.

Systém řízení bezpečnosti informací

Rozsah ISMS je stanoven, postupy pro řízení rizik jsou zavedeny a je prováděno hodnocení účinnosti ISMS, přičemž plánované audity bezpečnosti informací se mají vykonávat alespoň jedenkrát za rok. Aktualizace systému řízení bezpečnosti informací a související dokumentace se uskutečňuje na základě zjištění auditů a výsledků hodnocení ISMS. Důkazy o účinnosti bezpečnostních opatření jako výstup z procesu monitorování efektivity ISMS nejsou evidovány.

Řízení rizik

Metodiky pro identifikaci a hodnocení aktiv a rizik včetně určených kritérií pro přijetí rizik jsou stanoveny a u aktiv patřících do rozsahu ISMS je ohodnocena jejich důležitost. Při identifikaci rizik jsou zohledněny hrozby a zranitelnosti, zváženy potencionální dopady na aktiva a určena přijatelná rizika. Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováno prohlášení o aplikovatelnosti a plán zvládání rizik.

A.5 Politiky bezpečnosti informací

V organizaci je definována sada politik pro bezpečnost informací a vedení společnosti stanovuje směřování činností bezpečnosti informací. Proces posouzení vhodnosti a účinnosti bezpečnostní politiky je zaveden.

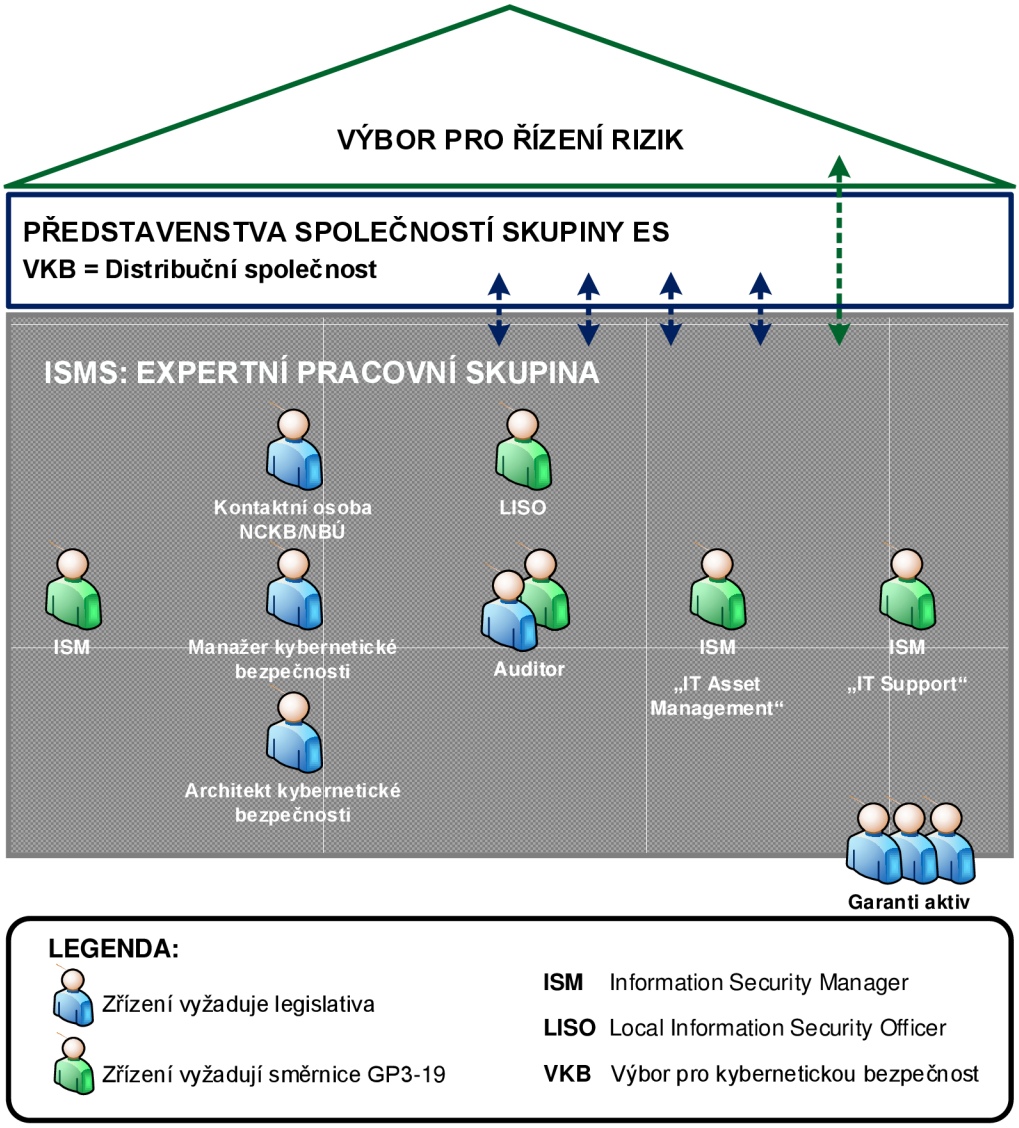
Mezi vytvořené, schválené a zavedené politiky bezpečnosti informací v ES patří:

- Systém řízení bezpečnosti informací,
- Organizace bezpečnosti,
- Klasifikace aktiv,
- Bezpečnost lidských zdrojů,
- Bezpečné chování uživatelů,
- Poskytování a nabývání licencí programového vybavení a informací,
- Fyzická bezpečnost,
- Bezpečné používání mobilních zařízení.

Společnost plánuje zpracovat dokumentaci pro ochranu před škodlivými kódy, řízení vztahů s dodavateli, zálohování a obnovu dat, řízení přístupu, používání kryptografické ochrany, řízení technických zranitelností a operační manuál pro komunikační sítě.

A.6 Organizace řízení bezpečnosti informací

Odpovědnosti za bezpečnost informací a principy oddělení povinností zaměstnanců jsou definovány a přiděleny. Pro řízení bezpečnosti informací byly určeny bezpečnostní role, které jsou stanoveny kybernetickým zákonem a koncernovými požadavky dle směrnice GP3-19. Pro splnění legislativních požadavků byl zřízen výbor pro řízení kybernetické bezpečnosti a bezpečnostní role garanta aktiva, manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti. Organizace řízení bezpečnosti informací v ES je uvedena na následujícím obrázku.



Obrázek 13: Organizace bezpečnosti informací ve společnosti (Upraveno dle interních materiálů)

A.7 Bezpečnost lidských zdrojů

Plán rozvoje bezpečnostního povědomí je zpracován a obsahuje definici formy a rozsahu potřebných školení. V rámci standardních personálních procesů jsou vedeny přehledy o absolvovaných školeních zaměstnanců a při ukončení nebo změně smluvního vztahu je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění. Pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel jsou určena. Společnost plánuje provádět vstupní a pravidelná školení o povinnostech a bezpečnostní politice v souladu s plánem rozvoje bezpečnostního povědomí pro uživatele, administrátory a osoby zastávající bezpečnostní role. Přezkoumávání dodržování bezpečnostní politiky je zajištěno pomocí auditů a monitorování činností technickými nástroji.

A.8 Řízení aktiv

Primární aktiva jsou evidována a hodnocení jejich důležitosti se provádí z hlediska důvěrnosti, integrity a dostupnosti. Pravidla pro přípustné způsoby používání aktiv, jejich manipulaci, bezpečné elektronické sdílení a fyzické přenášení jsou stanovena. Primární aktiva mají určeného odpovědného garanta. Způsoby pro spolehlivé smazání nebo zničení technických nosičů dat s ohledem na úroveň aktiv nejsou stanovena a v seznamu aktiv není určeno, která aktiva spadají do KII.

A.9 Řízení přístupu

Přístup k informačním a komunikačním systémům je řízen na základě bezpečnostních a provozních potřeb. Pravidla pro přístup k informacím a vybavení pro zpracování informací jsou stanovena. Přezkoumávání přístupových a administrátorských oprávnění se neprovádí pravidelně dle definovaných postupů. Společnost plánuje v komunikační síti a pro SCADA systémy zavést nástroje pro řízení přístupových oprávnění, ověřování identity uživatelů a centralizovaný sběr k zaznamenávání použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik. V rámci PIT se vyskytují sdílená hesla a politiky hesel nejsou uplatňovány.

Mezi mobilní zařízení dostupná v komunikační síti patří měřicí přístroje a notebooky sloužící jako terminály, přičemž bezpečnostní pravidla pro tato zařízení nejsou zavedena. Pro notebooky v CIT existuje politika a bezpečnostní manuál ICT.

A.10 Kryptografie

Implementace kryptografických opatření pro SCADA systémy a komunikační sítě je plánována ve třetí etapě projektu kybernetické bezpečnosti ES. Společnost musí vytvořit úroveň zabezpečení s ohledem na použitý kryptografický algoritmus a určit pravidla kryptografické ochrany informací při přenosu po komunikačních sítích, uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat. Pro používání kryptografických prostředků je nezbytné stanovit systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů.

A.11 Fyzická bezpečnost a bezpečnost prostředí

Opatření fyzické bezpečnosti k zamezení neoprávněného vstupu a zásahů do vymezených prostor, zajištění ochrany na úrovni a v rámci objektů jsou přijata, ale nepokrývají všechna rizika. Omezení fyzického přístupu k síti a zařízením průmyslových a řídících systémů je řešeno samostatným projektem.

A.12 Bezpečnost provozu

Za účelem podpory bezpečného provozu informačních a komunikačních systémů jsou stanoveny operační manuály, administrátorské příručky, provozní pravidla a postupy. Pro ochranu proti malwaru se používá Avast antivirus, u něhož probíhají pravidelné aktualizace signatur a definic. Společnost zamýšlí zavést systémy IDS/IPS k ochraně komunikace mezi sítěmi, serverů a sdílených datových úložišť. U činnosti uživatelů, administrátorů, informačních a komunikačních systémů se používá standartní logování na úrovni operačního systému, informační systém pro dispečerské řízení zaznamenává veškeré provozní činnosti. Monitoring činností v rámci PIT bude vylepšen implementací centralizovaného sběru událostí. Záložní kopie informací, softwaru a bitových kopií systému jsou pravidelně pořizovány, testovány a lokálně ukládány. Nastavení aktivních prvků komunikační sítě se zálohuje automatizovaným nástrojem při změně konfigurace.

A.13 Bezpečnost komunikací

Pravidla a postupy pro ochranu informací, jež jsou přenášeny komunikačními sítěmi, jsou stanovena, ale dokumentace popisující bezpečnost komunikační sítě není vytvořena. S ohledem na klasifikaci aktiv se výměna a předávání informací uskutečňuje na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací. Přístup mezi vnější a vnitřní sítí je řízený a pro síťovou infrastrukturu a SCADA systémy se používá princip oddělení. Společnost pro segmentaci síťové infrastruktury, zamezení přímé komunikace vnitřní sítě s vnější sítí a omezení propojení k síti průmyslových a řídících systémů používá firewally a demilitarizovanou zónou. Pro blokování přenášených dat, která nesplňují požadavky na ochranu komunikační sítě, se připravuje implementace systému IDS/IPS a ke zlepšení ochrany technických aktiv před využitím známých zranitelností se zavádí technologie SIEM.

A.14 Akvizice, vývoj a údržba systému

Společnost má stanoveny bezpečnostní požadavky při změnách v informačním nebo komunikačním systému a při žádosti o dodání nových funkcí od dodavatele existuje definovaný proces a pravidla pro logistiku včetně dohod s bezpečnostním manažerem. ES pracuje na vytvoření dokumentace pro bezpečnost komunikačních sítí, řešení údržby sítí a řízení technických zranitelností. Testování změn v informačních a komunikačních systémech se provádí před jejich zavedením do provozu. Nové aktivní prvky a jejich konfigurace jsou testovány ve vyhrazeném prostředí.

A.15 Vztahy s dodavateli

Vztahy s dodavateli jsou upravovány v rámci SLA smluv určujících způsoby a úrovně realizace bezpečnostních opatření a vzájemné smluvní odpovědnosti. Společnost plánuje stanovit a zdokumentovat pravidla pro dodavatele zohledňující potřeby řízení bezpečnosti informací, kontrolovat významné dodavatele a provádět hodnocení rizik před uzavřením smlouvy s poskytovateli služeb.

A.16 Řízení incidentů bezpečnosti informací

Proces řízení a komplexní evidence incidentů bezpečnosti informací není formálně stanoven. Zaměstnanci společnosti mají povinnost hlásit vzniklé bezpečnostní události a incidenty. Pro detekci bezpečnostních událostí, flexibilnější reakci na útoky, ověření a kontrolu komunikace je připravována implementace centralizovaného sběru událostí, systémů IDS/IPS a SIEM.

A.17 Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací

Práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role jsou stanoveny v dokumentu Business Continuity Management, pro něhož se připravuje směrnice. Společnost má zpracovány plány obnovy provozu, které avšak neobsahují scénáře potřebné k obnovení činnosti všech prvků infrastruktury. Z pohledu požadavků na dostupnost se v komunikační síti vyskytuje redundance optických tras zapojením do kruhu a kritického hardwaru. Na úrovni SCADA systémů je zaveden provozní monitoring, plně redundantní informační systém pro dispečerské řízení a rovněž je na základě smluv s dodavatelem systému zajištěna náhrada technických aktiv. ES zamýšlí zpracovat analýzu dopadů, strategii řízení kontinuity činnosti organizace a nasadit systémový monitoring.

A.18 Soulad s požadavky

Soulad s právními předpisy, normami, smluvními závazky a koncernovými požadavky je zajišťován pomocí auditů ISMS. Pravidelné kontroly dodržování bezpečnostní politiky jsou uskutečňovány a zdokumentovány. Audity kybernetické bezpečnosti a kontroly zranitelnosti technických prostředků automatizovanými nástroji jsou plánovány.

2.5 Shrnutí analýzy současného stavu ISMS ve společnosti

Společnost zavádí ISMS s ohledem na požadavky stanovené koncernovými směrnicemi GP3-19 a kybernetickým zákonem, přičemž strategie pro kybernetickou bezpečnost je součástí informační strategie a veškeré aktivity jsou realizovány v návaznosti na ochranu obchodních zájmů a aktiv společnosti.

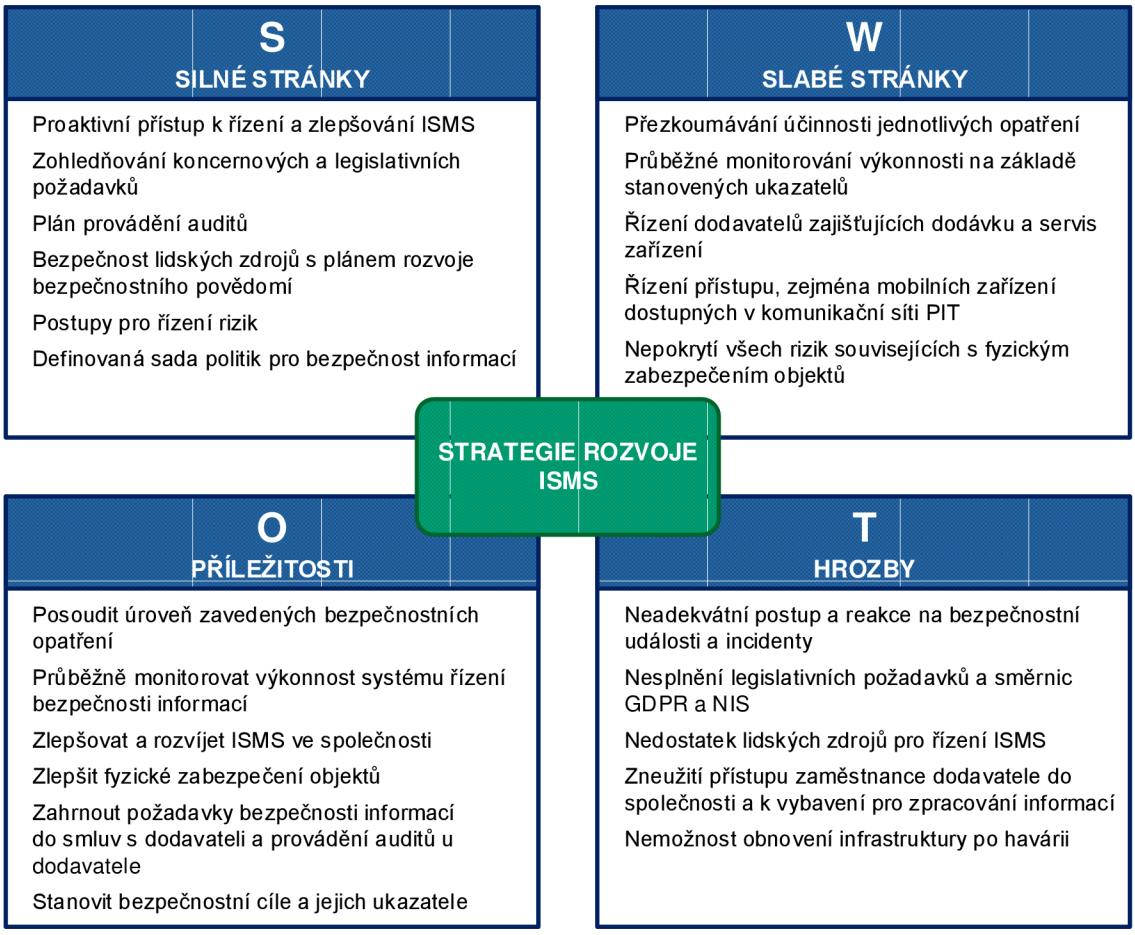
Mezi požadavky koncernových směrnic patří definice, dokumentace a přezkoumání cílů bezpečnosti informací, avšak součástí současné bezpečnostní strategie společnosti není přezkoumávání účinnosti jednotlivých opatření, porovnávání a průběžné monitorování výkonnosti na základě stanovených ukazatelů a vyhodnocování plnění cílů.

Jedním z největších rizik z pohledu bezpečnosti informací v rámci PIT představuje řízení dodavatelů zajišťujících dodávku a servis zařízení, neboť mají přístup do prostor společnosti a k vybavení pro zpracování informací. Nebezpečí lze spatřovat i v řízení přístupu mobilních zařízení dostupných v komunikační síti, pro něž nejsou zavedena bezpečnostní pravidla.

Další problematickou oblastí současného stavu řízení bezpečnosti informací je řízení kontinuity činnosti organizace pro obnovení všech prvků infrastruktury po havárii, nepokrytí všech rizik souvisejících s fyzickým zabezpečením objektů a nedostatek lidských zdrojů pro adekvátní řízení provozu ISMS.

Současný stav informační bezpečnosti dosahuje v některých oblastech vysoké úrovně, ale vyskytují se i výrazné nedostatky a rozdíly mezi popsanými a realizovanými opatřeními. Většinu nedostatků lze odstranit organizačními změnami, úpravou stávající dokumentace nebo implementací plánovaných technických opatření.

V následující tabulce je sestavena SWOT analýza ISMS v kontextu PIT, která zachycuje silné a slabé stránky současného stavu ISMS a jeho příležitosti a hrozby plynoucí z vnitřního i vnějšího prostředí. Příležitosti představují budoucí cíle nebo možnosti ke zlepšení, zatímco hrozby reprezentují negativní změny či potencionální rizika vzhledem k ISMS. Sestavená SWOT matice napomůže k definování strategie v ISMS založené na příležitostech a hrozbách a tím přispěje ke zvýšení účinnosti ISMS společnosti.



Obrázek 14: SWOT analýza ISMS společnosti (Zpracování vlastní)

Společnost nadále plánuje provádět pravidelná školení bezpečnosti, zavést IDS/IPS systémy, technologii SIEM, nástroj pro řízení přístupových oprávnění a ověřování identity uživatelů, kryptografická opatření, systémový monitoring, vypracovat analýzu dopadů a chybějící dokumentaci, a z tohoto důvodu nejsou uvedená opatření ve SWOT analýze řešena. Následující strategie ISMS se zaměří na využití uvedených příležitostí pro minimalizaci slabých stránek a zmírnění hrozeb za podpory silných stránek.

3 VLASTNÍ NÁVRHY ŘEŠENÍ, PŘÍNOS NÁVRHŮ ŘEŠENÍ

Kapitola vlastního návrhu řešení se zaměřuje na problematiku hodnocení zavádění systému řízení bezpečnosti informací v energetické společnosti. Nejprve je provedena analýza rizik bezpečnosti informací a pomocí sestaveného modelu zralosti je ohodnocena úroveň zavedených opatření vymezených normou ISO/IEC 27002. Na základě zjištěných nedostatků je navržen akční plán pro ISMS a vytvořen soubor ukazatelů ke stanovení jeho efektivity a efektivnosti. Na závěr jsou uvedeny přínosy práce pro teoretické poznání a podnikovou praxi.

3.1 Stanovení rozsahu přehodnocení ve společnosti

Rozsah přehodnocení je stanoven na řídící a monitorovací procesy v rámci PIT zahrnující informační aktiva, infrastrukturu a aplikační systémy pro kontrolu a přímé řízení výroby, přenosu a distribuce elektrické energie. Předmětem přezkoumání není CIT a procesy související s výrobou, přepravou, distribucí, uskladňováním a obchodováním s plynem.

3.2 Analýza rizik společnosti

Přijetí bezpečnostních opatření musí být dle normy ISO/IEC 27001 založeno na riziku. Požadavek lze splnit povedením analýzy rizik, která umožňuje určit prioritu rizik podle jejich vnímané důležitosti. Analýza rizik by měla být v rámci ISMS prováděna v pravidelných intervalech. Posouzení rizik stanovuje hodnotu informačních aktiv, identifikuje možné a existující hrozby a zranitelnosti, určuje stávající opatření a jejich účinek na riziko, determinuje potencionální dopady.

Analýza rizik společnosti obsahuje identifikaci a ohodnocení aktiv, identifikaci hrozeb a zranitelností a stanovení míry rizika za použití maticové metody analýzy rizik, přičemž postup je popsán v následujících podkapitolách. Kvalitativní analýza rizik byla provedena ve spolupráci s pracovníky z oddělení řízení rizik, správcem IT aktiv.

3.2.1 Identifikace a ohodnocení aktiv

Aktiva jsou nejprve identifikována a ohodnocena určením velikosti dopadu při narušení důvěrnosti, dostupnosti a integrity. Klasifikační schéma použité k hodnocení aktiv je uvedeno v následující tabulce.

Tabulka 5: Klasifikační stupnice dopadu pro určení hodnoty aktiva (Zpracování vlastní)

Hodnota aktiva	Hodnocení dopadu	Míra rizika
1	Žádný dopad na organizaci	Bezvýznamné riziko
2	Zanedbatelný dopad na organizaci	Akceptovatelné riziko
3	Potíže nebo finanční ztráty	Nízké riziko
4	Vážné potíže či podstatné finanční ztráty	Nežádoucí riziko
5	Existenční potíže	Nepřijatelné riziko

Tabulka 6 obsahuje seznam logicky seskupených aktiv a jejich ohodnocení. Identifikace aktiv je provedena na vhodném stupni podrobnosti, který poskytuje pro posouzení rizik dostatek informací. Hodnota aktiva je stanovena pomocí součtového algoritmu.

Tabulka 6: Seznam identifikovaných a ohodnocených aktiv společnosti (Zpracování vlastní)

Skupina	Zdroj	Dostupnost	Důvěrnost	Integrita	Hodnota
Data	Popisná data systému	1	2	2	2
	Historická provozní data	2	2	3	2
	Manipulační data reálného času	4	3	3	3
Aplikační systémy	Network management	4	3	4	4
	Network monitoring	3	2	3	3
	Aplikační SW SCADA	5	5	5	5
	Řídící systém	5	5	5	5
	Telekomunikační systém	5	4	5	5
	Řízení infrastruktury datacentra	4	4	4	4
Infrastruktura	Páteřní síť PIT	5	4	5	5
	LAN PIT	5	4	5	5
	WAN PIT	5	4	5	5
	Aktivní prvky PIT	4	3	4	4
	Kontrolní a řídící zařízení	4	2	3	3
	Rozvodna	5	4	5	5
	Záložní napájení	4	2	4	3
	Telefonní ústředny	5	4	5	5
	Datové centrum	5	5	5	5
	Serverovna	5	4	4	4
Hardware	Servery	5	4	4	4
	Notebooky a mobilní zařízení	2	3	2	2
	Dispečerské a PIT telefony	3	2	3	3
	Přenosné nosiče dat	2	3	2	2

3.2.2 Identifikace hrozeb a zranitelností

Pro sestavení matice zranitelností je nutné identifikovat hrozby a pravděpodobnosti jejich výskytu. Následující tabulka uvádí použité klasifikační schéma pro ohodnocení hrozeb a zranitelností.

Tabulka 7: Klasifikační stupnice pro pravděpodobnost výskytu hrozby (Zpracování vlastní)

Hodnota	Slovní vyjádření pravděpodobnosti výskytu hrozby
1	Velmi nízká pravděpodobnost výskytu hrozby
2	Nízká pravděpodobnost výskytu hrozby
3	Střední pravděpodobnost výskytu hrozby
4	Vysoká pravděpodobnost výskytu hrozby
5	Velmi vysoká pravděpodobnost výskytu hrozby

Následně jsou identifikovány významné hrozby, které mohou ohrozit aktiva nebo omezit provoz společnosti. Hrozby jsou vybrány na základě standardních hrozeb uvedených v normě ISO/IEC 27005, doporučení, zkušeností, názorů odborníků a vytvořeném seznamu hrozeb společnosti.

Z důvodu anonymizace a citlivých informací energetické společnosti je proces identifikace hrozeb a zranitelností proveden na obecnější úrovni, ale pro účely diplomové práce a dalšího zpracování poskytuje dostatek informací.

Norma ISO/IEC 27005 definuje typ relevantního zdroje hrozby následovně:

- **A – accindental** – náhodný – použito pro lidské činnosti, které mohou následně poškodit informační aktiva,
- **D – deliberate** – úmyslný – použito pro úmyslné akce zaměřené na aktiva,
- **E – enviromental** – environmentální – použito pro všechny incidenty, které nejsou založeny na lidské činnosti.

Výsledný seznam hrozeb je uspořádaný dle typů hrozeb a zahrnuje subjektivní hodnocení pravděpodobnosti jejich výskytu a typ relevantního zdroje.

Tabulka 8: Identifikace hrozeb společnosti s pravděpodobností jejich výskytu (Zpracování vlastní)

Typ	Hrozba	Zdroj	Pravděpodobnost výskytu
Prostředí	Přírodní katastrofa	E	1
	Požár	A, D, E	1
	Přerušení dodávky elektřiny	A, D, E	3
	Elektromagnetické záření a impulzy	A, D, E	2
Neoprávněné činnosti	Používání neschváleného hardwaru nebo softwaru	A, D	3
	Zneužití přístupových oprávnění uživatele	A, D	3
	Zneužití administrátorských oprávnění	A, D	2
	Neoprávněné kopírování dat	A, D	2
	Neoprávněný vstup do místností s technickým vybavením	A, D	2
Důvěrnost služeb	Škodlivý software	A, D	3
	Napadení hackerem	D	2
	Závislost na dodavatelích	A, D	4
	Nesprávně nastavená SLA	A	3
	Neoprávněný přístup do sítě	A, D	3
	Neoprávněný přístup k serverům	A, D	2
	Krádež technického vybavení	D	3
Lidský faktor	Fyzické poškození zařízení	A, D	2
	Nedostatek kvalifikovaných zaměstnanců	A, D, E	4
	Vzdálený přístup uživatelů	A, D	3
	Nedostatečné školení	A	3
	Nedodržování směrnic	A, D	3
	Narušení integrity dat	A, D	3
Technická selhání	Nevhodný hardware pro použití v ICS	A	2
	Selhání hardwaru	A	2
	Chybná konfigurace hardwaru a softwaru	A, D	3
	Výpadek komunikační sítě	A, D, E	3
	Chybné fungování aplikačního programového vybavení	A	2

Posouzení zranitelnosti jednotlivých aktiv společnosti jednotlivými hrozbami zachycuje matice zranitelnosti, která je uvedena v následující tabulce.

Tabulka 9: Matice zranitelnosti společnosti (Zpracování vlastní)

V *Zranitelnost*	**Popis hrozby**	Přírodní katastrofa	Požár	Přerušení dodávky elektřiny	Elektromagnetické záření a impulzy	Používání neschváleného hardwaru nebo softwaru	Zneužití přístupových oprávnění uživatele	Zneužití administrátorských oprávnění	Neoprávněné kopírování dat	Neoprávněný vstup do místností s technickým vybavením	Škodlivý software	Napadení hackerem	Závislost na dodavatelích	Nesprávně nastavená SLA	Neoprávněný přístup do sítě	Neoprávněný přístup k serverům	Krádež technického vybavení	Fyzické poškození zařízení	Nedostatek kvalifikovaných zaměstnanců	Vzdálený přístup uživatelů	Nedostatečné školení	Nedodržování směrnic	Narušení integrity dat	Nevhodný hardware pro použití v ICS	Selhání hardwaru	Chybná konfigurace hardwaru a softwaru	Výpadek komunikační sítě	Chybné fungování aplikačního programového vybavení
	T	**1**	**1**	**3**	**2**	**3**	**3**	**2**	**2**	**2**	**3**	**2**	**4**	**3**	**3**	**2**	**3**	**2**	**4**	**3**	**3**	**3**	**3**	**2**	**2**	**3**	**3**	**2**
Aktivum	**A**																											
Popisná data systému	**2**	2	2	1	1	1	1	1	2	1	1	1	0	0	1	1	2	1	0	1	1	2	3	1	1	2	1	1
Historická provozní data	**2**	2	2	1	1	1	1	1	2	1	1	1	0	0	1	1	2	1	0	1	1	2	3	1	1	2	1	1
Manipulační data reálného času	**3**	3	3	2	1	1	1	1	2	1	1	1	0	0	2	2	2	1	0	2	1	2	3	1	1	2	2	1
Network management	**4**	4	4	2	1	2	2	3	2	1	2	3	2	2	3	3	1	1	3	2	3	3	2	2	2	3	3	2
Network monitoring	**3**	4	4	2	1	2	2	3	2	1	2	3	2	2	3	3	1	1	3	2	3	3	2	2	2	3	3	2
Aplikační SW SCADA	**5**	5	5	4	1	3	3	4	3	2	3	4	4	3	4	4	2	2	4	3	4	4	3	3	3	4	4	3
Řídicí systém	**5**	5	5	4	1	3	3	4	3	2	3	4	4	3	4	4	2	2	4	3	4	4	3	3	3	4	4	3
Telekomunikační systém	**5**	5	5	3	1	2	2	3	2	1	2	3	3	2	3	3	2	1	3	2	3	3	2	2	3	3	4	2
Řízení infrastruktury datacentra	**4**	4	4	3	1	2	1	2	2	1	2	3	2	2	3	3	1	1	3	2	3	3	2	2	2	3	4	2
Páteřní síť PIT	**5**	5	5	2	3	1	2	3	1	3	2	2	2	2	2	1	2	2	2	2	2	2	1	4	2	2	3	1
LAN PIT	**5**	5	5	2	3	1	2	3	2	3	3	3	2	2	3	2	2	2	2	3	2	3	1	4	2	2	3	1
WAN PIT	**5**	5	5	2	3	1	2	3	1	3	2	2	2	2	2	2	2	2	2	2	2	3	1	4	2	2	3	1
Aktivní prvky PIT	**4**	3	3	2	2	3	2	3	1	3	2	2	2	2	3	2	3	3	3	3	3	3	3	4	3	3	3	2
Kontrolní a řídicí zařízení	**3**	3	3	2	2	1	1	2	1	2	1	1	2	2	2	1	3	3	3	2	3	2	2	3	2	3	2	2
Rozvodna	**5**	5	4	2	1	2	0	0	0	4	0	0	1	0	0	0	2	2	2	1	1	2	0	2	3	2	3	1
Záložní napájení	**3**	3	3	0	1	1	0	0	0	1	0	0	0	0	0	0	1	1	1	0	1	2	0	3	2	1	0	1
Telefonní ústředny	**5**	4	4	3	1	2	1	2	1	4	0	0	1	0	2	1	2	2	3	1	2	2	0	3	3	2	3	2
Datové centrum	**5**	5	4	3	2	3	2	3	2	4	2	2	3	3	2	2	2	2	3	2	3	3	2	3	2	2	3	2
Serverovna	**4**	5	4	3	2	3	2	2	2	4	3	3	2	3	2	2	2	2	3	2	3	3	2	3	3	2	3	2
Servery	**4**	4	4	2	3	3	4	4	2	3	3	3	1	2	3	3	3	3	3	3	4	4	3	4	3	4	3	3
Notebooky a mobilní zařízení	**2**	2	2	1	1	2	2	2	3	1	2	3	1	1	1	1	2	2	2	1	3	3	3	1	2	3	2	2
Dispečerské a PIT telefony	**3**	3	3	2	1	1	1	0	0	1	0	0	1	1	1	1	2	2	1	1	2	2	1	2	2	2	1	1
Přenosné nosiče dat	**2**	1	1	1	1	1	2	0	3	1	2	2	1	0	1	1	2	2	1	1	3	3	3	1	1	1	1	1

3.2.3 Stanovení míry rizik

Součástí analýzy rizik je sestavení matice rizik udávající míru rizik pro jednotlivá aktiva. Míra rizika je vypočtena jako součin pravděpodobnosti výskytu hrozby T, hodnoty aktiva A a zranitelnosti V.

Na závěr jsou stanoveny hranice rizika, přičemž rozsah a termíny si může společnost zvolit v závislosti na bezpečnostních potřebách. Pro určení přístupu k rizikům jsou jednotlivá rizika klasifikována do pěti úrovní. Hranice rizika a slovní vyjádření rizika zobrazuje tabulka 11.

Tabulka 10: Matice rizik společnosti (Zpracování vlastní)

R *Riziko*	**Popis hrozby**	Přírodní katastrofa	Požár	Přerušení dodávky elektřiny	Elektromagnetické záření a impulzy	Používání neschváleného hardwaru nebo softwaru	Zneužití přístupových oprávnění uživatele	Zneužití administrátorských oprávnění	Neoprávněné kopírování dat	Neoprávněný vstup do místností s technickým vybavením	Škodlivý software	Napadení hackerem	Závislost na dodavatelích	Nesprávně nastavená SLA	Neoprávněný přístup do sítě	Neoprávněný přístup k serverům	Krádež technického vybavení	Fyzické poškození zařízení	Nedostatek kvalifikovaných zaměstnanců	Vzdálený přístup uživatelů	Nedostatečné školení	Nedodržování směrnic	Narušení integrity dat	Nevhodný hardware pro použití v ICS	Selhání hardwaru	Chybná konfigurace hardwaru a softwaru	Výpadek komunikační sítě	Chybné fungování aplikačního programového vybavení
	T	1	1	3	2	3	3	2	2	2	3	2	4	3	3	2	3	2	4	3	3	3	3	2	2	3	3	2
Aktivum	**A**																											
Popisná data systému	2	4	4	6	4	6	6	4	8	4	6	4	0	0	6	4	12	4	0	6	6	12	18	4	4	12	6	4
Historická provozní data	2	4	4	6	4	6	6	4	8	4	6	4	0	0	6	4	12	4	0	6	6	12	18	4	4	12	6	4
Manipulační data reálného času	3	9	9	18	6	9	9	6	12	6	9	6	0	0	18	12	18	6	0	18	9	18	27	6	6	18	18	6
Network management	4	16	16	24	8	24	24	24	16	8	24	24	32	24	36	24	12	8	48	24	36	36	24	16	16	36	36	16
Network monitoring	3	12	12	18	6	18	18	18	12	6	18	18	24	18	27	18	9	6	36	18	27	27	18	12	12	27	27	12
Aplikační SW SCADA	5	25	25	60	10	45	45	40	30	20	45	40	80	45	60	40	30	20	80	45	60	60	45	30	30	60	60	30
Řídící systém	5	25	25	60	10	45	45	40	30	20	45	40	80	45	60	40	30	20	80	45	60	60	45	30	30	60	60	30
Telekomunikační systém	5	25	25	45	10	30	30	30	20	10	30	30	60	30	45	30	30	10	60	30	45	45	30	20	30	45	60	20
Řízení infrastruktury datacentra	4	16	16	36	8	24	12	16	16	8	24	24	32	24	36	24	12	8	48	24	36	36	24	16	16	36	48	16
Páteřní síť PIT	5	25	25	30	30	15	30	30	10	30	30	20	40	30	30	10	30	20	40	30	30	30	15	40	20	30	45	10
LAN PIT	5	25	25	30	30	15	30	30	20	30	45	30	40	30	45	20	30	20	40	45	30	45	15	40	20	30	45	10
WAN PIT	5	25	25	30	30	15	30	30	10	30	30	20	40	30	30	20	30	20	40	30	30	45	15	40	20	30	45	10
Aktivní prvky PIT	4	12	12	24	16	36	24	24	8	24	24	16	32	24	36	16	36	24	48	36	36	36	36	32	24	36	36	16
Kontrolní a řídící zařízení	3	9	9	18	12	9	9	12	6	12	9	6	24	18	18	6	27	18	36	18	27	18	18	18	12	27	18	12
Rozvodna	5	25	20	30	10	30	0	0	0	40	0	0	20	0	0	0	30	20	40	15	15	30	0	20	30	30	45	10
Záložní napájení	3	9	9	0	6	9	0	0	0	6	0	0	0	0	0	0	9	6	12	0	9	18	0	18	12	9	0	6
Telefonní ústředny	5	20	20	45	10	30	15	20	10	40	0	0	20	0	30	10	30	20	60	15	30	30	0	30	30	30	45	20
Datové centrum	5	25	20	45	20	45	30	30	20	40	30	20	60	45	30	20	30	20	60	30	45	45	30	30	20	30	45	20
Serverovna	4	20	16	36	16	36	24	16	16	32	36	24	32	36	24	16	24	16	48	24	36	36	24	24	24	24	36	16
Servery	4	16	16	24	24	36	48	32	16	24	36	24	16	24	36	24	36	24	48	36	48	48	36	32	24	48	36	24
Notebooky a mobilní zařízení	2	4	4	6	4	12	12	8	12	4	12	12	8	6	6	4	12	8	16	6	18	18	18	4	8	18	12	8
Dispečerské a PIT telefony	3	9	9	18	6	9	9	6	0	6	0	0	12	9	9	6	18	12	12	9	18	18	9	12	12	18	9	6
Přenosné nosiče dat	2	2	2	6	4	6	6	4	12	4	12	8	8	0	6	4	12	8	8	6	18	18	18	4	4	6	6	4

Tabulka 11: Stanovení hranic rizika společnosti (Zpracování vlastní)

Hranice rizika	Slovní vyjádření rizika
0 až 10	Bezvýznamné riziko
11 až 20	Akceptovatelné riziko
21 až 30	Mírné riziko
31 až 60	Nežádoucí riziko
60 a více	Nepřijatelné riziko

3.3 Posouzení bezpečnostních opatření pomocí zralostního modelu

Posouzení bezpečnostních opatření pomocí zralostního modelu ve stanoveném kontextu poskytne celkový přehled a dokumentovaný postup hodnocení současné úrovně činností, procesů a metod souvisejících s bezpečností informací. Získané výsledky ze zralostního modelu lze ve společnosti využít při určování cílů a priorit či pro neustálé zlepšování bezpečnosti informací.

3.3.1 Postup sestavení zralostního modelu

Referenčním modelem pro posouzení bezpečnostních opatření je norma ISO/IEC 27002, která poskytuje doporučení osvědčených postupů pro správu informační bezpečnosti v souladu s mezinárodně uznávaným standardem aplikovatelným v organizacích všech velikostí a úrovní zabezpečení. Mezi další důvody pro vymezení obsahového rámce zralostního modelu pomocí opatření z normy ISO/IEC 27002 patří technická zpráva ISO/IEC TR 27019, která z této normy vychází, koncernové požadavky a bezpečnostní strategie společnosti, jež stanovují pro ISMS použít principy řady norem ISO/IEC 27000 a případně i certifikaci systému řízení bezpečnosti informací dle ISO/IEC 27001.

Způsobilost opatření v sestaveném modelu zralosti je vyjádřena prostřednictvím stupnice normy ISO/IEC 15504 se souborem atributů indikujících dosažení příslušné úrovně. Škála způsobilosti byla vybrána na základě doporučení metodiky COBIT 5, která pro formální hodnocení míry způsobilosti procesu vychází z principů uvedených v normě ISO/IEC 15504. Následující tabulka zachycuje úrovně způsobilosti s jejich slovním popisem a atributy pro zralostní model.

Tabulka 12: Použitá stupnice pro vyjádření způsobilosti opatření s atributy (Upraveno dle: 20)

Způsobilost procesu	Slovní popis	Atributy
0: Neúplný	Proces není implementován nebo nedosahuje svého účelu.	Není systematicky dosahováno účelu procesu.
1: Vykonávaný	Proces je implementován a dosahuje svého účelu	1.1 Výkonnost procesu
2: Řízený	Vykonávaný proces je implementován řízeným způsobem a jeho pracovní produkty jsou vhodně vytvořeny, řízeny a udržovány.	2.1 Řízení výkonnosti 2.2 Řízení pracovních produktů
3: Zavedený	Je použit stanovený proces, který je schopen dosáhnout svých výsledků.	3.1 Vymezení procesu 3.2 Zavedení procesu
4: Předvídatelný	Zavedený proces pracuje v rámci stanovených omezení procesu, aby dosáhl svých výsledků.	4.1 Měření procesu 4.2 Kontrola procesu
5: Optimalizovaný	Předvídatelný proces je neustále zlepšován, aby splnil relevantní podnikové cíle.	5.1 Inovace procesu 5.2 Optimalizace procesu

Zralostní model pro hodnocení způsobilosti bezpečnostních opatření obsahuje množinu indikátorů, které posuzovatelům pomáhají zdůvodnit klasifikaci atributů a současně představují východiska pro opakovatelné použití modelu. Jednotlivá opatření uvedená v normě ISO/IEC 27002 poskytují výchozí kritéria, na jejichž základě je provedeno mapování indikátorů v atributech identifikujících způsobilost opatření.

Úrovně zralosti jsou navrženy jako možné popisy současného a budoucího stavu opatření a rozsah dosažení atributu je charakterizován na stanovené klasifikační stupnici, která je uvedena v následující tabulce.

Tabulka 13: Použitá klasifikační stupnice určující rozsah dosažení atributu (Zpracování vlastní)

Rozsah dosažení atributu	Použitá zkratka	Rozsah dosažení atributu v [%]
Nedosaženo	N	0-15 %
Částečně dosaženo	P	15-50 %
Významně dosaženo	L	50-85 %
Úplně dosaženo	F	85-100 %

Zralost opatření je určena kombinací dosažení atributů a jejich seskupováním. Přechod na vyšší úroveň způsobilosti je podmíněn úplným splněním všech atributů na nižší úrovni a na daném stupni zralosti musí být atributy významně dosaženy. Dělení podle stupně zralosti poskytuje návod při definici současného a budoucího stavu opatření a identifikaci nezbytných zlepšení pro oblast bezpečnosti informací.

3.3.2 Realizace posouzení pomocí zralostního modelu

Účelem přezkoumání je pro stanovený rozsah přehodnocení zjištění současné úrovně bezpečnostních opatření s identifikací souvisejících procesů a určení nezbytných zlepšení jednotlivých opatření.

Posouzení způsobilosti bezpečnostních opatření prostřednictvím zralostního modelu bylo provedeno ve spolupráci s vedoucím pracovníkem pro bezpečnost informací (LISO), zaměstnanci z oddělení řízení rizik a správcem IT aktiv. Pro určení současného stavu opatření některých kapitol normy ISO/IEC 27002 bylo shromažďování údajů realizováno formou konzultací s osobami odpovědnými za vykonávání daného opatření či odborníky pro danou oblast. Objektivní důkazy pro ověření informací obsahuje dokumentace ISMS.

Fáze hodnocení způsobilosti opatření pomocí zralostního modelu tvoří:

- **Analýza činností souvisejících s opatřením** zahrnující identifikaci všech aktivit a procesů pro dosažení cíle bezpečnostního opatření,
- **Určení současné úrovně zralosti opatření** vycházející z míry plnění indikátorů vymezujících rozsah dosažení atributů,
- **Stanovení požadované úrovně zralosti** splňující kladené požadavky na zvýšení účinnosti a efektivnosti opatření,
- **Přidělení priority** vyjadřující relativní důležitost bezpečnostního opatření a celé kapitoly normy ISO/IEC 27002 pro společnost, na jejímž základě lze usměrňovat budoucí úsilí v oblasti bezpečnosti informací,
- **Návrh nezbytných zlepšení pro dosažení cílové úrovně** obsahující plánovaná zdokonalení k odstranění zjištěných nedostatků.

Pro účely tvorby auditního záznamu byl sestaven hodnotící list obsahující:

- Seznam opatření a kapitoly normy ISO/IEC 27002,
- Hodnotu současné úrovně zralosti opatření,
- Hodnotu požadované úrovně zralosti opatření,
- Stanovenou prioritu opatření a oblastí,
- Určení osob odpovědných za vykonání přehodnocení opatření,
- Identifikaci souvisejících procesů a činností k opatření,
- Definici nezbytných zlepšení opatření.

Pro vyjádření priority opatření a oblasti bezpečnosti informací je stanovena klasifikační stupnice, jež je zobrazena v následující tabulce.

Tabulka 14: Klasifikační stupnice pro vyjádření priority opatření a oblasti (Zpracování vlastní)

Hodnota	Slovní vyjádření priority opatření a oblasti
1	Velmi nízká relativní důležitost opatření nebo oblasti pro snížení rizika
2	Nízká relativní důležitost opatření nebo oblasti pro snížení rizika
3	Střední relativní důležitost opatření nebo oblasti pro snížení rizika
4	Vysoká relativní důležitost opatření nebo oblasti pro snížení rizika
5	Velmi vysoká relativní důležitost opatření nebo oblasti pro snížení rizika

Posouzení způsobilosti bezpečnostních opatření v rámci PIT zahrnuje všechna opatření vymezená normou ISO/IEC 27002. Po dokončení hodnocení zralosti opatření je nutné sdělit výsledky vedení společnosti, osobám odpovědným za dané opatření a pracovníkům zastávající bezpečnostní role.

3.3.3 Výsledky posouzení pomocí zralostního modelu

Podkapitola obsahuje získané výsledky z posouzení bezpečnostních opatření pomocí sestaveného zralostního modelu. Z důvodu ochrany citlivých údajů společnosti jsou uvedena pouze souhrnná data. Představen je i postup identifikace opatření vyžadujících nezbytná zlepšení.

Postup identifikace opatření vyžadujících nezbytná zlepšení

Zralostní model k vyhodnocení jednotlivých opatření využívá tři parametry, kterými jsou současná úroveň způsobilosti, požadovaná úroveň způsobilosti a priorita opatření. Výsledná celočíselná hodnota pro dané opatření je vypočtena pomocí vztahu:

$$\boldsymbol{RV_o = (RM_o - CM_o) \cdot PM_o},$$

kde použité symboly mají následující význam:

RV_o – výsledná hodnota pro dané opatření,

RM_o – požadovaná úroveň způsobilosti opatření,

CM_o – současná úroveň způsobilosti opatření,

PM_o – stanovená priorita opatření.

Pro vymezení přístupu k opatření jsou pro výslednou hodnotu stanoveny hranice, které klasifikují jednotlivá opatření do tří úrovní podle míry splnění požadavků normy a jejich relativní důležitosti. Rozsah pro individuální úrovně je zvolen s ohledem na použitou škálu pro současnou a požadovanou úroveň způsobilosti (0-5) a stupnici určující prioritu (1-5). Hranice pro ustanovení přístupu k opatření a jejich slovní vyjádření jsou uvedeny v tabulce 15.

Tabulka 15: Stanovené hranice pro určení přístupu k opatření (Zpracování vlastní)

Hranice pro opatření	Slovní vyjádření
0 až 4	Nízké rozdíly mezi současnou a požadovanou úrovní opatření s ohledem na prioritu. U opatření není potřeba provádět významné změny.
5 až 10	Střední rozdíly mezi současnou a požadovanou úrovní opatření s ohledem na prioritu. U opatření je vhodné provést změny.
11 a více	Velké rozdíly mezi současnou a požadovanou úrovní opatření s ohledem na prioritu. Opatření vyžaduje provedení významných změn.

Určení souhrnných výsledků a jejich interpretace

Každé opatření má přidělenou prioritu představující jeho důležitost pro společnost. K vyjádření souhrnných hodnot každé kapitoly normy ISO/IEC 27002 je proto použit vážený průměr. Nejprve je pro konkrétní kapitolu vypočten vážený průměr současné a požadované úrovně zralosti. Výsledná hodnota je pro danou kapitolu získána vynásobením rozdílu průměrné současné úrovně zralosti a průměrné požadované úrovně zralosti stanovenou prioritou pro oblast normy. Postup výpočtu a jednotlivé vzorce pro určení souhrnných údajů jsou uvedeny v následujících odstavcích.

Průměrná současná zralost opatření v kapitole normy je vypočtena pomocí vztahu:

$$\boldsymbol{WACM_j = \frac{\sum_{i=1}^{n} CM_i \cdot PM_i}{\sum_{i=1}^{n} PM_i}},$$

kde použité symboly mají následující význam:

$WACM_j$ – průměrná současná zralost opatření pro j-tou kapitolu normy,

CM_i – současná zralost i-tého opatření kapitoly normy,

PM_i – priorita i-tého opatření kapitoly normy,

n – počet přezkoumaných opatření v kapitole normy.

Výpočet průměrné požadované zralosti opatření v kapitole normy je určen vzorcem:

$$\boldsymbol{WARM_j = \frac{\sum_{i=1}^{n} RM_i \cdot PM_i}{\sum_{i=1}^{n} PM_i}},$$

kde použité symboly vyjadřují:

$WARM_j$ – průměrná požadovaná zralost opatření pro j-tou kapitolu normy,

RM_i – požadovaná zralost i-tého opatření kapitoly normy,

PM_i – priorita i-tého opatření kapitoly normy,

n – počet přezkoumaných opatření v kapitole normy.

Následně je pro každou kapitolu normy stanovena výsledná hodnota, na jejímž základě lze vymezit budoucí směrování aktivit bezpečnosti informací ve společnosti. Výsledná hodnota pro kapitoly normy je dána vzorcem:

$$\boldsymbol{RV_j = \left(WARM_j - WACM_j\right) \cdot PM_j},$$

kde použité symboly mají následující význam:

RV_j – výsledná hodnota j-té kapitoly normy,

$WARM_j$ – průměrná požadovaná zralost opatření j-té kapitoly normy,

$WACM_j$ – průměrná současná zralost opatření j-té kapitoly normy,

PM_j – stanovená priorita j-té kapitoly normy.

Ustanovení přístupu a klasifikace kapitol normy ISO/IEC 27002 vychází ze stanovených hranic uvedených v tabulce 15. Jelikož je výsledná hodnota j-té kapitoly vyjádřena jako desetinné číslo, jednotlivé hranice jsou upraveny a vystiženy pomocí intervalů, které jsou se slovním vyjádřením zobrazeny v následující tabulce.

Tabulka 16: Stanovené hranice pro určení přístupu ke kapitolám normy (Zpracování vlastní)

Hranice pro kapitolu	Slovní vyjádření
$\langle 0; 4\rangle$	Nízké rozdíly mezi současnou a požadovanou úrovní opatření v j-té kapitole s ohledem na prioritu. Opatření v kapitole nevyžadují významné změny.
$(4; 10\rangle$	Střední rozdíly mezi současnou a požadovanou úrovní opatření v j-té kapitole s ohledem na prioritu. U opatření v kapitole je vhodné provést změny.
$(10; 25\rangle$	Velké rozdíly mezi současnou a požadovanou úrovní opatření v j-té kapitole s ohledem na prioritu. Opatření v kapitole vyžadují významné změny.

Na závěr je určena celková průměrná současná způsobilost opatření podle normy ISO/IEC 27002, která je vypočtena prostřednictvím váženého průměru současné úrovně zralosti veškerých přezkoumaných opatření.

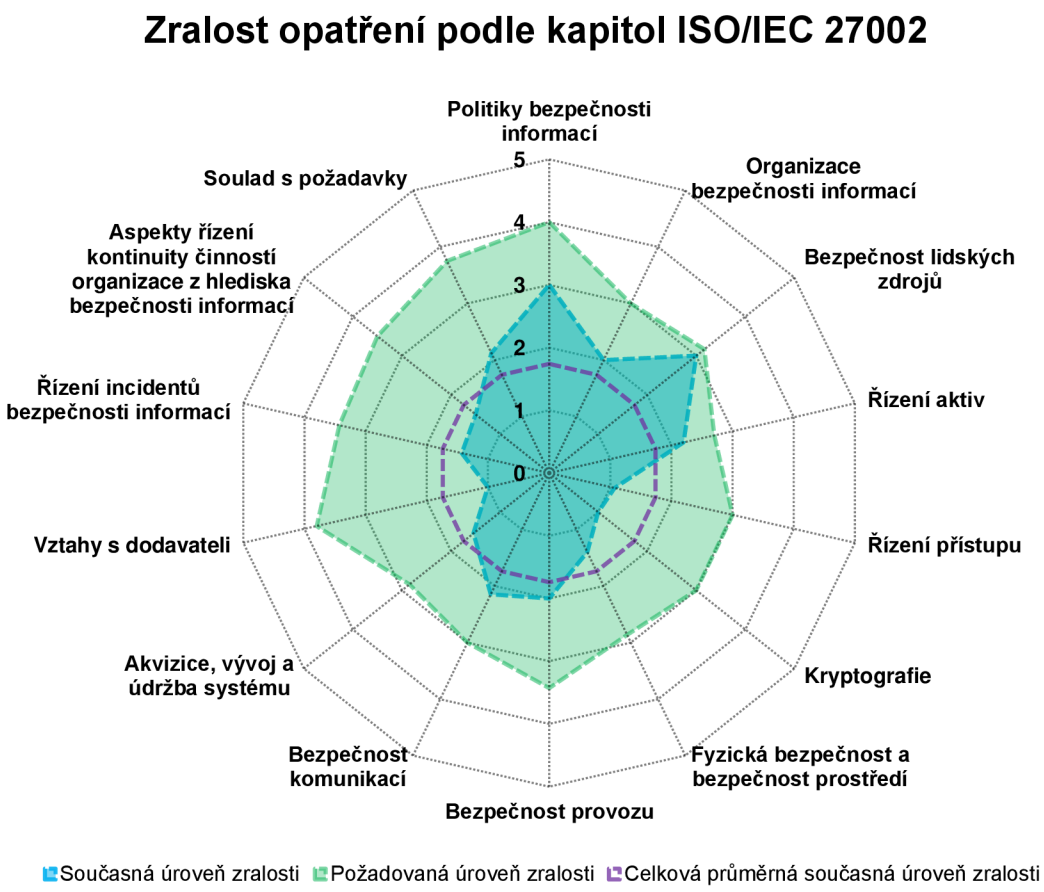
Tabulka 17 uvádí souhrnné výsledky z posouzení zralosti opatření podle jednotlivých kapitol normy ISO/IEC 27002.

Tabulka 17: Souhrnné výsledky zralostního modelu dle kapitol ISO/IEC 27002 (Zpracování vlastní)

Kapitola	Současná úroveň zralosti $WACM_j$	Požadovaná úroveň zralosti $WARM_j$	Priorita kapitoly PM_j	Výsledná hodnota RV_j
A.5 Politiky bezpečnosti informací	3,00	4,00	1	1,00
A.6 Organizace bezpečnosti informací	2,00	3,00	2	2,00
A.7 Bezpečnost lidských zdrojů	3,00	3,17	3	0,51
A.8 Řízení aktiv	2,20	2,70	3	1,50
A.9 Řízení přístupu	1,07	3,00	2	3,86
A.10 Kryptografie	1,00	3,00	2	4,00
A.11 Fyzická bezpečnost a bezpečnost prostředí	1,40	2,87	3	4,41
A.12 Bezpečnost provozu	2,00	3,43	4	5,72
A.13 Bezpečnost komunikací	2,14	3,00	3	2,58
A.14 Akvizice, vývoj a údržba systému	1,54	2,85	2	2,62
A.15 Vztahy s dodavateli	1,00	3,80	5	14,00
A.16 Řízení incidentů bezpečnosti informací	1,43	3,43	5	10,00
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	1,50	3,50	3	6,00
A.18 Soulad s požadavky	2,13	3,75	3	4,86
Celková průměrná současná zralost opatření ve společnosti podle normy ISO/IEC 27002				**1,74**

Celková průměrná současná způsobilost opatření zjištěná posouzením opatření pomocí vytvořeného zralostního modelu dosahuje hodnoty 1,74, jejíž význam lze interpretovat na základě použité stupnice pro způsobilost opatření a atributů určujících dosažení úrovně zralosti. Zavedená opatření v průměru dosahují svého účelu prováděním nezbytných činností a jsou přizpůsobována stanoveným požadavkům. Odpovědnosti a pravomoci pro oblast bezpečnosti informací jsou přiřazeny a sděleny. Při vytváření dokumentace ISMS jsou využívány přístupné zdroje a informace. Politiky a směrnice bezpečnosti informací jsou k zajištění jejich vhodnosti a přiměřenosti přezkoumávány a dány na vědomí všem relevantním zaměstnancům a třetím stranám.

Pro grafické znázornění souhrnných výsledků posouzení opatření pomocí zralostního modelu je použit pavučinový graf zachycující rozdíly mezi současnou a požadovanou úrovní zralosti pro jednotlivé kapitoly normy ISO/IEC 27002.



Obrázek 15: Současné a požadované úrovně zralosti jednotlivých kapitol normy (Zpracování vlastní)

Nejlepšího výsledku dosahuje bezpečnost lidských zdrojů. Relativně nízké rozdíly mezi současnou a požadovanou úrovní způsobilosti vykazují politiky bezpečnosti informací, organizace bezpečnosti informací, řízení aktiv a bezpečnost komunikací. Oblasti fyzická bezpečnost a bezpečnost prostředí, bezpečnost provozu, vztahy s dodavateli, řízení incidentů bezpečnosti informací, aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací a soulad s požadavky vykazující největší nedostatky v porovnání s normou ISO/IEC 27002. Pravidelným posuzováním bezpečnostních opatření je možné dosahovat neustálého zlepšování, plánování a řízení ISMS. Vyšší úroveň způsobilosti opatření nezajišťuje soulad s požadavky normy ISO/IEC 27001, legislativou a splnění podmínek pro certifikaci ISMS.

3.4 Akční plán pro ISMS společnosti

Sestavení akčního plánu vychází z provedené analýzy rizik a posouzení bezpečnostních opatření pomocí zralostního modelu. Při definici nezbytných zlepšení systému řízení bezpečnosti informací ve společnosti jsou vzaty v úvahu výsledky provedeného auditu, požadavky kybernetického zákona a koncernových směrnic GP3-19.

3.4.1 Shrnutí výsledků analýzy rizik a zralostního modelu

Analýza rizik identifikovala největší rizika a velikosti jejich dopadu v případě naplnění bezpečnostních hrozeb. Nejzávažnější riziko představuje závislost ES na dodavatelích. Identifikovaná rizika byla podle jejich hodnoty rozdělena do pěti kategorií, přičemž podstoupeno je riziko, které je klasifikováno jako bezvýznamné nebo akceptovatelné. Společnost musí přijatá rizika sledovat pro případ zvýšení jejich míry a v případě potřeby na ně včas reagovat. Sestavený akční plán by se měl zaměřovat především na rizika určená jako nežádoucí či nepřijatelná.

Posouzením bezpečnostních opatření prostřednictvím zralostního modelu byla vymezena nezbytná zlepšení pro oblast bezpečnosti informací a stanoveny priority pro následující rozvoj ISMS ve společnosti. Komplexní analýza bezpečnostních opatření může být dostatečná pro výpočet aktuální úrovně způsobilosti opatření a identifikaci dodatečných rizik. Posouzením bezpečnostních opatření byly na základě výsledné hodnoty jednotlivé kapitoly rozděleny do tří kategorií. Pozornost pro následný rozvoj ISMS by se měla zaměřit na oblasti, u nichž se vyskytují střední nebo velké rozdíly mezi současnou a požadovanou úrovní zralosti opatření s ohledem na prioritu. Některá zlepšení mohou vyžadovat finanční zdroje nebo větší změny v současných procesech. Každý nový cyklus hodnocení by měl zahrnovat přehodnocení opatření a revizi akčního plánu ISMS.

Následný akční plán systému řízení bezpečnosti informací by se měl zaměřit především na následující oblasti:

- Vztahy s dodavateli,
- Řízení incidentů bezpečnosti informací,
- Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací.

3.4.2 Akční plán ISMS

Akční plán zahrnuje bezpečnostní opatření pro snížení zjištěných nedostatků a plnění legislativních požadavků stanovených kybernetickým zákonem. Výběr a implementace technických nástrojů je součástí projektu kybernetické bezpečnosti. V následujících odstavcích jsou uvedena doporučená opatření včetně odhadu časové náročnosti.

A.6 Organizace bezpečnosti informací

Cíl: Řízení bezpečnosti informací, stanovení rolí a odpovědností za bezpečnost informací ve společnosti a definice politik mobilních zařízení.

A.6.1.5 Bezpečnost informací v řízení projektů

Bezpečnost informací je řešena v rámci projektů bez ohledu na jejich povahu. Posuzování rizik bezpečnosti informací se provádí ve všech fázích použité projektové metodiky. Odpovědnosti za bezpečnost informací jsou vymezeny a přiřazeny rolím definovaných metodami řízení projektů.

Zavedení bezpečnosti informací do řízení projektů: 7 člověkohodin.

A.6.2.1 Politika mobilních zařízení

Vytvoření a zavedení bezpečnostních pravidel pro mobilní zařízení v PIT, přičemž v každém mobilním zařízení musí být nastavena záloha dat, možnost zablokování zařízení na dálku v případě odcizení či vymazání obsahu.

Vytvoření pravidel pro mobilní zařízení v PIT: 2 člověkohodiny.

A.8 Řízení aktiv

Cíl: Identifikace a přiměřená ochrana aktiv, klasifikace a zabezpečení informací podle jejich charakteru a definice postupů bezpečné likvidace médií.

A.8.3.2 Likvidace médií

Vypracování formálního postupu pro spolehlivé smazání nebo zničení médií v souladu s klasifikací aktiv, určení odpovědností a identifikace nosičů dat vyžadujících bezpečnou likvidaci. Pro zachování auditního záznamu musí být průběh likvidace dokumentován.

Vypracování postupů bezpečné likvidace médií: 3 člověkohodiny.

A.9 Řízení přístupu

Cíl: Řízení přístupu k informacím, zařízením pro zpracování informací a oprávněných uživatelů k informačním systémům a službám. Řízení přístupu uživatelů bude vylepšeno zavedením nástroje Identity Management v rámci projektu kybernetické bezpečnosti.

A.9.1.1 Politika řízení přístupu

Stanovení přístupových pravidel a oprávnění pro každého uživatele či skupinu uživatelů zahrnující fyzický a logický přístup k zařízení s ohledem na bezpečnostní politiky. Vytvořená pravidla by měla být založena na předpokladu: Obecně je vše zakázáno, pokud to není výslovně povoleno.

Definice politiky řízení přístupu: 4 člověkohodiny.

A.9.2.5 Přezkoumání přístupových práv uživatele

Přístupová práva uživatelů musí být přezkoumávána v pravidelných intervalech nebo při změně pozice zaměstnance a pracovního poměru dle určeného procesu zahrnujícího nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích.

Přezkoumání přístupových práv uživatelů: 2 člověkohodiny.

A.9.2.6 Odebrání nebo úprava přístupových práv

Při odchodu zaměstnance je proces správy přístupových práv nastaven a funkční. Formální postup odebrání a úpravy přístupových práv musí být rovněž nadefinován při změně pracovní pozice zaměstnance.

Vymezení postupu odebrání a úpravy přístupových práv: 2 člověkohodiny.

A.9.4.3 Systém správy hesel

Při autentizaci uživatele prostřednictvím hesla musí být vyžadováno použití silného hesla s minimální délkou osm znaků a minimální složitostí zajištěnou kombinací malých a velkých písmen, číslic a speciálních znaků. Hesla musí být v pravidelných intervalech změněna. Maximální doba pro povinnou výměnu hesla nepřesahuje sto dnů. Hesla nesmí být zaznamenána na papíře nebo v nezabezpečených souborech či médiích.

Zdokumentování pravidel pro vytváření hesel: 2 člověkohodiny.

A.10 Kryptografie

Nasazení kryptografických prostředků a politika pro používání kryptografických opatření v rámci PIT je řešena v rámci projektu kybernetické bezpečnosti, a proto není součástí rozsahu diplomové práce.

A.11 Fyzická bezpečnost a bezpečnost prostředí

Cíl: Předcházení neautorizovanému přístupu, poškození a zásahu do informací a vybavení pro zpracování informací.

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Použití zařízení pro uchování a zpracování informací mimo prostory společnosti musí být schváleno managementem. Pokud je vybavení přenášeno mezi různými jednotlivci nebo externími stranami, jsou vedeny záznamy obsahující alespoň jména osob a organizace odpovědných za zařízení.

Vypracování politik pro bezpečnost aktiv mimo prostory organizace: 2 člověkohodiny.

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení

Při opakovaném použití paměťových médií je prováděna jejich kontrola z důvodu možnosti výskytu citlivých dat. Média obsahující důvěrné údaje musí být fyzicky zničena či obsažené informace vymazány nebo přepsány pomocí technik, které neumožňují obnovení původní informace. Průběh bezpečné likvidace nebo opakovaného použití zařízení je nezbytné plánovat a monitorovat.

Vytvoření postupů pro bezpečnou likvidaci nebo opakované použití: 2 člověkohodiny.

A.12 Bezpečnost provozu

Cíl: Bezpečné provozování programového vybavení a zařízení pro zpracování informací.

A.12.1.4 Princip oddělení prostředí vývoje, testování a provozu

Vývojová, testovací a provozní prostředí musí být oddělena, pravidla pro převod softwaru dokumentována a testovací prostředí popsáno. Testování nesmí být prováděno na provozních systémech. Citlivé údaje by neměly být kopírovány do testovacího systémového prostředí. Oddělení prostředí vývoje, testování a provozu je řešeno centrálně v rámci koncernových pravidel a není řešeno v diplomové práci.

A.12.3.1 Zálohování informací

Politika zálohování by měla zahrnovat požadavky organizace na zálohování informací, softwaru a systémů, na uchovávání a ochranu záloh a na postupy obnovy dat. U záložních médií musí být uskutečňovány pravidelné testy jejich čitelnosti. Mělo by být zavedeno pravidlo 3-2-1, přičemž trojka značí počet kopií, dvojka znamená umístění souborů na dvou různých typech médií a jedna ze záloh má být uložena mimo prostory společnosti.

Dokumentace zálohování informací: 2 člověkohodiny.

A.12.4.1 Zaznamenávání událostí formou logů

Činnosti uživatelů, informačních a komunikačních systémů jsou logovány na úrovni operačního systému a informační systém pro dispečerské řízení zaznamenává veškeré provozní činnosti. Monitoring v prostředí PIT bude v rámci projektu kybernetické bezpečnosti vylepšen nasazením centralizovaného sběru událostí a technologie SIEM. Záznamy formou logů musí být pravidelně přezkoumávány.

A.14 Akvizice, vývoj a údržba systému

Cíl: Bezpečnostní požadavky na informační systémy a zajištění bezpečnosti v procesech vývoje a podpory.

A.14.2.2 Postupy řízení změn systémů

Změny systémů v rámci životního cyklu vývoje jsou řízeny a kontrolovány pomocí formálních postupů řízení změn, které jsou zdokumentovány. Zavádění nových systémů a významných změn u stávajících systémů vychází ze stanoveného procesu, specifikace, testování, kontroly kvality a řízené implementace. Postupy řízení změn systémů zahrnují posouzení rizik, analýzu dopadů změn a určení nutných opatření v oblasti bezpečnosti.

Vytvoření postupů pro řízení změn systémů: 3 člověkohodiny.

A.15 Vztahy s dodavateli

Cíl: Zabezpečit ochranu aktiv přístupných dodavatelům a udržovat bezpečnost informací v rámci dodavatelského řetězce, splnění požadavků kybernetického zákona, směrnic GDPR a NIS.

A.15.1.1 Politika bezpečnosti informací pro oblast vztahů s dodavateli

Oblast vztahů s dodavateli určuje opatření pro bezpečnost informací a řízení přístupu dodavatelů k informacím a aktivům společnosti. Politika by měla stanovovat pravidla pro hodnocení dodavatelů, provádění posouzení rizik plynoucích ze vztahů s dodavateli před uzavřením smlouvy, definici požadavků pro řešení bezpečnosti informací v rámci smluv, typy dodavatelů, kterým je umožněn přístup k informacím, a druhy přístupů, jež jsou povoleny různým dodavatelům. Po dodavateli může být vyžadována implementace bezpečnostních opatření.

Vypracování politiky bezpečnosti informací pro vztahy s dodavateli: 4 člověkohodiny.

A.15.1.2 Řešení bezpečnosti v rámci smluv s dodavateli

Ustanovení o bezpečnosti informací musí být zařazena do smluv s dodavateli, které obsahují popis a metody poskytnutých nebo zpřístupněných informací a klasifikaci informací podle klasifikačního schématu společnosti. Nadále musí být určen explicitní seznam pracovníků dodavatele s autorizovaným přístupem k aktivům a informacím společnosti. Smlouvy s dodavateli vymezují požadavky na řízení, oznámení a spolupráci při nápravě incidentů, povinnosti zavést dohodnutý soubor technických a organizačních opatření, vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření a zajištění potřebné důvěrnosti dat v celém dodavatelském řetězci.

Stanovení požadavků bezpečnosti informací ve smlouvách s dodavateli: 4 člověkohodiny.

A.15.1.3 Řetězec dodavatelů informačních a komunikačních technologií

Smlouvy s dodavateli zahrnují požadavky z oblasti bezpečnosti informací pro celý řetězec dodavatelů účastnící se dodávky služeb informačních a komunikačních technologií. Společnost vyžaduje zavedení technických, organizačních a procesních bezpečnostních opatření v rámci celého dodavatelského řetězce, zajištění důvěrnosti dat a oznamování bezpečnostních incidentů spojených s únikem dat. Ve smlouvách s dodavateli je zaveden proces identifikace komponent produktů nebo služeb zajištěných subdodavateli.

Dokumentace požadavků pro řetězec dodavatelů: 3 člověkohodiny.

A.15.2.1 Monitorování a přezkoumání služeb dodavatelů

Společnost musí pravidelně monitorovat a přezkoumávat udržování dohodnuté úrovně bezpečnosti informaci a dodávky služeb ve shodě s dodavatelskými dohodami. Proces řízení služeb by měl zahrnovat:

- Sledování úrovně služeb,
- Přezkoumání požadavků na bezpečnost informací a zajištění potřebné důvěrnosti dat v dodavatelském řetězci,
- Přezkoumání a hlášení zpráv o událostech a incidentech bezpečnosti informací,
- Přezkoumání auditních záznamů dodavatelů.

Provádění auditů u dodavatelů: 120 člověkohodin.

A.16 Řízení incidentů bezpečnosti informací

Cíl: Vytvoření efektivního přístupu k řízení incidentů zahrnujícího komunikaci ohledně bezpečnostních událostí a slabých míst.

A.16.1.4 Posuzování a rozhodování o událostech bezpečnosti informací

Opatření posuzování a rozhodování o událostech bezpečnosti informací bude zlepšeno implementací centralizovaného sběru událostí a technologie SIEM, které jsou součástí projektu kybernetické bezpečnosti. Výstupy ze systému SIEM jsou nezbytné pro splnění kybernetického zákona a směrnice NIS. Nadále je nutné vypracovat dokument pro řízení bezpečnostních událostí a incidentů s klasifikační stupnicí pro události a incidenty bezpečnosti informací.

A.16.1.6 Ponaučení z incidentů bezpečnosti informací

Zkušenosti získané při řešení bezpečnostních incidentů musí být zahrnuty do systému řízení bezpečnosti informací. Způsob využití znalostí z řešení incidentů bezpečnosti informací bude v rámci projektu kybernetické bezpečnosti vylepšen implementací systému SIEM, čímž se splní požadavek kybernetického zákona na využívání informací ke zlepšování zavedených bezpečnostních opatření v kritické informační infrastruktuře. Získané znalosti budou použity ke snížení pravděpodobnosti či dopadu budoucích incidentů.

A.16.1.7 Shromažďování důkazů

Stanovení interních postupů pro identifikaci, shromažďování, získávání a uchovávání informací, které mohou sloužit jako důkazy. Nashromážděné důkazy se musí uchovávat po dobu 18 měsíců.

Vývoj postupů pro zacházení s důkazy: 2 člověkohodiny.

A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

Cíl: Zajištění kontinuity činností organizace za nepříznivých situací a katastrof.

A.17.1.2 Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací

Společnost musí ověřovat definované plány kontinuity v pravidelných intervalech na základě testování funkčnosti procesů, postupů a opatření. Platnost a efektivnost kontinuity činností je přezkoumávána i v případě změn informačních systémů, procesů, postupů a opatření. V případě výpadků, poruch či opětovného spuštění systémů by měly plány kontinuity zahrnovat komunikaci s dodavatelem.

Přezkoumávání plánů kontinuity realizovat periodicky podle stanoveného plánu.

3.4.3 Ekonomické zhodnocení

Náklady na akční plán zahrnují především dokumentaci a zavedení politik bezpečnosti informací vyžadovaných kybernetickým zákonem. Legislativa dále požaduje pravidelné provádění auditů u dodavatelů, které vzhledem k počtu uzavřených smluv představují výraznou časovou zátěž pro společnost. Mzda zaměstnance pracujícího na zavádění a revizi opatření je stanovena na 400 Kč za člověkohodinu. Jednorázový časový fond na zavedení opatření je odhadnut na 164 člověkohodin při celkových nákladech 65 600 Kč.

Každý rok musí být proveden interní audit bezpečnosti informací, jehož doba trvání je odhadnuta na 50 člověkohodin s náklady 50 000 Kč. Do kalkulace nákladů je zahrnuta každoroční revize opatření a uskutečňování auditů u dodavatelů s přibližnou časovou náročností 134 člověkohodin a celkovými ročními náklady 53 600 Kč.

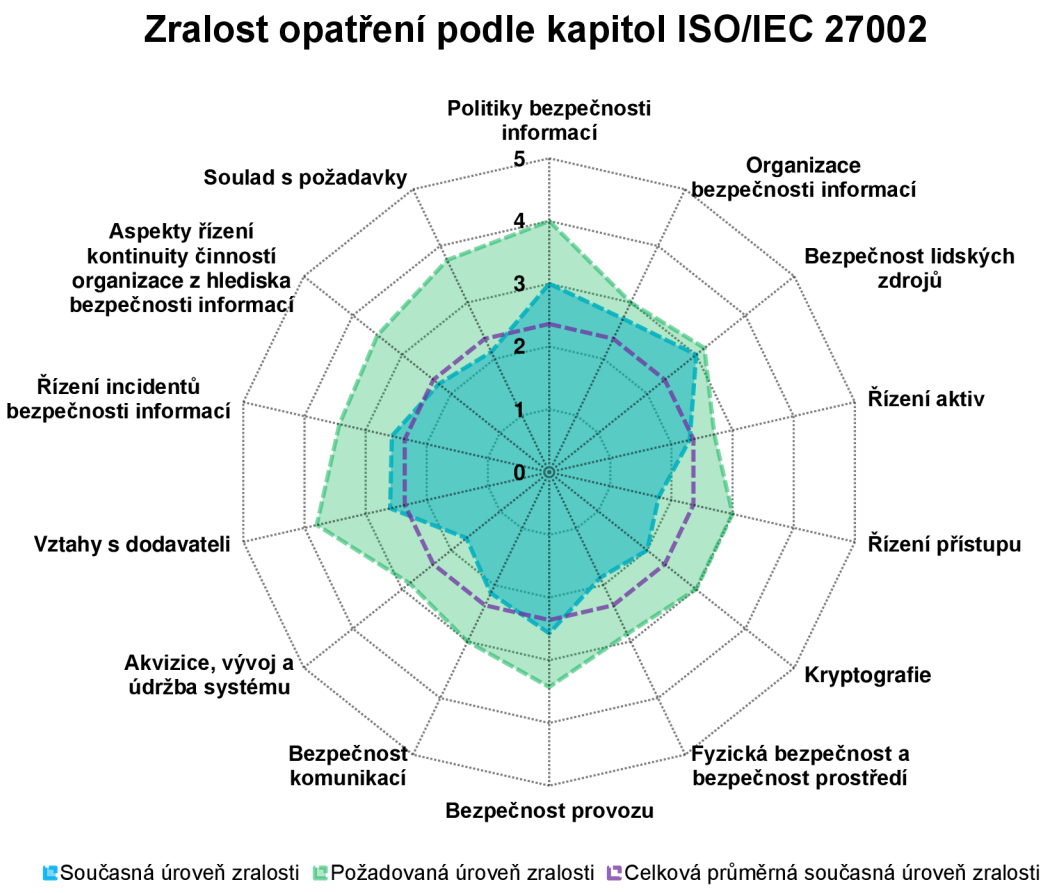
Ekonomické zhodnocení neobsahuje náklady na zavedení nástrojů, které jsou součástí projektu kybernetické bezpečnosti. Implementace technických opatření bude vyžadovat investice, čímž se celkové náklady na realizaci akčního plánu výrazně navýší.

Tabulka 18: Ekonomické zhodnocení akčního plánu (Zpracování vlastní)

Položka	Jednorázové náklady	Roční náklady
Zavedení opatření	65 600 Kč	-
Údržba a zlepšování opatření, audit u dodavatelů	-	53 600 Kč
Interní audit	-	50 000 Kč
Celkem	**65 600 Kč**	**103 600 Kč**

Výše investic energetické společnosti do bezpečnostních opatření a technických nástrojů je v porovnání s možnými ztrátami a udělenými sankcemi za nesplnění legislativních požadavků minimální.

Následující obrázek zachycuje odhadovanou úroveň současné způsobilosti kapitol normy ISO/IEC 27002 po realizaci akčního plánu. Průměrná současná zralost opatření vzroste přibližně na hodnotu 2,36, přičemž v oblastech s největšími nedostatky se sníží rozdíly mezi současnou a požadovanou úrovní způsobilosti.



Obrázek 16: Současné a požadované úrovně zralosti po realizaci akčního plánu (Zpracování vlastní)

3.5 Návrh metrik pro stanovení efektivity a efektivnosti ISMS

Metriky monitorují a měří výkonnost bezpečnostních procesů a zavedených opatření, čímž představují východisko při řízení a zlepšování ISMS. Získané kvantitativní údaje identifikují neúčinná opatření, podporují odůvodnění zamyšlených výdajů do bezpečnosti informací, umožňují určit priority budoucího rozvoje ISMS a ověřují rozsah plnění externích a interních požadavků. Vývoj metrik pro stanovení efektivity a efektivnosti ISMS je neustále se opakující proces, který vyžaduje pravidelnou revizi v reakci na změny stanovených cílů a informačních potřeb.

Při sestavování programu měření ISMS lze vycházet z normy ISO/IEC 27004, která pro používání metrik doporučuje následující postup (22):

- Vývoj metrik a měření,
- Provádění měření,
- Analýza dat a hlášení výsledků,
- Vyhodnocení a zlepšování programu měření (22).

Výběr metrik pro společnost vychází z dostupnosti lidských zdrojů, informačních potřeb bezpečnostních pracovníků a technických nástrojů na sběr přesných dat. Počáteční rozsah měření je omezen na opatření a činnosti s vysokou prioritou v rámci PIT. Rovněž jsou zahrnuty i vybrané oblasti, u kterých byly prostřednictvím analýzy rizik a zralostního modelu zjištěny významné nedostatky. S ohledem na zájmy zainteresovaných stran by bylo vhodné s rozvojem ISMS rozšířit stanovený kontext z důvodu možnosti sledovat významné činitele v oblasti bezpečnosti informací.

Základem při tvorbě souboru metrik a poskytnutí obecného přehledu je určení důležitých bezpečnostních procesů a jednotlivých skupin opatření. Oblasti měření jsou vybrány s ohledem na úroveň zavedeného ISMS ve společnosti. Zpočátku je vhodné stanovit menší počet ukazatelů, který se při následném rozvoji ISMS bude nadále rozšiřovat.

Pro zjištění účinnosti systému řízení bezpečnosti informací je navrženo šest oblastí, do nichž jsou jednotlivé ukazatelé roztříděny. Tabulka 19 uvádí monitorované procesy či skupiny opatření ISMS a účel měření s důvody pro zavedení měření. Charakteristika vybraných ukazatelů je uvedena v další části kapitoly.

Tabulka 19: Přehled procesů a skupin opatření ISMS s účelem měření (Zpracování vlastní)

Proces / Skupina opatření	Účel měření
Řízení incidentů bezpečnosti informací	Ohodnocení účinnosti řízení incidentů bezpečnosti informací, zvládání rizik a implementace bezpečnostních opatření
Školení ISMS	Vyhodnocení shody s požadavkem na školení a zvyšování povědomí bezpečnosti informací u zaměstnanců
Posuzování a zvládání rizik	Určení rozsahu analýzy a hodnocení rizik u významných informačních aktiv společnosti
Plánování kontinuity	Analýza úrovně řízení kontinuity činnosti se zaměřením na dokumentaci a přezkoumání plánů kontinuity
Zlepšování ISMS	Sledování zjištěných nedostatků při provedených interních a externích auditech ISMS
Řešení bezpečnosti v rámci smluv s dodavateli	Zachování bezpečnosti informací a prostředků zpracování informací, ke kterým mohou přistupovat externí subjekty

3.5.1 Popis metrik

Šablona pro definování metrik bezpečnosti informací vychází z normy ISO/IEC 27004 a obsahuje nejvýznamnější atributy, které lze podle preferencí a potřeb zainteresovaných stran rozšířit. Součástí každého ukazatele je i popis indikátoru zahrnující analytický model, rozhodovací kritéria a formu hlášení.

Analytický model kombinuje metriky pro přiřazení hodnoty k indikátoru a vytvoření dostatečně vypovídajícího výstupu pro zainteresované strany. U každému indikátoru jsou stanovena rozhodovací kritéria pojednávající o pokroku a prahových úrovních k zahájení činností zlepšování ISMS. Určená kritéria poskytují návod pro interpretaci indikátoru a forma hlášení umožňuje názorně prezentovat metriky.

a) Řízení incidentů bezpečnosti informací

Při řízení incidentů bezpečnosti informací je potřeba zajistit důsledný a efektivní přístup zahrnující komunikaci ohledně bezpečnostních událostí a slabých míst ve společnosti. Výsledky z řešení a výskytů incidentů musí být pro komplexní porozumění trendů a vzorů analyzovány, sledovány a pravidelně kontrolovány. Ponaučením z incidentů bezpečnosti informací je možné omezit dopad na výkonnost a běžný provoz společnosti. V kombinaci s dalšími metrikami lze vyhodnocovat úroveň ohrožení, účinnost bezpečnostních opatření nebo schopnost detekce incidentů.

Počet incidentů bezpečnosti informací

Počet incidentů udává množství zjištěných bezpečnostních incidentů během časového období. Ukazatel lze použít k získání přehledu o relativní úrovni ISMS v jednotlivých obchodních jednotkách. Cílem je minimalizovat hodnotu metriky, avšak nízký počet incidentů může indikovat nedostatečnou způsobilost detekce incidentů. Metrika může rovněž určovat účinnost zavedených bezpečnostních opatření ve společnosti.

Tabulka 20: Počet incidentů bezpečnosti informací (Zpracování vlastní)

Název metriky	**Počet incidentů bezpečnosti informací**
Význam	Metrika určuje počet bezpečnostních incidentů zjištěných za časové období
Funkce měření	$Y = \sum_{i=1}^{n} A_i$ A_i – počet incidentů bezpečnosti informací i-tý den n – počet dní za dané časové období
Měrná jednotka	Počet incidentů za časové období
Typ měřítka	Kardinální
Interpretace hodnot	Minimalizace
Zdroj dat	Hlášení incidentů bezpečnosti informací, logy operačního systému, logy antivirového programu
Vlastník	Manažeři odpovědní za ISMS, vedení společnosti
Odpovědnost za sběr dat	Pracovníci bezpečnosti
Frekvence sběru dat	Měsíčně
Frekvence hlášení	Měsíčně
Popis indikátoru	
Indikátor	Sloupcový graf zobrazující tempo přírůstku (Y) ukazatele v časovém období s konstantní vodorovnou čárou znázorňující průměrné tempo přírůstku ($\bar{Y}$) za více period hlášení
Analytický model	$Y = \left(\frac{A_i}{A_{i-1}} - 1\right) \cdot 100\ [\%]$ $\bar{Y} = \left(\sqrt[n-1]{\prod_{i=2}^{n} \frac{A_i}{A_{i-1}}} - 1\right) \cdot 100\ [\%]$ A_i – počet incidentů v i-tém časovém období A_{i-1} – počet incidentů v předcházejícím časovém období n – počet period hlášení výsledků
Rozhodovací kritéria	Červená $Y \geq 20$ – vyžadováno přezkoumání příčin nárůstu počtu incidentů, je-li červená pro více period hlášení, je nezbytné opatření k nápravě Žlutá $0 \leq Y < 20$ – vyžadováno monitorování trendu ukazatele, pokud se hodnoty nezlepšují, je zahájeno přezkoumání Zelená $Y < 0$ – není požadována žádná akce
Forma hlášení	Sloupcový graf s barevnými sloupci na základě rozhodovacích kritérií doplněný o možná opatření a komentáře k vývoji hodnot

Pro dosažení vyšší informační hodnoty ukazatele a identifikaci oblastí s nedostatečně účinnými opatřeními je vhodné bezpečnostní incidenty klasifikovat. Realizace měření s kategorizací počtu incidentů závisí na zvážení společnosti a dostupnosti technických nástrojů umožňujících snadný sběr dat. Počet incidentů je možné rozčlenit podle původu, závažnosti, zneužitých zranitelností či rozsahu kompromitovaných informací.

Za současných podmínek ve společnosti lze doporučit vytvoření hierarchie ukazatele počtu incidentů rozdělených nejprve podle původu na interní, externí a dodavatel. Druhá úroveň zahrne podrobnější dělení podle dopadu na základě rozsahu narušení nebo ztráty důvěrnosti, dostupnosti či integrity dat a způsobené finanční újmy. Interpretace výsledků, použitý indikátor, rozhodovací kritéria a forma hlášení by byly pro každou skupinu v souladu s popisem ukazatele uvedeného výše. K prezentaci dat se použije výsečový graf zachycující procentuální podíl kategorie na celkovém počtu bezpečnostních incidentů. Na základě porovnání s historickými informacemi lze sledovat změny struktury počtu incidentů podle původu či dopadu a vyhodnocovat účinnost implementovaných opatření.

b) Školení ISMS

Jednou z největších hrozeb bezpečnosti informací je nevyškolený uživatel. Zavedením pravidelně se opakujícího školení se zaměřením na zvyšování bezpečnostního povědomí a obeznámením zaměstnanců s bezpečnostními politikami a zásadami je možné zvýšit ochranu významných aktiv společnosti, snižovat riziko vzniku lidské chyby a omezit počet bezpečnostních incidentů. Uvedené metriky hodnotí rozsah školení ISMS u osob zastávajících bezpečnostní role a provádění zvyšování povědomí o bezpečnosti informací u všech zaměstnanců společnosti. Ukazatel lze použít pro sledování školení ISMS nebo kybernetické bezpečnosti v souladu s ročním plánem.

Procento vyškoleného personálu ISMS

Společnost musí u pracovníků zastávajících bezpečnostní role zajistit jejich vzdělávání pro vykonávání požadovaných úkolů formou pravidelného školení. Odborně způsobilí zaměstnanci jsou předpokladem pro efektivní řízení a správu ISMS ve společnosti. Vysoká hodnota ukazatele vyjadřuje zvyšování kvalifikace personálu odpovědného za ISMS v souladu s ročním plánem. Naopak s poklesem hodnoty se zvyšuje riziko neadekvátního neporozumění bezpečnostním politikám a příslušným povinnostem při ochraně aktiv organizace.

Tabulka 21: Procento vyškoleného personálu ISMS (Upraveno dle: 22)

Název metriky	Procento vyškoleného personálu ISMS
Význam	Udává procento personálu ISMS, kteří absolvovali školení bezpečnosti informací v souladu s ročním plánem školení
Funkce měření	$Y = (A/B) \cdot 100$ A – počet personálu ISMS, kteří se zúčastnili školení ISMS v souladu s ročním plánem školení ISMS B – počet personálu ISMS, kteří se měli zúčastnit školení
Měrná jednotka	Procento [%]
Typ měřítka	Poměrové
Interpretace hodnot	Maximalizace, cílová hodnota 95 %
Zdroj dat	Záznamy školení ISMS, plán školení ISMS
Vlastník metriky	Manažeři odpovědní za ISMS
Odpovědnost za sběr dat	Pracovník odpovědný za školení ISMS
Frekvence sběru dat	Měsíčně
Frekvence hlášení	Čtvrtletně
Popis indikátoru	
Indikátor	Sloupcový graf zobrazující shodu po několik period hlášení ve vztahu k prahovým hodnotám (červená, žlutá, zelená) definovaných v analytickém modelu.
Analytický model	0–60 % červená, 60–90 % žlutá, 90–100 % zelená Pokud pro žlutou prahovou hodnotu nebylo za čtvrtletí dosaženo pokroku alespoň 10 %, ohodnocení je automaticky červené
Rozhodovací kritéria	Červená – je zapotřebí intervence a provedení analýzy příčin Žlutá – sledování indikátoru pro možný posun do červené Zelená – není vyžadováno žádné opatření
Forma hlášení	Sloupcový graf s barevnými sloupci na základě rozhodovacích kritérií doplněný o význam metriky a možná opatření

Procento zaměstnanců, kteří absolvovali pravidelné školení ISMS

Metrika vyhodnocuje plnění požadavku na pravidelně se opakující školení a zvyšování povědomí o bezpečnosti informací a zavedených politikách zaměstnanců společnosti. S rostoucí úrovní ukazatele se zvyšuje informovanost zaměstnanců o potencionálních hrozbách, jejich povinnostech a odpovědnostech při dodržování bezpečnostních politik či směrnic. Pokud společnost nerealizuje pravidelná školení ISMS u všech pracovníků s ohledem na jejich pracovní pozici, vzroste míra rizika porušení definovaných pravidel a vzniku lidské chyby, bezpečnostního incidentu či události.

Tabulka 22: Procento zaměstnanců, kteří absolvovali pravidelné školení ISMS (Upraveno dle: 22)

Název metriky	Procento zaměstnanců, kteří absolvovali pravidelné školení ISMS
Význam	Vyhodnocení shody požadavku na roční školení zvyšování povědomí o bezpečnosti informací u zaměstnanců společnosti
Funkce měření	$Y = (A/B) \cdot 100$ A – počet zaměstnanců, kteří se zúčastnili ročního školení zvyšování povědomí bezpečnosti informací B – počet zaměstnanců, kteří se mají zúčastnit ročního školení zvyšování povědomí bezpečnosti informací
Měrná jednotka	Procento [%]
Typ měřítka	Poměrové
Interpretace hodnot	Maximalizace, cílová hodnota 95 %
Zdroj dat	Záznamy školení ISMS, plán školení ISMS
Vlastník	Manažeři odpovědní za ISMS, vedení společnosti
Odpovědnost za sběr dat	Pracovník odpovědný za školení ISMS
Frekvence sběru dat	Měsíčně
Frekvence hlášení	Čtvrtletně
Popis indikátoru	
Indikátor	Sloupcový graf zobrazující shodu po několik period hlášení ve vztahu k prahovým hodnotám (červená, žlutá, zelená) definovaných v analytickém modelu
Analytický model	0–60 % červená, 60–90 % žlutá, 90–100 % zelená Pokud pro žlutou prahovou hodnotu nebylo za čtvrtletí dosaženo pokroku alespoň 10 %, ohodnocení je automaticky červené
Rozhodovací kritéria	Červená – je zapotřebí intervence a provedení analýzy příčin Žlutá – sledování indikátoru pro možný posun do červené Zelená – není vyžadováno žádné opatření
Forma hlášení	Sloupcový graf s barevnými sloupci na základě rozhodovacích kritérií doplněný o význam metriky a možná opatření

c) Posuzování a zvládání rizik

Proces posouzení a zvládání rizik významně ovlivňuje efektivitu ISMS, neboť na základě výsledků hodnocení rizik jsou pro snížení míry rizika zavedena bezpečnostní opatření.

Procento ICT systémů, u nichž bylo provedeno hodnocení rizik

Účelem metriky je sledování rozsahu a postupu analýzy a hodnocení rizik u ICT systémů ve společnosti. Stanovený podíl ICT systémů, u nichž bylo provedeno hodnocení rizik, vůči celkovému množství ICT systémů umožňuje vyhodnotit úroveň neznámého rizika pro informační a komunikační technologie v produkčním prostředí společnosti. Hodnoty ukazatele by měly být v čase rostoucí.

Tabulka 23: Procento ICT systémů, u nichž bylo provedeno hodnocení rizik (Zpracování vlastní)

Název metriky	Procento ICT systémů, u nichž bylo provedeno hodnocení rizik
Význam	Podíl ICT systémů zahrnutých do procesu řízení rizik
Funkce měření	$Y = (A/B) \cdot 100$ A – počet ICT systémů, u nichž bylo provedeno hodnocení rizik B – celkový počet ICT systémů ve stanoveném rozsahu ISMS
Měrná jednotka	Procento [%]
Typ měřítka	Poměrové
Interpretace hodnot	Maximalizace
Zdroj dat	Analýza a řízení rizik ISMS
Vlastník	Manažeři odpovědní za ISMS, vedení společnosti
Odpovědnost za sběr dat	Oddělení řízení rizik
Frekvence sběru dat	Čtvrtletně
Frekvence hlášení	Ročně
Popis indikátoru	
Indikátor	Trend podílu ICT systémů zahrnutých do procesu řízení rizik
Analytický model	Porovnání současného poměru s předcházejícími hodnotami za více časových období
Rozhodovací kritéria	Výsledný trend by měl být v čase rostoucí
Forma hlášení	Výsečový graf zobrazující podíl ICT systémů zahrnutých do procesu řízení rizik vůči celkovému počtu ICT systému

d) Plánování kontinuity

Plánování kontinuity umožňuje v reakci na incidenty stanovit postupy obnovy klíčových procesů společnosti na minimální úroveň. Plány kontinuity by měly být dokumentovány, pravidelně testovány a revidovány. Absence plánů kontinuity vyjadřuje relativní míru rizika pro chod a výkonnost společnosti během nepříznivé situace.

Procento plánů kontinuity s revizí ve stanoveném intervalu

U plánů kontinuity je potřeba pravidelně ověřovat zavedená opatření kontinuity, aby byla zajištěna jejich platnost a účinnost během nepříznivých situací. Metrika vyjadřuje podíl plánů kontinuity s revizí ve stanoveném intervalu vůči celkovému počtu plánů kontinuity a lze ji použít pro vyhodnocování úrovně provádění přezkoumání vytvořených plánů a efektivnosti řízení kontinuity činností.

Tabulka 24: Procento plánů kontinuity s revizí ve stanoveném intervalu (Zpracování vlastní)

Název metriky	Procento plánů kontinuity s revizí ve stanoveném intervalu
Význam	Vyhodnocení revize plánů kontinuity ve stanoveném intervalu
Funkce měření	$Y = (A/B) \cdot 100$ A – počet plánů kontinuity s revizí ve stanoveném intervalu B – celkový počet dokumentovaných plánů kontinuity
Měrná jednotka	Procento [%]
Typ měřítka	Poměrové
Interpretace hodnot	Maximalizace
Zdroj dat	Plány kontinuity
Vlastník	Manažeři odpovědní za ISMS, management společnosti
Odpovědnost za sběr dat	Pracovníci ISMS
Frekvence sběru dat	Ročně
Frekvence hlášení	Ročně
Popis indikátoru	
Indikátor	Sloupcový graf zobrazující shodu po několik period hlášení ve vztahu k prahovým hodnotám (červená, žlutá, zelená) definovaných v analytickém modelu
Analytický model	0–80 % červená, 80–95 % žlutá, 95–100 % zelená Pokud pro žlutou prahovou hodnotu nebylo meziročně dosaženo pokroku alespoň 5 %, ohodnocení je automaticky červené
Rozhodovací kritéria	Červená – přezkoumání příčin neprovádění revizí plánů kontinuity podle stanoveného harmonogramu Žlutá – vyžadováno monitorování, pokud se trend nezlepšuje, je zahájeno přezkoumání Zelená – není požadována žádná akce
Forma hlášení	Sloupcový graf s barevnými sloupci na základě rozhodovacích kritérií doplněný o možná opatření a komentáře k vývoji hodnot

Procento významných ICT systémů s plánem kontinuity

Metrika určuje podíl informačních a komunikačních technologií, pro něž jsou stanoveny plány kontinuity. Hodnoty ukazatele indikují připravenost společnosti na katastrofy či krizové stavy, redukovat relativní míru rizika související s výskytem nežádoucí situace a schopnost předcházet haváriím. Kontinuita činností může zajistit důvěru ve vztazích organizace se zákazníky či obchodními partnery a vyhodnocení její implementace a řízení představuje pro společnost jednu z klíčových oblastí ke splnění legislativních požadavků stanovených kybernetickým zákonem.

Tabulka 25: Procento významných ICT systémů s plánem kontinuity (Zpracování vlastní)

Název metriky	Procento významných ICT systémů s plánem kontinuity
Význam	Stanovení rozsahu plánů kontinuity pro významné ICT systémy
Funkce měření	$Y = (A/B) \cdot 100$ A – počet dokumentovaných plánů kontinuity pro významné ICT systémy B – celkový počet významných ICT systémů
Měrná jednotka	Procento [%]
Typ měřítka	Poměrové
Interpretace hodnot	Maximalizace
Zdroj dat	Plány kontinuity
Vlastník	Manažeři odpovědní za ISMS, management společnosti
Odpovědnost za sběr dat	Garant aktiva, pracovníci ISMS
Frekvence sběru dat	Ročně
Frekvence hlášení	Ročně
Popis indikátoru	
Indikátor	Sloupcový graf zobrazující shodu po několik period hlášení ve vztahu k prahovým hodnotám (červená, žlutá, zelená) definovaných v analytickém modelu
Analytický model	0–80 % červená, 80–95 % žlutá, 95–100 % zelená Pokud pro žlutou prahovou hodnotu nebylo meziročně dosaženo pokroku alespoň 5 %, ohodnocení je automaticky červené
Rozhodovací kritéria	Červená – přezkoumání příčin nevytváření plánů kontinuity u významných ICT systémů Žlutá – vyžadováno monitorování, pokud se trend nezlepšuje, je zahájeno přezkoumání Zelená – není požadována žádná akce
Forma hlášení	Sloupcový graf s barevnými sloupci na základě rozhodovacích kritérií doplněný o možná opatření a komentáře k vývoji hodnot

Míra redundance u významných ICT systémů

Ukazatel vyhodnocuje míru redundance u významných informačních a komunikačních prvků nacházejících se v PIT a vyjadřuje množství ICT systémů, které mohou selhat bez ovlivnění sítě jako celku. Cílem redundance je zmírnit riziko nedostupnosti systémů při výpadcích a zajistit kontinuitu jejich provozu pomocí okamžité reakce a omezení vlivů selhání zařízení na činnost společnosti. Vysoká hodnota metriky vyjadřuje odolnost infrastruktury proti chybám při zachování služeb na přijatelné úrovni.

Tabulka 26: Míra redundance u významných ICT systémů (Zpracování vlastní)

Název metriky	Míra redundance u významných ICT systémů
Význam	Vyhodnocuje zajištění dostupnosti ICT systémů pomocí redundance v PIT
Funkce měření	$Y = (A/B) \cdot 100$ A – počet redundantních významných ICT systémů B – celkový počet významných ICT systémů a zařízení
Měrná jednotka	Procento [%]
Typ měřítka	Poměrové
Interpretace hodnot	Maximalizace
Zdroj dat	Provozní a síťová dokumentace
Vlastník	Manažeři odpovědní za ISMS, management společnosti
Odpovědnost za sběr dat	Garanti aktiv, síťový administrátor
Frekvence sběru dat	Čtvrtletně
Frekvence hlášení	Ročně
Popis indikátoru	
Indikátor	Trend míry redundance významných ICT systému
Analytický model	Porovnání současné míry redundance významných ICT systémů s předchozími hodnotami za více časových období
Rozhodovací kritéria	Výsledný trend by měl být v čase rostoucí
Forma hlášení	Spojnicový graf zobrazující míru redundance významných ICT systémů

e) Zlepšování ISMS

Účelem měření je sledování zjištěných nedostatků při auditech ISMS, na jejichž základě je učiněna aktualizace systému řízení bezpečnosti informací a příslušné dokumentace, čímž je zvyšována celková účinnost ISMS.

Zjištěné nedostatky auditů ISMS

Měření lze provádět individuálně pro interní, externí a kybernetické audity nebo společně pro interní a externí audity ISMS. Metrika udává průměrný počet zjištěných nedostatků při auditech ISMS provedených za poslední rok. Pro srovnatelnost měření musí být audity prováděny za použití konzistentních standardů a postupů. Čím nižší je získaná hodnota ukazatele při zachování stejného rozsahu přehodnocení ISMS, tím méně nedostatků bylo zjištěno. Zjištěné nedostatky je vhodné rozdělit podle statusu do kategorií nový, vyřešený, otevřený a nedořešený.

Tabulka 27: Zjištěné nedostatky auditů ISMS (Zpracování vlastní)

Název metriky	Zjištěné nedostatky auditů ISMS
Význam	Sledování zjištěných nedostatků při auditech ISMS pro stanovený rozsah
Funkce měření	$Y = \sum_{i=1}^{n} \frac{A_i}{n}$ A_i – počet zjištěných nedostatků při i-tém auditu n – počet auditů za posledních 12 měsíců
Měrná jednotka	Procento [%]
Typ měřítka	Poměrové
Interpretace hodnot	Minimalizace
Zdroj dat	Záznamy z auditů
Vlastník	Manažeři odpovědní za ISMS
Odpovědnost za sběr dat	Interní audit, pracovníci ISMS
Frekvence sběru dat	Ročně
Frekvence hlášení	Ročně
Popis indikátoru	
Indikátor	1 Trend zjištěných nedostatků auditů ISMS 2 Trendy poměrů vůči celkovému počtu zjištěných nedostatků rozdělených podle statusu: 1. kategorie: Nový 2. kategorie: Vyřešený 3. kategorie: Otevřený 4. kategorie: Nedořešený
Analytický model	1 Porovná se stav zjištěných nedostatků auditů ISMS s předchozím stavem 2 Pro jednotlivé kategorie se porovná současný počet zjištěných nedostatků auditů ISMS s předchozí hodnotou za více časových období
Rozhodovací kritéria	1 Výsledný trend by měl být v čase klesající 2 Nový – výsledný trend by měl být v čase klesající, Vyřešený – trend by měl být v čase rostoucí, Otevřený – výsledný trend by měl být v čase klesající, Nedořešený – výsledný trend by měl být v čase klesající
Forma hlášení	1 Spojnicový graf zobrazující zjištěné nedostatky auditů 2 Skupinový sloupcový graf pro kategorie přes více period hlášení s komentáři k nedostatkům se statusem nový, otevřený, nedořešeno

f) Řešení bezpečnosti v rámci smluv s dodavateli

Východiskem při řízení rizik bezpečnosti informací v rámci dodavatelských vztahů jsou uzavřené smlouvy obsahující relevantní požadavky na bezpečnost a právo na audit. Každý dodavatel, jenž poskytuje komponenty do IT infrastruktury či může přistupovat, zpracovávat a přenášet informace společnosti, by měl odsouhlasit a dodržovat stanovené bezpečnostní požadavky.

Smlouvy s dodavateli obsahující klauzule bezpečnosti informací

Ukazatel vyhodnocuje požadavek na zachování bezpečnosti informací a prostředků pro zpracování informací, které jsou přístupné, zpracovávané či spravované externími subjekty. Pro vývoj hodnot ukazatele je žádoucí rostoucí trend, který naznačuje zvýšenou úroveň řízení rizik bezpečnosti informací v rámci dodavatelských vztahů.

Tabulka 28: Smlouvy s dodavateli obsahující klauzule bezpečnosti informací (Zpracování vlastní)

Název metriky	**Smlouvy s dodavateli obsahující klauzule bezpečnosti informací**
Význam	Ohodnocení míry zohlednění bezpečnosti ve smlouvách s dodavateli
Funkce měření	$Y = (A/B) \cdot 100$ A – počet smluv s dodavateli pokrývající veškeré relevantní bezpečnostní požadavky B – celkový počet smluv s dodavateli
Měrná jednotka	Procento [%]
Typ měřítka	Poměrové
Interpretace hodnot	Maximalizace
Zdroj dat	Dohody s dodavateli
Vlastník	Manažeři odpovědní za ISMS
Odpovědnost za sběr dat	Pracovníci bezpečnosti
Frekvence sběru dat	Čtvrtletně
Frekvence hlášení	Ročně
Popis indikátoru	
Indikátor	Sloupcový graf zobrazující shodu po několik period hlášení ve vztahu k prahovým hodnotám (červená, žlutá, zelená) definovaných v analytickém modelu
Analytický model	0–80 % červená, 80–95 % žlutá, 95–100 % zelená Pokud pro žlutou prahovou hodnotu nebylo meziročně dosaženo pokroku alespoň 5 %, ohodnocení je automaticky červené
Rozhodovací kritéria	Červená – přezkoumání příčin nezohlednění bezpečnosti ve smlouvách s dodavateli a návrh následného postupu Žlutá – vyžadováno monitorování, pokud se trend nezlepšuje pro dvě periody hlášení, je zahájeno přezkoumání Zelená – není požadována žádná akce
Forma hlášení	Sloupcový graf s barevnými sloupci na základě rozhodovacích kritérií doplněný o možná opatření a komentáře k vývoji hodnot

3.6 Přínos práce pro teoretické poznání a podnikovou praxi

Diplomovou práci lze využít jako východisko při řízení a neustálém zlepšování systému řízení bezpečnosti informací. Veškeré uvedené poznatky mohou zaměstnanci energetické společnosti zastávající bezpečnostní role použít jako základní metodiku pro opakovatelné a objektivní posouzení implementovaných opatření a postupů v rámci hodnocení PIT, čímž bude zajištěna jejich vhodnost, přiměřenost a celková efektivnost ISMS. Zavedením systematického přístupu k měření výkonnosti procesů a analýze opatření se minimalizují rizika, zmírní následky případných selhání a optimalizují postupy bezpečnosti informací.

Výstupy práce poskytují v rámci procesu monitorování efektivity ISMS evidenci důkazů o účinnosti bezpečnostních opatření. Uvedené metody rovněž předkládají informace pro usměrňování a stanovování priorit při alokaci lidských zdrojů a finančních prostředků do bezpečnosti informací k ochraně klíčových procesů a řízení rizik společnosti.

Sestavený zralostní model představuje relativně rychlý a objektivní nástroj poskytující celkový přehled a dokumentovaný postup hodnocení současné úrovně činností, procesů a metod souvisejících s bezpečností informací. Získané výsledky ze zralostního modelu lze ve společnosti využít pro neustálé zlepšování ISMS, odůvodnění potřeby následného postupu zavádění ISMS nebo při určování cílů a priorit bezpečnosti informací. Vytvořený model je možné dále přizpůsobovat požadavkům společnosti a rozšířit o další standardy nebo nejlepší praktiky bezpečnosti informací. Za předpokladu sdílení výsledků hodnocení může zralostní model do budoucna posloužit jako benchmarkový nástroj ke srovnání výkonnosti ISMS s ostatními konkurenty v odvětví.

Používáním navržených metrik za účelem hodnocení účinnosti ISMS bude podporováno neustálé zlepšování bezpečnosti informací, identifikace a vyhodnocení nevyhovujících a neúčinných postupů bezpečnosti informací ve společnosti. Výsledky měření poskytnou objektivní důkazy pro řízení rizik a přezkoumání ISMS managementem společnosti a lze je použít při stanovení priorit činností spojených s rozvojem procesů a opatření. Uvedený soubor ukazatelů umožňuje zainteresovaným stranám uskutečňovat neustálé zlepšování bezpečnosti informací a ISMS, přičemž postupy měření je nezbytné ve společnosti neustále zlepšovat a revidovat.

ZÁVĚR

Diplomová práce se zabývala návrhem následného postupu zavádění ISMS a hodnocením úrovně bezpečnosti informací v energetické společnosti pomocí vytvořeného zralostního modelu a souboru ukazatelů. Zavedením navrhované metodiky lze sledovat významné činitele bezpečnosti informací, stanovit výkonnost nebo priority při zlepšování ISMS.

Analýza problému a současné situace se zaměřila na charakteristiku odvětví energetiky, představení společnosti a současný stav bezpečnosti informací ve stanoveném rozsahu. Součástí byla podniková, informační a bezpečnostní strategie a popis infrastruktury s přehledem odpovědností za uskutečněná rozhodnutí v oblastech IS/ICT a systému řízení bezpečnosti informací. V rámci bezpečnostní strategie byly představeny faktory podněcující vytvoření ISMS a používané zdroje k identifikaci požadavků na bezpečnost. Současný stav bezpečnosti informací se zabýval procesní infrastrukturou a obsahoval implementovaná opatření rozčleněnými podle kapitol normy ISO/IEC 27001. Na závěr byly zjištěné poznatky shrnuty s konstatováním ohledně nedostatků zavedeného ISMS, neexistence nástroje pro přezkoumávání účinnosti zavedených opatření a chybějícího souboru ukazatelů pro průběžné monitorování výkonnosti ISMS.

Kapitola návrhu vlastního řešení se specializovala na analýzu rizik, hodnocení úrovně způsobilosti opatření vymezených normou ISO/IEC 27002 prostřednictvím sestaveného zralostního modelu, stanovení akčního plánu ISMS a definici metrik k určení výkonnosti systému řízení bezpečnosti informací. Analýza rizik vymezila největší rizika společnosti a velikosti jejich dopadu v případě naplnění bezpečnostních hrozeb. Zralostní model rozpoznal největší rozdíly mezi současnou a požadovanou úrovní zralosti zavedených opatření, identifikoval související procesy a činnosti k opatření a definoval nezbytná zlepšení pro jednotlivá opatření. Na základě zjištěných nedostatků pomocí analýzy rizik a zralostního modelu byl stanoven akční plán pro ISMS. Součástí navrhovaných zlepšení bylo i ekonomické zhodnocení s odhadem jednorázových a předpokládaných ročních nákladů. Na závěr byl vytvořen soubor ukazatelů pro hodnocení efektivity a efektivnosti systému řízení bezpečnosti informací a uvedeny přínosy poznatků pro ES při řízení a zlepšování ISMS, na jejichž základě lze usoudit, že vymezených cílů diplomové práce bylo dosaženo.

SEZNAM POUŽITÉ LITERATURY

(1) ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

(2) JORDÁN, V. a V. ONDRÁK. *Infrastruktura komunikačních systémů II: Kritické aplikace*. Brno: CERM, 2015. ISBN 978-80-214-5240-4.

(3) ČSN ISO/IEC 27000. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(4) ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(5) NOVÁK, L. a J. POŽÁR. Systém řízení informační bezpečnosti. In: GOGELA, R. *Pracovní příručka bezpečnostního manažera*. Praha: Policejní akademie ČR v Praze, 2011, s. 5-19. ISBN: 978-80-7251-364-2.

(6) ISO/IEC TR 27019:2013. *Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.* Geneva: International Organization for Standardization, 2013.

(7) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000.

(8) BURIAN, D. K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR). *PRÁVNÍ PROSTOR* [online]. 2016 [cit. 2017-01-18]. ISSN 2336-4114. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr

(9) NCKB. *Národní centrum kybernetické bezpečnosti* [online]. 2011 [cit. 2017-01-27]. Dostupné z: http://www.govcert.cz

(10) Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ze dne 23. července 2014.

(11) DURAČINSKÁ, Z. Co přináší nová směrnice EU o informační bezpečnosti? *IT Systems* [online]. 2016, 10/2016 [cit. 2017-02-09]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/clanky/co-prinasi-nova-smernice-eu-o-informacni-bezpecnosti.htm

(12) ČSN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(13) NOVOTNÝ, O. *Řízení výkonnosti podnikové informatiky*. Praha: Professional Publishing, 2010. ISBN 978-80-7431-040-9.

(14) UČEŇ, P. *Zvyšování výkonnosti firmy na bázi potenciálu zlepšení*. Praha: Grada, 2008. ISBN 978-80-247-2472-0.

(15) KAPLAN, Robert S. a David P. NORTON. *Efektivní systém řízení strategie: nový nástroj zvyšování výkonnosti a vytváření konkurenční výhody*. Praha: Management Press, 2010. ISBN 978-80-7261-203-1.

(16) VOLCHKOV, A. How to Measure Security From a Governance Perspective. *ISACA Journal* [online]. 2013, Volume 5 [cit. 2017-02-18]. ISSN 1526-7407. Dostupné z: http://www.isaca.org/JOURNAL/ARCHIVES/2013/VOLUME-5/Pages/How-to-Measure-Security-From-a-Governance-Perspective.aspx

(17) HERATH, T., H. HERATH a Wayne G. BREMSER. Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management. *Information Systems Management* [online]. 2010, 27(1), 72-81 [cit. 2017-03-10]. ISSN 10580530. Dostupné z: DOI 10.1080/10580530903455247.

(18) JIRASEK, V. Practical application of information security models. *Information Security Technical Report* [online]. 2012, 17(1/2), 1-8 [cit. 2017-05-02]. ISSN 13634127. Dostupné z: DOI 10.1016/j.istr.2011.12.004.

(19) Zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon) ze dne 28. listopadu 2000.

(20) ČSN ISO/IEC 15504-2. *Informační technologie – Posuzování procesu. Část 2: Realizace posouzení*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2005.

(21) ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(22) ČSN ISO/IEC 27004. *Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření*. Praha: Úřad pro technickou normalizaci metrologii a státní zkušebnictví, 2011.

SEZNAM POUŽITÝCH ZKRATEK

BSC	Balanced Scorecard
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CIT	Commercial Infrastructure
COBIT	Control Objectives for Information and related Technology
CPM	Corporate Performance Management
CSIRT	Computer Security Incident Response Team
ČSN	Česká technická norma
ES	Energetická společnost
GDPR	General Data Protection Regulation
HDO	Hromadné dálkové ovládání
HMI	Human Machine Interface
ICS	Industrial Control System
ICT	Informační a komunikační technologie
IDS/IPS	Intrusion Detection/Prevention System
IEC	International Electrotechnical Commission
IS	Informační systém
ISM	Information Security Manager
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
KII	Kritická informační infrastruktura
KPI	Key Performance Indicators
KRI	Key Results Indicators
LAN	Local Area Network
LISO	Local Information Security Officer
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NIS	Network and Information Security

NIST	National Institute for Standards and Technology
PDCA	Plan, Do, Check, Act
PI	Performance Indicators
PIT	Process Infrastructure
PLC	Programmable Logic Controller
PQM	Power Quality Monitoring
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SW	Software
TR	Technical Report
VKB	Výbor pro kybernetickou bezpečnost
VPN	Virtual Private Network
WAN	Wide Area Network

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

Příloha 1: Ukázka sestaveného zralostního modelu pro kapitolu A.5

ZRALOSTNÍ MODEL PRO OPATŘENÍ NORMY ISO/IEC 27002 Hodnotící stupnice: 0: Neúplný 1: Vykonávaný 2: Řízený 3: Zavedený 4: Předvídatelný 5: Optimalizovaný		
A.5 Politiky bezpečnosti informací		
A.5.1 Pokyny managementu organizace k bezpečnosti informací		
A.5.1.1 Politiky pro bezpečnost informací		
Zralost	**Atribut**	**Indikátor**
1	**Výkonnost**	a. Politiky pro bezpečnost informací jsou definovány.
2	**Řízení výkonnosti**	a. Politika bezpečnosti informací stanovuje přístup organizace k řízení svých cílů bezpečnosti informací. b. Odpovědnosti a pravomoci pro definici, schválení a zveřejnění politik pro bezpečnost informací jsou vymezeny a přiřazeny. c. Rozhraní mezi zúčastněními stranami jsou řízena tak, aby se zajistila efektivní komunikace a jasné přiřazení odpovědností.
	Řízení pracovních produktů	a. Politika bezpečnosti informací organizace je dokumentována. b. Politika bezpečnosti informací je schválena managementem organizace. c. Politiky pro bezpečnost informací jsou dostupné všem zaměstnancům organizace a relevantním externím stranám.
3	**Vymezený**	a. Politika bezpečnosti informací obsahuje definici bezpečnosti informací, cílů a principů, které nasměrují veškeré činnosti související s bezpečností informací. b. Politiky pro bezpečnost informací jsou dány na vědomí všem zaměstnancům a relevantním externím stranám. c. Požadované odborné způsobilosti a role pro definici, schválení a zveřejnění politik pro bezpečnost informací jsou identifikovány. d. Vhodné metody pro monitorování efektivnosti a vhodnosti definice, schválení a zveřejnění politik bezpečnosti informací jsou určeny.
	Zavedený	a. Politika bezpečnosti informací obsahuje prohlášení pro přiřazení odpovědností a pravomocí k definovaným rolím pro řízení bezpečnosti informací. b. Politika bezpečnosti informací obsahuje postupy pro zacházení s odchylkami a výjimkami. c. Požadované zdroje a informace nezbytné pro definici, schválení a zveřejnění politik pro bezpečnost informací jsou zpřístupněny a používány. d. Zaměstnanci vykonávající definici, schválení a zveřejnění politik pro bezpečnost informací jsou odborně způsobilí na základě vzdělání, výcviku a zkušeností. e. Role, odpovědnosti a pravomoci pro definici, schválení a zveřejnění politik bezpečnosti informací jsou přiřazeny a sděleny.

4	**Měření**	a. Vhodné metody pro hodnocení a měření efektivnosti a vhodnosti definice, schválení a zveřejnění politik pro bezpečnost informací jsou aplikovány. b. Cíle, míry a četnost měření pro definici, schválení a zveřejnění politik pro bezpečnost informací jsou stanoveny. c. Výsledky hodnocení a měření jsou shromážděny, analyzovány a zpracovány do zpráv k monitorování rozsahu splnění cílů.
	Kontrola	a. Formální proces přezkoumání odchylek pro definici, schválení a zveřejnění politik pro bezpečnost informací je stanoven. b. Kontrolní omezení pro definici, schválení a zveřejnění politik pro bezpečnost informací jsou stanovena. c. Nápravná opatření změřená na zvláštní příčiny odchylek při definici, schválení a zveřejnění politik pro bezpečnost informací jsou prováděna.
5	**Inovace**	a. Politika bezpečnosti informací je přizpůsobována podnikatelské strategii. b. Politika bezpečnosti informací je přizpůsobována požadavkům vyvolanými předpisy, legislativou a smlouvami. c. Politika bezpečnosti informací je přizpůsobována požadavkům vyvolanými hrozbami bezpečnosti informací. d. Vhodná data pro identifikaci možností zlepšení definice, schválení a zveřejnění politik bezpečnosti informací jsou analyzována. e. Strategie implementace pro zlepšování definice, schválení a zveřejnění politik pro bezpečnost informací jsou zpracovány.
	Optimalizace	a. Dopad všech navrhovaných změn pro definici, schválení a zveřejnění politik pro bezpečnost informací je posouzen. b. Implementace všech dohodnutých změn pro definici, schválení a zveřejnění politik pro bezpečnost informací je řízena.
A.5.1.2 Politiky pro bezpečnost informací		
Zralost	**Atribut**	**Indikátor**
1	**Výkonnost**	a. Politiky pro bezpečnost informací jsou přezkoumávány.
2	**Řízení výkonnosti**	a. Politiky pro bezpečnost informací jsou přezkoumávány v plánovaných intervalech nebo pokud dojde k významným změnám. b. Odpovědnosti a pravomoci pro přezkoumání politik bezpečnosti informací jsou vymezeny a přiřazeny. c. Rozhraní mezi zúčastněními stranami jsou řízena tak, aby se zajistila efektivní komunikace a jasné přiřazení odpovědností.
	Řízení pracovních produktů	a. Revidované politiky pro bezpečnost informací jsou schváleny managementem organizace. b. Přezkoumání politik zahrnuje posouzení možností pro zlepšování a přístupu organizace k řízení bezpečnosti informací.
3	**Vymezený**	a. Přezkoumání politik je realizováno v reakci na změny v prostředí organizace, podmínek podnikatelské činnosti, právních podmínek a technického prostředí. b. Přezkoumání politik pro bezpečnost informací zajišťuje vhodnost, přiměřenost a efektivnost politik bezpečnosti informací. c. Požadované odborné způsobilosti a role pro přezkoumání politik pro bezpečnost informací jsou identifikovány. d. Vhodné metody pro monitorování efektivnosti a vhodnosti přezkoumání politik pro bezpečnost informací jsou určeny.
	Zavedený	a. Každá politika má vlastníka. b. Požadované zdroje a informace nezbytné pro přezkoumání politik pro bezpečnost informací jsou zpřístupněny a používány. c. Zaměstnanci přezkoumávající politiky bezpečnosti informací jsou odborně způsobilí na základě vzdělání, výcviku a zkušeností. d. Role, odpovědnosti a pravomoci pro přezkoumání politik pro bezpečnost informací jsou přiřazeny a sděleny.

4	**Měření**	a. Vhodné metody pro hodnocení a měření efektivnosti a vhodnosti přezkoumání politik pro bezpečnost informací jsou aplikovány. b. Cíle, míry a četnost měření pro přezkoumání politik pro bezpečnost informací jsou stanoveny. c. Výsledky hodnocení a měření jsou shromážděny, analyzovány a zpracovány do zpráv k monitorování rozsahu splnění cílů.
	Kontrola	a. Formální proces přezkoumání odchylek pro přezkoumání politik pro bezpečnost informací je stanoven. b. Kontrolní omezení pro přezkoumání politik pro bezpečnost informací jsou stanovena. c. Nápravná opatření změřená na zvláštní příčiny odchylek při přezkoumání politik pro bezpečnost informací jsou prováděna.
5	**Inovace**	a. Přezkoumání politik pro bezpečnost informací bere v úvahu výsledky přezkoumání prováděné managementem. b. Vhodná data pro identifikaci možností zlepšení přezkoumání politik bezpečnosti informací jsou analyzována. c. Strategie implementace pro zlepšování přezkoumání politik pro bezpečnost informací jsou zpracovány.
	Optimalizace	a. Dopad všech navrhovaných změn pro přezkoumání politik bezpečnosti informací je posouzen. b. Implementace všech dohodnutých změn pro přezkoumání politik pro bezpečnost informací je řízena.