VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZAVEDENÍ BEZPEČNOSTNÍCH OPATŘENÍ V SOULADU S ISMS PRO SPOLEČNOST

IMPLEMENTATION OF ISMS SECURITY COUNTERMEASURES PROPOSAL FOR A COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Petr Vyhňák**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Petr Vyhňák**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2018/19

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:

Návrh zavedení bezpečnostních opatření v souladu s ISMS pro společnost

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je návrh zavedení bezpečnostních opatření v souladu se systémem řízení informační bezpečnosti pro společnost.

Základní literární prameny:

ČSN EN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

ČSN ISO/IEC 27002. Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

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

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

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

Abstrakt

Diplomová práce se zabývá návrhem zavedení bezpečnostních opatření v souladu se systémem řízení informační bezpečnosti pro společnost. V první části práce jsou definována teoretická východiska. V další části je představena společnost, popsán její současný stav z pohledu bezpečnosti a provedena analýza bezpečnostních opatření za pomoci podpůrného materiálu. Poslední část obsahuje již samotný návrh zavedení bezpečnostních opatření. Součástí práce je analýza rizik, návrh vybraných bezpečnostních opatření včetně postupu zavedení s časovým plánem a ekonomické zhodnocení.

Klíčová slova

ISMS, informační bezpečnost, asistované zhodnocení, ISO/IEC 27001, ISO/IEC 27002

Abstract

The master thesis deals with the proposal of introduction security countermeasures in accordance with the information security management system for the company. The theoretical part is defined in the first part of the thesis. The next part introduces the company, describes the current state of security and analysis security countermeasures with the help of supporting material. The last part includes the proposal to introduce new security countermeasures. The thesis includes risk analysis, design of selected security countermeasures including the implementation procedure with a time schedule and economic evaluation.

Key words

ISMS, information security, assisted assessment, ISO/IEC 27001, ISO/IEC 27002

Bibliografická citace

VYHŇÁK, Petr. *Návrh zavedení bezpečnostních opatření v souladu s ISMS pro společnost* [online]. Brno, 2019 [cit. 2019-05-10]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119784. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

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 10. května 2019

……

podpis autora

Poděkování

Rád bych poděkoval vedoucímu mé diplomové práce panu Ing. Petru Sedlákovi a oponentovi panu Ing. Viktoru Ondrákovi, Ph.D. za cenné rady a odbornou pomoc. Dále také vedení společnosti za konzultace a poskytnutí potřebných podkladů při tvorbě této práce. V neposlední řadě patří poděkování mé rodině.

OBSAH

ÚVOD

Každá organizace disponuje informacemi, které pro ně mají velkou, někdy až nevyčíslitelnou hodnotu. Paradoxem však je, že právě ochrana informací, veškerých dat i zařízení před zneužitím, poškozením či ztrátou je u mnoha organizací opomíjena a podceňována. Snahou každé organizace bez rozdílu na to, zda produkují statky nebo poskytují služby, by měla být ochrana svých dat a informací. Na informace a data působí velké množství již existujících hrozeb a každým dnem vznikají nové. Snažením každé organizace by mělo být předejít těmto hrozbám a minimalizovat škody jimi zapříčiněné. Požadavek na vyšší bezpečnost jde ruku v ruce se zvyšujícími se náklady na zavedení přiměřených opatření. Je na každé organizaci, jakou výši finančních prostředků je ochotna do zabezpečení investovat. Je důležité však zvážit, zda vynaložené finanční prostředky opravdu přinesou odpovídající navýšení bezpečnosti.

Bezpečnost zdaleka není jen záležitostí technickou. Velmi významným prvkem této (ne)bezpečnosti je totiž lidský faktor neboli zaměstnanci, dodavatelé, zákazníci a jiné externí strany. Lidský faktor je stále nejslabším článkem celé bezpečnosti organizace.

Za účelem lepšího pochopení řízení informační bezpečnosti v organizaci vzniklo množství norem. Postupování dle pokynů v normách vede ke zvýšení celkové bezpečnosti organizace. Zavedením celého systému řízení informační bezpečnosti je možné usilovat o certifikaci. Certifikace vede ke zvýšení důvěryhodnosti pro partnery, efektivnímu řízení investic vkládaných do bezpečnosti a naplnění legislativních požadavků. S příchodem kybernetického zákona se zvýšila důležitost certifikace systému řízení informační bezpečnosti. Organizace, které budou chtít dodávat produkty nebo služby do kritické infrastruktury, jsou povinny mít certifikát systému řízení informační bezpečnosti.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem této diplomové práce je zpracovat návrh zavedení bezpečnostních opatření v souladu se systémem řízení informační bezpečnosti pro softwarovou společnost. Vedení společnosti se pro zpracování návrhu rozhodlo z důvodu zvýšení informační bezpečnosti. Společnost v dohledné době neplánuje usilovat o certifikaci ISMS, jde ji pouze o zlepšení současného stavu. Z toho důvodu není nutné zavádět všechna bezpečnostní opatření normy ISO/IEC 27001, ale vybrat pouze ta, která jsou důležitá pro minimalizaci značných bezpečnostních rizik a která povedou ke zlepšení současné situace ve společnosti. Při návrhu budu vycházet z provedené analýzy bezpečnostních opatření a požadavků vedení společnosti.

Samotná práce bude rozdělena do tří základních částí. V první části budou definována teoretická východiska z oblasti informační bezpečnosti, ze kterých budu následně vycházet při návrhu vlastního řešení.

Po teoretických východiscích bude následovat část věnována analýze současného stavu. V této části bude představena společnost, popsán její současný stav z pohledu bezpečnosti a provedena analýza bezpečnostních opatření za pomoci podpůrného materiálu.

Třetí a zároveň poslední část bude zaměřena na samotný návrh zavedení bezpečnostních opatření v souladu se systémem řízení informační bezpečnosti. Tato část bude obsahovat analýzu rizik, návrh vybraných bezpečnostních opatření včetně postupu zavedení s časovým plánem a ekonomické zhodnocení.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole budou popsána teoretická východiska z oblasti informační bezpečnosti, ze kterých budu následně vycházet při návrhu vlastního řešení.

1.1 Základní pojmy

Na úvod je potřeba si vymezit několik pojmů, které jsou důležité pro pochopení dané problematiky.

Data

Data neboli údaje představují holá fakta, která jsou získávána čtením, měřením, vážením, pozorováním atd. Jsou vyjádřena symboly (čísla, písmena, text, zvuk nebo obraz), které samy o sobě nemají význam. Data slouží jako podklad pro vznik informací [1].

Informace

Informace jsou účelově zpracovaná data s významem. Mohou být sdíleny, přenášeny nebo vnímány v rámci rozhodovacího procesu [1].

Informační systém

Informační systém je formulován jako systém vzájemně propojených procesů a informací, které s těmito informacemi pracují [2].

Informační technologie

Souhrnný pojem, který zahrnuje nástroje, procesy a další prostředky sloužící k vytváření, zpracovávání, ukládání a zabezpečení dat a také jejich manipulaci, přenosu a prezentaci [3].

Informační a komunikační technologie

Informační technologie jsou doplněny o komunikační technologie, tedy o množinu technických prostředků využívající se pro sdělování a přijímání informací [3].

Síťová infrastruktura

Zahrnuje všechny síťové prvky a zařízení, které jsou použity při realizaci ICT prostředí [2].

Aktivum

Za aktivum lze považovat cokoliv, co má pro vlastníka nějakou hodnotu. Jeho zneužití, ztráta nebo modifikace by vlastníkovi způsobily škodu. Jsou dělena na hmotná a nehmotná [1].

Zranitelnost

Je slabé místo aktiva nebo systému, tedy HW prostředku, aplikace nebo služby, které může být zneužito hrozbou a zapříčinit tak vznik bezpečnostního incidentu [9].

Hrozba

Hrozbu můžeme chápat jako vlivy působící na aktivum, která může mít za následek vyvolání bezpečnostního incidentu [9].

Bezpečnostní událost

Je proces nebo činnost, která může způsobit nebo vést k narušení informačních systémů a technologií a pravidel definovaných k jeho ochraně [4].

Bezpečnostní incident

Nežádoucí nebo neočekáváná bezpečnostní událost, která vede k narušení pravidel bezpečnosti v organizaci [4].

Dopad

Dopad je škoda způsobená účinkem hrozby na určité aktivum [2].

Riziko

Riziko vyjadřuje pravděpodobnost vzniku bezpečnostního incidentu [9].

Úroveň rizika

Dostaneme vynásobením rizika vzniku bezpečnostního incidentu možným dopadem incidentu. Úroveň následně charakterizuje nebezpečnost hrozby pro organizaci [9].

Opatření

Jakýkoliv prostředek sloužící pro modifikaci bezpečnostních rizik, tedy snížení úrovně rizika jedné nebo více hrozeb [9].

Důvěrnost

Poskytování informací pouze oprávněným uživatelům [2].

Integrita

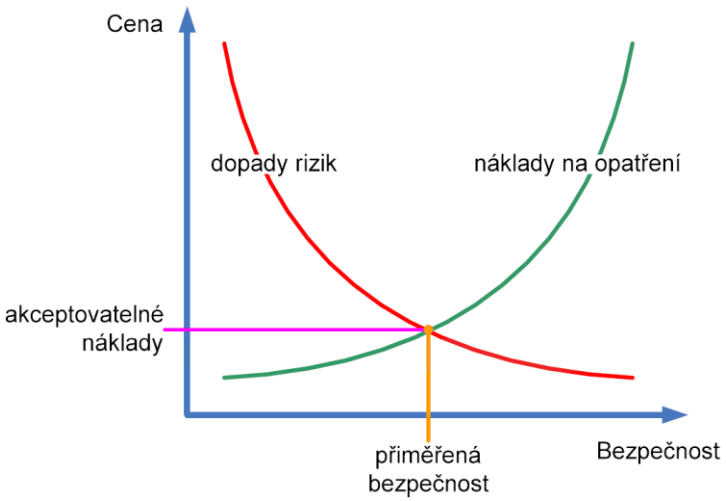
Zajištění, že jsou poskytovány pouze správné a úplné informace [2].

Dostupnost

Vlastnost vyjadřující přístupnost a použitelnost na žádost oprávněného uživatele [4].

Přiměřená bezpečnost

Je stav bezpečnosti, kdy úsilí a investice vynaložené do bezpečnosti musí odpovídat míře možných rizik a hodnotě aktiv. Stanovuje ji především bezpečnostní politika organizace [2].



Obrázek č. 1: Přiměřená bezpečnost za akceptovatelné náklady [Zdroj: 2, s. 36]

Standard

Dokumentovaná úmluva sestávající se z technických specifikací nebo jiných podobných přesně stanovených kritérií používaných jako pravidla nebo směrnice. Často bývá nástrojem k dynamickému prosazení technické politiky a následného pokroku [2].

Norma

Doporučení pro daný standard nebo řešení. V oboru ICT představuje norma předpis nebo směrnici vydávanou různými konsorcii uživatelů a výrobců IT. Bývá výsledkem těžce dosaženého kompromisu [2].

1.1.1 Informační bezpečnost

Informační bezpečnost, nazývaná také jako bezpečnost informací, chrání informace před narušením **tří hlavních atributů** – známé také jako **CIA triáda**:

- důvěrnost (Confidentiality),
- integrita (Integrity),
- dostupnost (Availability) [2].

Informační bezpečnost je ve vzájemném vztahu s bezpečností organizace a bezpečností IS/ICT [5].

*„Nejvyšší kategorií je **bezpečnost organizace**. Její součástí je zajištění bezpečnosti objektů a majetku organizace. Některé její činnosti napomáhají zároveň i zajištění bezpečnosti IS/ICT (např. kontrola oprávnění fyzického přístupu do budov). Její součástí, kromě jiných, je i bezpečnost informací“* [5, s. 55].

*„Cílem a úkolem řízení **bezpečnosti informací** je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu a všech typů – tedy nejen s informacemi v digitální formě“* [5, s. 55].

*„Samotná **bezpečnost IS/ICT** má za úkol chránit „pouze“ ta aktiva, která jsou součástí informačního systému firmy, podporovaného informačními a komunikačními technologiemi. Proto je bezpečnost IS/ICT relativně nejužší oblastí řízení bezpečnosti“* [5, s. 56].

Obrázek č. 2: Vztah úrovní bezpečnosti v organizaci [Zdroj: 2, s. 14]

1.1.2 Kybernetická bezpečnost

Kybernetická bezpečnost je definována jako souhrn právních, organizačních, technických a vzdělávacích prostředků spějící k zajištění ochrany kybernetického prostoru. Kybernetickým prostorem se rozumí digitální prostředí, ve kterém je umožněn vznik, zpracování a výměna informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací [13].

Pojmy kybernetická bezpečnost a informační bezpečnost bývají často považovány za stejné, i když tomu tak není. V určitém bodě se překrývají, rozdíl je však v jejich perimetru. Informační bezpečnost se vztahuje na organizaci na úrovni fyzické, organizační, personální a komunikační bezpečnosti, zatímco kybernetická bezpečnost se vztahuje na kybernetický prostor, tedy na digitální prostředí umožňující vznik, zpracování

a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací [8, 13].

Ústředním správním orgánem pro kybernetickou bezpečnost v České republice je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Vznikl novelou zákona o kybernetické bezpečnosti k 1. srpna 2017 [14].

Kybernetická bezpečnost je v České republice řešena vyhláškami a zákony. Aktuální legislativa:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti),
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti),
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS),
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích,
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury,
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby [15].

1.2 Systém řízení informační bezpečnosti

Information Security Management System (dále jen ISMS), do českého jazyka překládán jako systém řízení informační bezpečnosti, je jádrem pro účelné a efektivní řízení bezpečnosti informací. Cílem ISMS je ochránit informační aktiva před narušením důvěrnosti, integrity a dostupnosti prostřednictvím politik, postupů, směrnic

a příslušných zdrojů a činností, které organizace řídí. ISMS je zaměřen na ustanovení, zavádění, provoz, monitorování, přezkoumávání, údržbu a zlepšování bezpečnosti informací organizace. ISMS je postaveno na posuzování rizik a přijímání rizik organizace na úrovni, která je navržena pro efektivní ošetření rizik a pro jejich řízení [4].

Na ISMS lze také nahlížet jako na efektivní dokumentovaný systém řízení a správy informačních aktiv, jehož cílem je vyloučit jejich možnou ztrátu nebo poškození tím, že:

- jsou definována aktiva, která se mají chránit,
- jsou vybrána a řízena možná rizika informační bezpečnosti,
- jsou nastolena opatření s žádanou úrovní záruk, která jsou kontrolována [2].

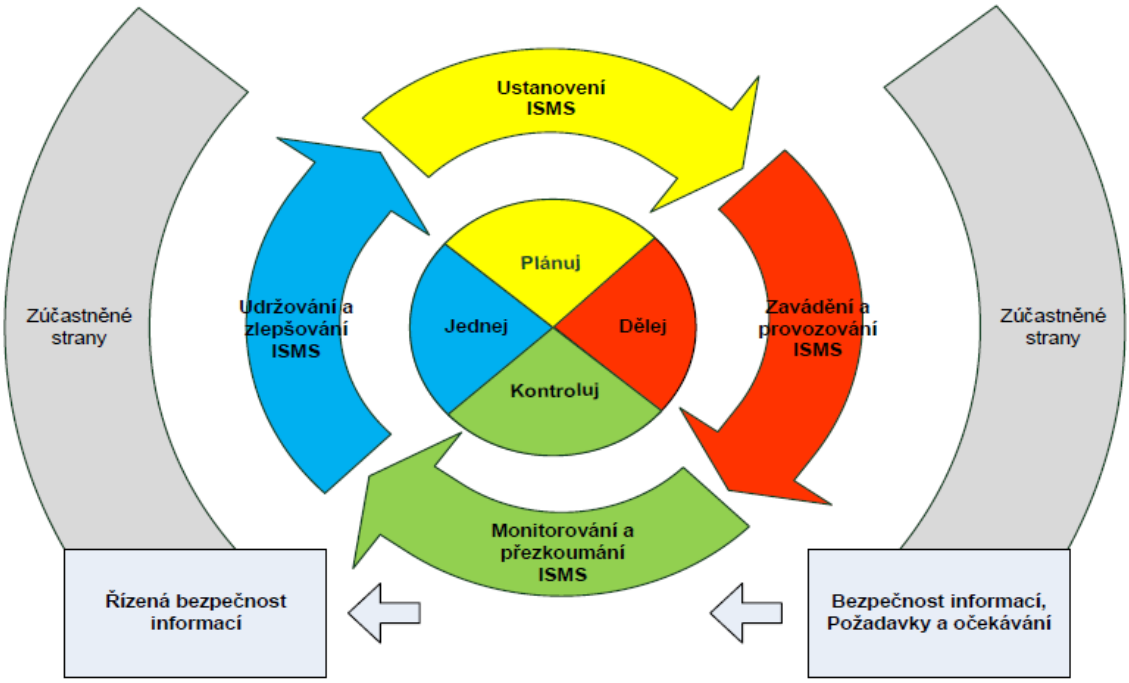
1.2.1 PDCA cyklus

PDCA cyklus, označován také jako Demingův cyklus, byl vyvinut americkým statistikem Williamem Edwardsem Demingem. Jedná se o metodu postupného zlepšování například kvality služeb, procesů, aplikací či dat za pomocí čtyř neustále se opakujících činností:

- plan (plánuj),
- do (dělej),
- check (kontroluj),
- act (jednej) [2, 5].

ISMS je obdobně jako ostatní systémy řízení založen na PDCA cyklu. V případě ISMS však mluvíme o těchto čtyřech neustále se opakujících etapách:

- ustanovení ISMS,
- zavádění a provoz ISMS,
- monitorování a přezkoumávání ISMS,
- údržba a zlepšování ISMS [2].



Obrázek č. 3: Cyklus PDCA v ISMS [Zdroj: 2, s. 25]

1.2.2 Ustanovení ISMS

První etapou budování ISMS je jeho ustanovení. Dochází zde k definování základů celého systému řízení informační bezpečnosti. Výsledky této etapy se promítají do dalších navazujících etap. Je proto důležité zvážit veškeré souvislosti již v této etapě, neboť pozdější úpravy jsou nesnadně realizovatelné a vyžadují větší finanční náklady. Ustavení ISMS lze rozdělit do několika kroků. Prvním krokem etapy je definování rozsahu a hranic ISMS. Vedení společnosti následně podepsáním dokumentu „Prohlášení o politice ISMS“ odsouhlasí a vyjádří podporu v zavedení tohoto systému. Na základě souhlasu je možné zahájit práci s riziky. Je provedena analýza a zvládání rizik včetně vybrání vhodných bezpečnostních opatření. Posledním krokem etapy je získání formálního souhlasu vedení organizace s výběrem daných opatření a se zbytkovými riziky [5].

Definice rozsahu a hranic ISMS

Jak již samotný název napovídá, jedná se stanovení rozsahu a hranic, ve kterých je ISMS uplatňován. Výchozí rozsah a hranice ISMS nemusí vždy pokrývat celou organizaci. V případě, že se však rozhodneme aplikovat ISMS na celou organizaci, bude již od počátku řešena informační bezpečnost napříč celou organizací. Tato aplikace však žádá poměrně značné investice z hlediska spotřeby zdrojů i financí. Je proto často vhodné rozsah ISMS omezit na jasně definovanou část organizace např. vybranou pobočku, určený organizační celek či informační systém. Nemusí se naléhavě jednat o nejdůležitější část organizace. Důležité je vybrat tu část, která je otevřená pro zavádění změn a zlepšení [5].

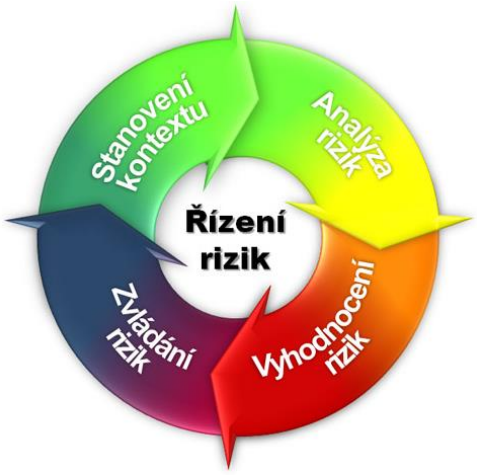
Prohlášení o politice ISMS

Politika ISMS je významný dokument, ve kterém vedení organizace deklaruje plnou připravenost a odpovědnost k prosazení cílů při zavádění systému řízení informační bezpečnosti. V tomto dokumentu jsou upřesněny cíle ISMS, kterých má být v rámci ISMS dosaženo, a je definován směr pro řízení informační bezpečnosti. Dále také stanovuje kritéria pro popis a hodnocení rizik. Celá politika ISMS musí být schválena vedením organizace [2, 5].

Řízení rizik

Řízení rizik je klíčovým nástrojem pro systematické řízení informační bezpečnosti. Podstatným způsobem ovlivňuje efektivitu fungování celého ISMS. Cílem řízení rizik je identifikovat a kvantifikovat rizika, kterým je potřeba čelit a poté vhodným způsobem rozhodnout o zvládání těchto rizik. Přesná znalost skutečných bezpečnostních rizik vede k účinnému vynakládání úsilí při prosazování bezpečnostních opatření, které tak přinášejí větší efektivitu [2, 5].

Řízení rizik se skládá z několika na sebe navazujících fází (viz Obrázek č. 4).



Obrázek č. 4: Fáze řízení rizik [Zdroj: 16]

Analýza rizik je podrobněji popsána v kapitole 1.6.

Souhlas vedení se zavedením ISMS a se zbytkovými riziky

V tomhle kroku je zapotřebí, aby vedení organizace odsouhlasilo návrh bezpečnostních opatření, která jsou nezbytná pro snížení bezpečnostních rizik. Vedení by mělo zároveň rozhodnout, zda jsou existující rizika pro chod organizace akceptovatelná či nikoli [5].

Prohlášení o aplikovatelnosti

Dokumentované prohlášení, v němž jsou popsány cíle opatření a jednotlivá bezpečnostní opatření, která jsou důležitá a aplikovatelná na ISMS organizace. Pro organizace, které usilují o shodu svého ISMS s normou ISO/IEC 27001, je tento dokument povinný [2].

1.2.3 Zavádění a provoz ISMS

Druhou etapou budování ISMS je jeho zavedení a provoz. Cílem je prosadit všechna bezpečnostní opatření tak, jak byla navržena v etapě ustanovení ISMS [5].

V této etapě je nutné provést níže uvedené činnosti:

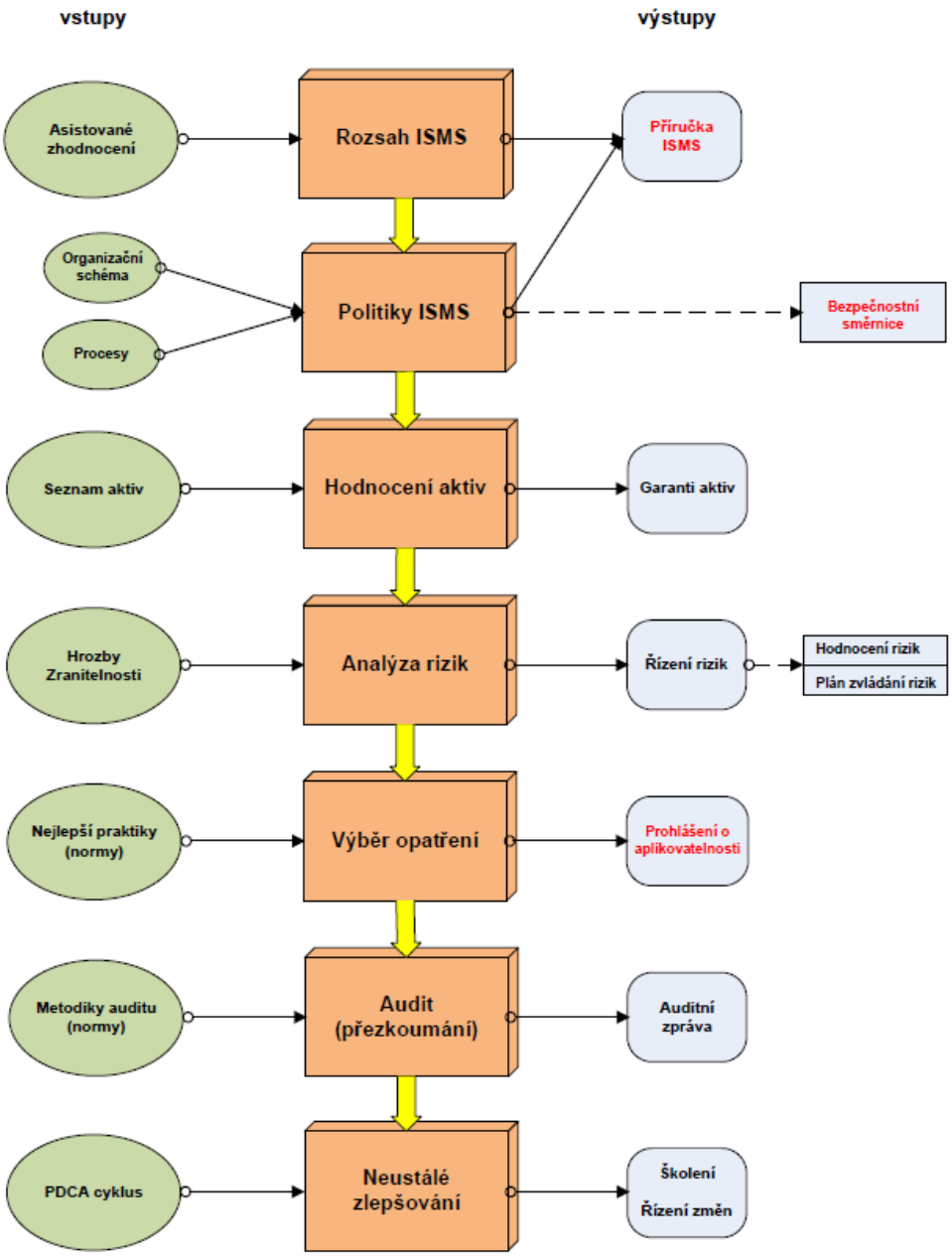
- formulovat dokument „Plán zvládání rizik“,
- zavést navržená bezpečnostní opatření a sepsat příručku informační bezpečnosti,
- definovat program budování bezpečnostního povědomí a provést zaškolení všech pracovníků z úseku informatiky a z oblasti řízení bezpečnosti,
- specifikovat způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele,
- zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty,
- spravovat dokumenty, záznamy a zdroje ISMS [5].

1.2.4 Monitorování a přezkoumávání ISMS

Třetí etapou budování ISMS je jeho monitorování a přezkoumávání. Cílem této etapy je zajistit účinnou zpětnou vazbu, která je pro fungování ISMS nezbytná. Dochází k pravidelnému prověřování všech aplikovaných bezpečnostních opatření s ohledem na výsledky bezpečnostních auditů, incidentů, výsledků měření účinnosti opatření a návrhu všech zainteresovaných stran. Důležitou roli hraje interní audit ISMS, který zajišťuje nezávislý pohled na fungování ISMS [2, 5].

1.2.5 Údržba a zlepšování ISMS

Čtvrtou a zároveň poslední etapou budování ISMS je jeho údržba a zlepšování. Dochází ke sběru podnětů ke zlepšení ISMS a k nápravě všech nedostatků (neshod), které se v ISMS objevují. Provádí se opatření k nápravě a preventivní opatření [5].



Obrázek č. 5: Rekapitulace kroků zavedení ISMS [Zdroj: 8]

1.3 Knihovna ITIL a metodika COBIT

V oblasti řízení informační bezpečnosti lze také využít knihovnu ITIL a metodiku COBIT.

1.3.1 ITIL

Information Technology Infrastructure Library (ITIL) je celosvětově uznávaný rámec v oblasti řízení IT služeb. Řeší, jak dodávat kvalitní IT služby za přiměřené náklady. Nejedná se o normu, ani o metodiku, ale o rámec vycházející z nejlepších praktických zkušeností a osvědčených postupů (best practices). Osvědčené postupy knihovny ITIL jsou v současné době podrobně popsány v pěti ústředních publikacích, které mapují celý životní cyklus IT služby a souvisejících procesů, počínaje vytvořením strategie (Service Strategy), tvorbou návrhu (Service Design), realizací a nasazením do provozu (Service Transition) až po každodenní provozování (Service Operation) a neustálé zlepšování všech aspektů služeb (Continual Service Improvement) [2, 6].

1.3.2 COBIT

Control Objectives for Information and Related Technology (COBIT) je celosvětově uznávaná metodika vytvořená mezinárodní asociací ISACA pro správu a řízení ICT. COBIT představuje soubor všeobecně uznávaných praktik řízení ICT, tak aby využití informací a nasazení ICT přispívalo k perspektivnímu rozvoji organizace, prohlubovalo její strategické cíle a snižovalo rizika souvisejí s použitím ICT. Metodika COBIT se snaží složitý systém řízení ICT strukturovat takovým způsobem, aby mu rozuměli řídící pracovníci a uživatelé bez detailnějších znalostí IT. Princip metodiky je postaven na cílech organizace, zdrojích IT a procesech. Tyto tři komponenty využívá tzv. kostka COBIT, která znázorňuje vzájemné prolínání procesů IT, zdrojů informatiky a požadavků na informační kritéria [2, 5].

1.4 Normalizační instituce

International Organization for Standardization (ISO)

ISO je nezávislá, nevládní a mezinárodní organizace zabývající se podporou rozvoje standardizačních a s tím spojených aktivit. Má členství ve 164 národních normalizačních orgánech. Prostřednictvím svých členů spojuje odborníky, kteří předávají znalosti a rozvíjejí dobrovolné, konsensuální, relevantní mezinárodní normy poskytují řešení globálních problémů a podporují inovace [2, 17].

International Electrotechnical Comission (IEC)

IEC je přední světová organizace, která připravuje a zveřejňuje mezinárodní normy pro všechny elektrické, elektronické a související technologie. IEC úzce spolupracuje s organizací ISO a ITU [18].

International Telecommunations Union (ITU)

ITU je mezinárodní organizace, která spadá do hierarchie OSN. Podpořila růst mnoha technologií jako např. mobilní technologie a Internet. Představuje vedoucí roli ve správě spekter radiové frekvence, čím umožňuje radiově založeným systémům (např. celulární telefony, letecké a námořní naváděcí systémy, vědecké výzkumné stanice, satelitní komunikace a rádiové a televizní vysílání) dál poskytovat spolehlivé bezdrátové služby napříč celým světem. Činnost ITU je rozdělena do tří odvětví: rozvoj telekomunikací (ITU-D), standardizace telekomunikací (ITU-T) a radiokomunikace (ITU-R) [2, 19].

Organizace ISO, IEC a ITU při vypracovávání norem, které mají celosvětovou působnost, úzce spolupracují [5].

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ)

„ÚNMZ je organizační složkou státu v resortu Ministerstva průmyslu a obchodu ČR. Hlavním posláním ÚNMZ je zabezpečovat úkoly vyplývající ze zákonů České republiky upravujících technickou normalizaci, metrologii a státní zkušebnictví a úkoly v oblasti technických předpisů a norem uplatňovaných v rámci členství ČR v Evropské unii. Od 1.1.2018 přechází všechny činnosti související s tvorbou, vydáváním a distribucí technických norem na Českou agenturu pro standardizaci“ [20].

Česká technická norma (ČSN) vzniká dvojím způsobem:

- přejímáním evropských a mezinárodních norem do českých technických norem formou ČSN EN (ČSN IEC, ČSN ISO a tak dále),
- tvorbou původních ČSN plynoucí (plynoucích) z národních potřeb a ze stanovisek zachování funkčnosti fondu ČSN [2].

1.5 Normy řady ISO/IEC 27000

Řada norem pro řízení informační bezpečnosti ISO/IEC 27000 pomáhá organizacím všech typů a velikostí zavést a provozovat systém řízení informační bezpečnosti. Řada norem se skládá z mezinárodních norem se společným názvem *Informační technologie – Bezpečnostní techniky* [4].

ISO/IEC 27000 *Systémy řízení bezpečnosti informací – Přehled a slovník*

Norma uvádějící přehled systémů řízení informační bezpečnosti, použitých termínů a definic v řadě norem ISO/IEC 27000 [4].

ISO/IEC 27001 *Systémy řízení bezpečnosti informací – Požadavky*

Norma specifikuje požadavky na ustanovení, zavádění a provozování, monitorování a přezkoumávání, udržování a zlepšování ISMS v kontextu celkových rizik činnosti organizace. Specifikuje také požadavky na výběr a zavedení bezpečnostní opatření chránící informační aktiva [4].

ISO/IEC 27002 *Soubor postupů pro opatření bezpečnosti informací*

Norma poskytuje doporučení pro výběr bezpečnostních opatření v rámci procesu zavádění ISMS založeném na normě ISO/IEC 27001. Rovněž je určena pro použití při vypracovávání směrnic pro řízení informační bezpečnosti v organizaci [2].

ISO/IEC 27003 *Směrnice pro implementaci systému řízení bezpečnosti informací*

Norma skýtá praktické pokyny k implementaci a dále informace pro ustanovení, zavádění a provozování, monitorování a přezkoumávání, udržování a zlepšování ISMS v souladu s požadavky normy ISO/IEC 27001. Je použitelná při zavádění ISMS do všech typů organizací [4].

ISO/IEC 27004 *Řízení bezpečnosti informací – Měření*

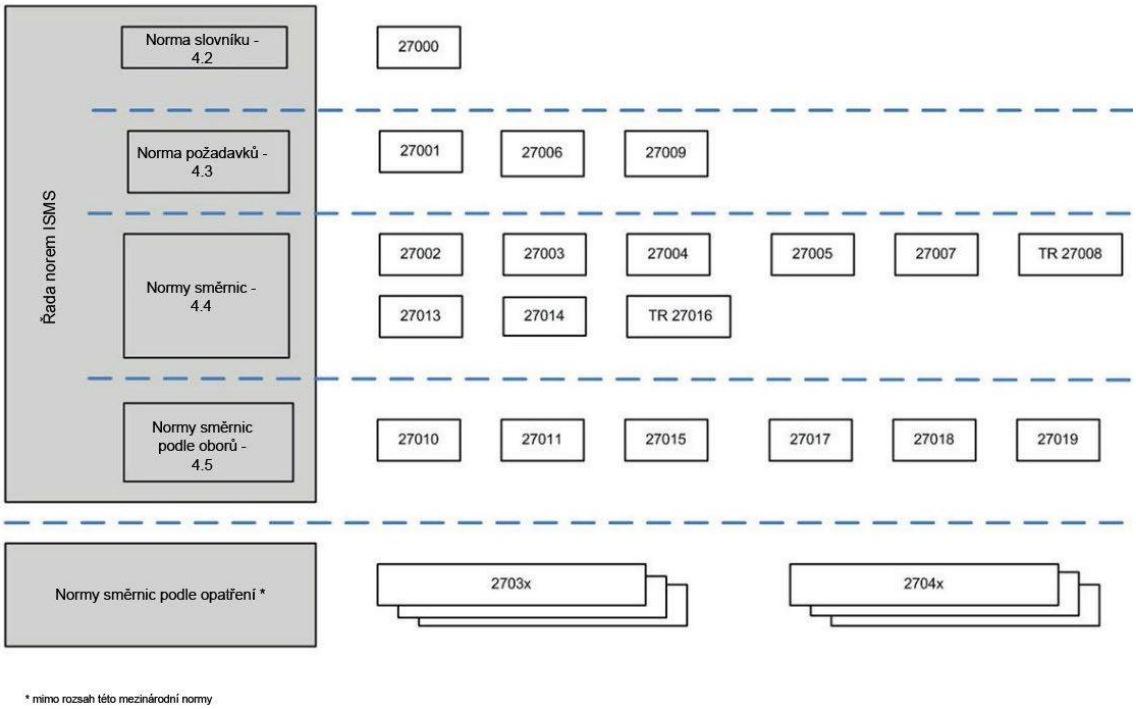
Norma skýtá doporučení pro vývoj a použití měření k posouzení efektivnosti ISMS, opatření nebo skupin opatření dle normy ISO/IEC 27001 [4].

ISO/IEC 27005 *Řízení rizik bezpečnosti informací*

Norma poskytuje směrnice pro řízení rizik informační bezpečnosti v rámci organizace. Nenabízí však konkrétní metodiku pro řízení rizik informační bezpečnosti. Záleží jen na organizaci, jaký přístup k řízení rizik zvolí. Norma je využitelná ve všech typech organizací, které chtějí řídit rizika, která mohou narušit informační bezpečnost organizace [2, 4].

ISO/IEC 27006 *Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací*

Norma skýtá požadavky a dává doporučení orgánům, které provádějí audit a certifikaci ISMS a doplňuje tak požadavky zahrnuté v ISO/IEC 17021 a ISO/IEC 27001 [4].



Obrázek č. 6: Vztahy mezi normami řady ISO/IEC 27000 [Zdroj: 4, s. 26]

1.6 Analýza rizik

Analýza rizik je proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti [7].

1.6.1 Fáze analýzy rizik

První fáze

Cílem první fáze analýzy rizik je prozkoumat potenciální dopady při narušení důvěrnosti, integrity a dostupnosti informací. V rámci této fáze dochází k identifikaci a ohodnocení aktiv. Identifikace spočívá ve vytvoření seznamu aktiv na přiměřeně podrobné úrovni. Aktiva lze dělit několika způsoby. Lze je dělit na softwarová, hardwarová, informační aktiva, služby a lidé. Další možností dělení aktiv je na primární (např. obchodní procesy a činnosti, informace) a podpůrná (např. hardware, software, sítě, pracovníci, lokalita, organizace). Po identifikaci aktiv dochází ke stanovení hodnoty aktiva na základě zvoleného klasifikačního schématu. Hodnotu lze tedy stanovit na základě finančního ohodnocení nebo také dle dopadu na organizaci při narušení jednotlivých atributů informační bezpečnosti (důvěrnost, integrita a dostupnost) [2, 7, 12].

Druhá fáze

Cílem druhé fáze je ohodnotit potenciální hrozby a zranitelnost aktiv a následně stanovit úroveň rizik. V rámci této fáze dochází k identifikaci a ohodnocení hrozeb a zranitelnosti a stanovení úrovně rizik. Při identifikaci hrozeb a zranitelnosti lze vycházet z normy ISO/IEC 27005, která obsahuje v příloze C a D příklady typických hrozeb a zranitelnosti. Při identifikaci je zapotřebí se držet kontextu organizace, protože ne všechny hrozby a zranitelnosti jsou pro organizaci relevantní. Úroveň rizika je pro každé aktivum stanovena pomocí hodnoty aktiva, hodnoty hrozby a zranitelnosti [10, 12].

Třetí fáze

Cílem třetí a zároveň poslední fáze je vybrat vhodná bezpečnostní opatření na základě výpočtu úrovně rizika. Opatření mohou být vybrána z dostupných norem či metodik např. z normy ISO/IEC 27002 nebo metodiky CRAMM [2].

1.6.2 Metody analýzy rizik

Analýzu rizik lze provádět v různých úrovních v závislosti na kritičnosti aktiv, rozsahu zranitelnosti a předcházejících incidentech zasahující organizaci. Může být kvalitativní, kvantitativní nebo kombinací obou, záleží na okolnostech [12].

Kvalitativní analýza rizik

Kvalitativní analýza používá škálu klasifikačních atributů k popisu velikosti potenciálních následků (např. nízký, střední a vysoký) a pravděpodobnosti, že se tyto následky vyskytnou. Úroveň škály klasifikačních atributů je obvykle určována klasifikačním odhadem, při kterém se může projevit subjektivita hodnotitele. Výhodou této analýzy je její jednoduchost, rychlost a snadná pochopitelnost všemi příslušnými pracovníky. Nevýhodou je závislost na subjektivním výběru škály [12].

Kvantitativní analýza rizik

Kvantitativní analýza používá pro určení následků a pravděpodobnosti stupnici s číselnými hodnotami a čerpá přitom data z různých zdrojů. Kvalita analýzy záleží na přesnosti a úplnosti číselných hodnot. Výhodou této analýzy je, že často využívá historická data incidentů, což může mít přímou závislost s cíli informační bezpečnosti a

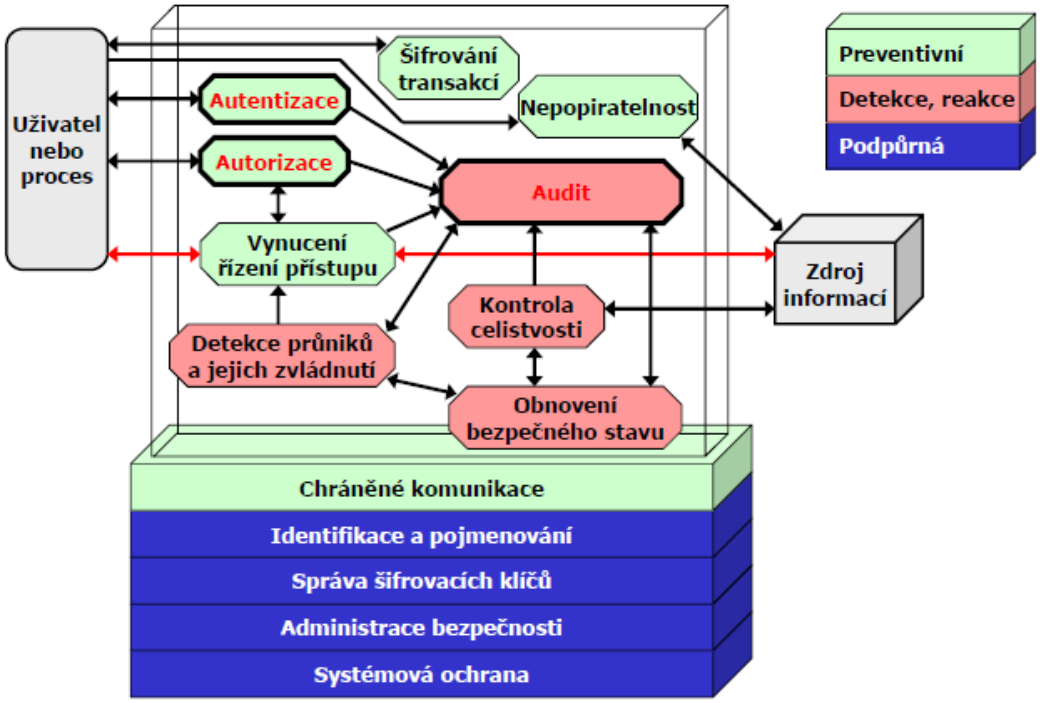
zájmy organizace. Nevýhodou je postrádání těchto dat u nových rizik nebo slabých míst v bezpečnosti [12].

1.7 Opatření

Bezpečnostním opatřením rozumíme jakýkoliv prostředek (např. proces, politiku, postup, metodický pokyn nebo technický prostředek) pomocí kterého modifikujeme bezpečnostní rizika, tedy snižujeme úroveň rizika jedné nebo několika hrozeb [12].

Základní typy bezpečnostních opatření:

- preventivní,
- detekce a reakce,
- podpůrná [2].



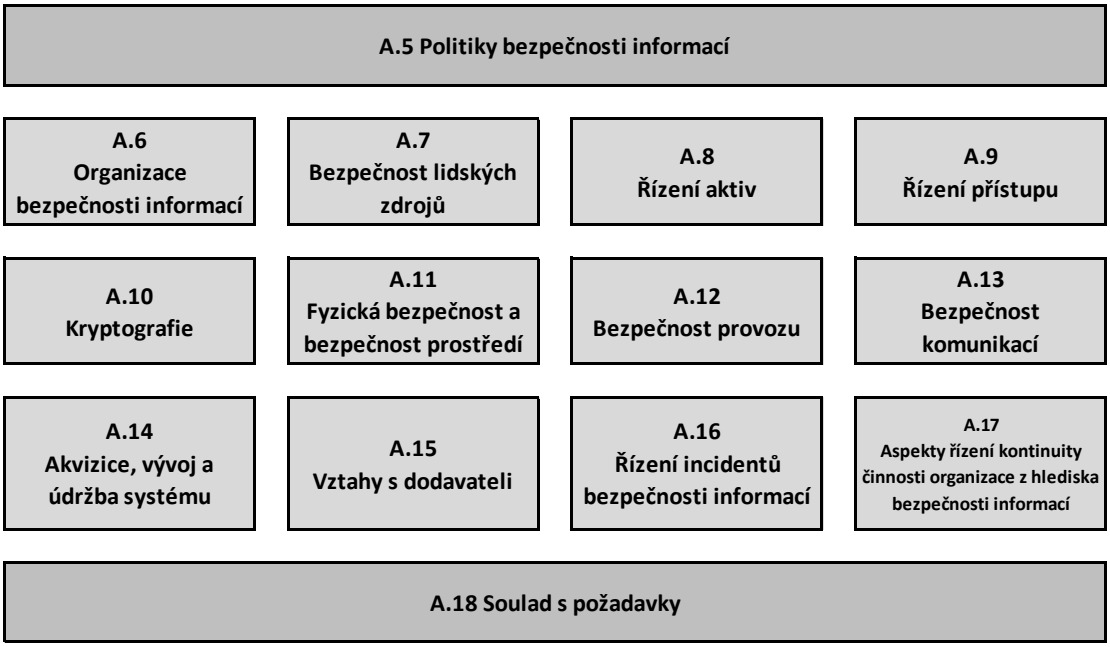
Obrázek č. 7: Rozlišení bezpečnostních opatření [Zdroj: 2, s. 100]

1.7.1 Výběr opatření

Bezpečnostní opatření mohou být vybrána z dostupných norem či metodik nebo mohou být navržena nová bezpečnostní opatření dle specifických potřeb organizace [11].

„Výběr opatření je závislý na organizačních rozhodnutích na základě kritérií pro přijetí rizika, možností ošetření rizika a obecného přístupu k řízení rizik platícího pro organizaci, a měl by také podléhat veškeré příslušné národní a mezinárodní legislativě a nařízení. Výběr opatření závisí také na způsobu, jakým na sebe opatření vzájemně působí, aby poskytovala hloubkovou ochranu“ [11, s. 8].

Norma ISO/IEC 27002 obsahuje 114 bezpečnostních opatření rozdělených do 14 oblastí [11].



Obrázek č. 8: Oblasti ISMS dle normy ISO/IEC 27002 [Zdroj: Vlastní zpracování dle: 11]

2 ANALÝZA SOUČASNÉHO STAVU

V této kapitole představím společnost, pro kterou budu zpracovávat návrh zavedení bezpečnostních opatření v souladu se systémem řízení informační bezpečnosti. Představím společnost, popíši její současný stav z pohledu bezpečnosti rozdělený do několika oblastí a provedu analýzu bezpečnostních opatření za pomoci podpůrného materiálu.

2.1 Představení společnosti

Společnost si nepřeje být jmenována ani býti identifikovatelná z informací uvedených v této práci z důvodu povahy tématu. Ve své práci tedy nebudu uvádět exaktní název společnosti a informace, které by mohly vést k její identifikaci. Informace, které v mé práci o společnosti použiji, můžou být z výše popsaného důvodu modifikované.

Společnost, jejíž správní forma je společnost s ručením omezeným, poskytuje profesionální služby v oblastech softwarový vývoj a integrace, quality assurance, support a konzultace. Své dlouholeté zkušenosti z těchto oblastí úspěšně uplatňuje v různých segmentech trhu jako jsou telekomunikace, pojišťovnictví a finančnictví, průmyslová výroba, služby, zpracování odpadu a logistika. Společnost působí na území České i Slovenské republiky.

Více než dvě třetiny procesů a činností, které jsou ve společnosti nastaveny, jsou řízeny formou projektů. Jedná se tedy o projektově orientovanou společnost s maticovou organizační strukturou. Ta je tvořena vedením společnosti, vedoucími oddělení, projektovými manažery a jednotlivými pracovníky.

Softwarová společnost dosahuje ročního obratu několika stovek milionů korun. Na území České a Slovenské republiky má několik poboček. Tato práce bude zaměřena na pobočku sídlící v Brně, která tvoří polovinu ročního obratu společnosti. Tato pobočka v současné

době zaměstnává přibližně 140 pracovníků. Ti jsou tvořeni převážně vývojáři, aplikačními administrátory, konzultanty a projektovými manažery.

2.1.1 ICT infrastruktura

Kancelářský prostor společnosti se nachází v pronajaté dvoupatrové budově v centru Brna. V tomto prostoru má každý zaměstnanec přiděleno své pracovní místo, kterému přináleží datová zásuvka se dvěma přípojnými místy. Zaměstnanci k práci využívají firemní přenosný osobní počítač s periferiemi. Celý kancelářský prostor je pokryt bezdrátovou sítí.

I přesto, že je společnost dlouhodobě zlatým partnerem společnosti Microsoft, z čehož vyplývá řada licenčních výhod, není ICT infrastruktura postavená výhradně na produktech této společnosti. Více než polovina zaměstnanců má na svém osobním počítači nainstalovaný operační systém Windows 10. Zbylá část zaměstnanců preferuje linuxové distribuce (Debian, Fedora nebo Ubuntu). U serverových operačních systémů převládají linuxové distribuce (CentOS a Ubuntu).

Společnost se v minulosti potýkala s nepravidelnými výpadky síťové infrastruktury. Vedení společnosti se proto rozhodlo přemístit produkční servery do cloudu. Od této doby začala společnost hojně využívat služeb cloud computingu (IaaS, PaaS a SaaS). Zbylá část serverů, převážně vývojářských a testovacích, běží ve virtuálním prostředí na fyzických serverech umístěných v uzamykatelné místnosti v prostoru budovy. Společnost má také pronajatý virtuální privátní server, na kterém poskytuje služby zákazníkům.

Celá ICT infrastruktura je monitorována dohledovým systémem Zabbix, který proaktivně informuje IT oddělní o nestandardních stavech. Systém také poskytuje data pro měření SLA a vyhodnocování kvality interních a externích služeb.

2.2 Současný stav bezpečnosti

V této podkapitole popíši současný stav společnosti z pohledu bezpečnosti rozdělený do několika oblastí.

2.2.1 Fyzická bezpečnost a bezpečnost prostředí

Kancelářský prostor společnosti se nachází v pronajaté dvoupatrové budově v centru Brna. K budově náleží krytá parkovací stání ve dvorním traktu. Bezpečnostní perimetr mezi dvorním traktem a veřejným prostorem je vymezen zdmi a garážovými vraty, které lze ovládat pouze pomocí dálkového ovládání nebo mobilního telefonu. Celý prostor je monitorován kamerovým systémem se záznamem.

Fyzický přístup do budovy, respektive do kancelářského prostoru, je zajištěn dvěma způsoby. Je zajištěn vchodovými dveřmi, které nelze z vnější strany otevřít jinak než klíčem, a poplachovým zabezpečovacím a tísňovým systémem (PZTS), který identifikuje osoby na základě otisku prstu. V kancelářích a na chodbách jsou rozmístěna pohybová čidla, která jsou napojena na tento systém. Každý zaměstnanec pracující na plný nebo zkrácený úvazek má k dispozici svůj vlastní klíč a zaregistrovaný otisk prstu, pomocí něhož ovládá PZTS. Návštěvníci a zaměstnanci, kteří mají uzavřenou dohodu o provedení práce se zájmem vstoupit do kancelářského prostoru, využívají zvonek u vchodových dveří. Recepční za pomoci zvonku s kamerou a mikrofonem provede kontrolu osoby. Pokud se jedná o návštěvníka, je nutné sdělit účel návštěvy. Na základě toho dojde buď k povolení nebo zamítnutí vstupu.

Jednotlivé kanceláře jsou vybaveny posuvnými dveřmi. To však neplatí u kanceláří určených pro práci vedení společnosti, personálnímu a účetnímu oddělení. Tyto kanceláře jsou opatřeny dveřmi s mechanickým zámkem, protože se v nich nacházejí dokumenty a datová média obsahující citlivé informace. Zaměstnanci pracující v těchto oddělení jsou povinni po skončení pracovní doby uzamykat tento prostor.

Místnost s datovým rozvaděčem je uzamykatelná a umístěna tak, aby v jejím okolí nebylo žádné vodovodní potrubí. Vstup do ní je povolen pouze oprávněným osobám. V místnosti se nachází servery, datová úložiště a aktivní prvky sítě. Všechna tato zařízení jsou připojena ke zdroji nepřerušovaného napájení (UPS), který je v případě výpadku elektrické energie vydrží napájet po určitou dobu. Zařízení, která zaměstnanci využívají ke své každodenní práci, jsou umístěna tak, aby se minimalizovalo riziko fyzického poškození, neoprávněného přístupu a sledování. Vedení silových a telekomunikačních kabelových rozvodů je vzájemně odděleno.

2.2.2 Bezpečnost komunikace a přenosu dat

Pro ochranu bezpečnosti sítě je zajištěna její segmentace. Segmentace zejména použitím virtuálních LAN a demilitarizované zóny. Blokování nežádoucí komunikace je aktivně řešeno na úrovni firewallu. Ve společnosti není zaveden systém pro centralizovanou správu a analýzu logů, proto je veškerý provoz na síti je zaznamenáván do logů, které jsou uchovávány v jednotlivých aktivních prvcích, operačních systémech a serverech.

Společnost pro svůj chod využívá řadu serverů, které jsou děleny dle prostředí na produkční, vývojové a testovací. Administrátoři i vývojáři se k jednotlivým serverům připojují přes SSH. Servery jsou zabezpečeny osobní firewallem a u linuxových distribucí je navíc zapnut SELinux. Všechny servery, které jsou dostupné z vnější sítě, jsou umístěny do demilitarizované zóny. Produkční servery jsou pravidelně automaticky zálohovány. Zálohy jsou jednou týdně přesouvány na externí disk, který je umístěn mimo budovu společnosti.

Kancelářský prostor je pokryt bezdrátovou sítí s odděleným přístupem pro návštěvníky a zaměstnance společnosti. Přístup k interní bezdrátové síti je zabezpečen protokolem IEEE 802.1X ve spolupráci s FreeRADIUS serverem. Autentizace probíhá pomocí doménového uživatelského jména a hesla. Zaměstnancům je umožněn vzdálený přístup do interní sítě. Ve společnosti je zavedena OpenVPN, která používá pro autentizaci uživatelů TLS certifikáty.

Povinností každého zaměstnance je mít chráněna data na svém osobním počítači, a to v zásadě dvěma možnosti – zamčením disku heslem nebo šifrováním celého disku za pomoci specializovaného softwaru např. Bitlocker nebo VeraCrypt. Použití antivirového programu je na zvážení každého zaměstnance. Ti, kteří mají na svém osobním počítači nainstalovaný operační systém Windows, jsou chránění výchozím antivirovým programem Windows Defender.

2.2.3 Bezpečnost lidských zdrojů a řízení přístupu

Společnost zveřejňuje volné pracovní pozice na svých internetových stránkách. Uchazeč před odesláním životopisu musí zaškrtnout políčko, kterým dává souhlas, že byl seznámen se zásadami zpracování osobních údajů pro výběrové řízení. Výběrové řízení je zpravidla dvoukolové. Prvnímu kolu předchází krátký pohovor po telefonu, kdy personalistka zjišťuje uchazečovo očekávaní od pozice, mzdovou představu a možný nástup do zaměstnání. V prvním kole je uchazeči podrobněji představena společnost a pozice, je také ověřena úroveň cizího jazyka. Formou malých úkolů a her je testováno kreativní a analytické myšlení. U některých pozic je vyžadováno vypracování programátorského testu, který ověřuje praktické znalosti. V případě úspěšného absolvování prvního kola, je uchazeč pozván do kola druhého, které se zaobírá technickými otázkami a je vedeno jeho potenciálním budoucím nadřízeným.

Po nalezení vhodného uchazeče se postupuje podle stanovených pravidel. S úspěšným uchazečem uzavírá jednatel společnosti pracovní smlouvu, která mimo jiné obsahuje i povinnost mlčenlivosti a ochranu obchodního tajemství, a to i po skončení pracovního poměru. Nový zaměstnanec je seznámen s pracovními podmínkami, svými právy a povinnostmi. Zaměstnanec také dává svým podpisem souhlas se zpracováním osobních údajů během pracovního poměru.

Po podepsání pracovní smlouvy zadá personální oddělení do interního informačního systému požadavek na vytvoření přístupu pro nového zaměstnance. IT oddělení převezme

požadavek a na základě uvedených informací vytvoří přístupy v adresářové službě Active Directory. Podle pracovní pozice jsou následně zaměstnanci přidělena přístupová práva.

V den nástupu si zaměstnanec vyzvedne svůj osobní počítač včetně příslušenství. IT oddělení mu zajistí přístup do budovy, který spočívá v sejmutí otisku prstu a provede školení na PZTS.

Při ukončení pracovního poměru se postupuje podle vytyčených pravidel. Ta v sobě zahrnují povinnosti navrátit veškerá svěřená hardwarová aktiva, přesměrování e-mailu, revokování certifikátu, odebrání přístupových práv a zablokování veškerých přístupů. Odcházející zaměstnanec je povinen dodržovat podmínky, které byly sjednány v pracovní smlouvě (povinnost mlčenlivosti a ochrana obchodního tajemství).

2.3 Asistované zhodnocení

Cílem asistovaného zhodnocení je získat přehled o bezpečnostních opatření ve společnosti. K analýze byla přiměřeně použita „Pomůcka k auditu bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.“. Jedná se o podpůrný materiál používaný Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). Analýza dle podpůrného materiálu byla provedena kompletně, nicméně do diplomové práce jsem vybral pouze její stěžejní části.

Šablona provedené analýzy:

Požadavek	
Stav	*Komentář*

Položka **stav** má definovány čtyři možnosti:

zavedeno
částečně zavedeno
nezavedeno
nerelevantní

2.3.1 ISMS

Je stanoven rozsah ISMS.
nezavedeno
Jsou stanoveny cíle ISMS.
nezavedeno
Je zaveden proces řízení rizik.
nezavedeno
Jsou vytvořeny, schváleny a zavedeny bezpečnostní politiky v oblasti ISMS, zavedena příslušná bezpečnostní opatření.
nezavedeno
Je prováděn audit kybernetické bezpečnosti u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti“).
nezavedeno
Zajištěno pravidelné vyhodnocení účinnosti ISMS, které obsahuje hodnocení stavu ISMS včetně revize hodnocení rizik, posouzeny výsledky provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na ISMS.
nezavedeno
Je prováděna aktualizace ISMS a související dokumentace na základě zjištění auditů kybernetické bezpečnosti, výsledků hodnocení účinnosti ISMS a v souvislosti s prováděnými významnými změnami.
nezavedeno
Řízen provoz a zdroje ISMS, zaznamenávány činnosti spojené s ISMS a řízením rizik.
nezavedeno

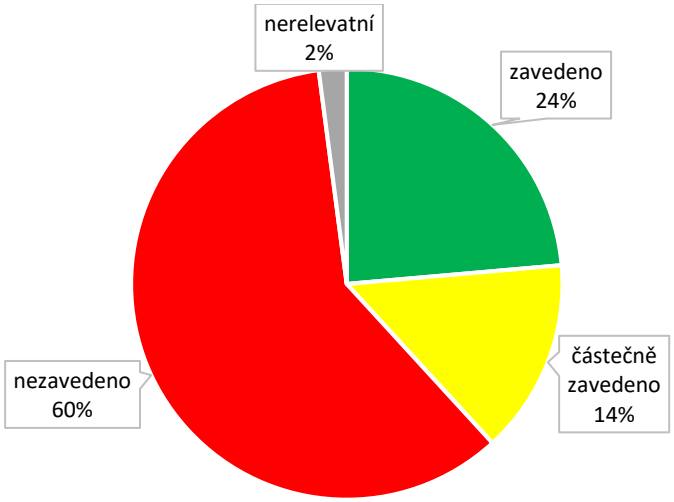
2.3.2 Řízení aktiv

Jsou identifikována a evidována aktiva.	
zavedeno	
Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za aktiva.	
zavedeno	
Je hodnocena důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a tato aktiva jsou zařazena do jednotlivých úrovní.	
částečně zavedeno	*Aktiva jsou pouze hodnocena, rozřazení chybí.*
Jsou určeny a evidovány vazby mezi primárními a podpůrnými aktivy a hodnoceny důsledky závislostí mezi primárními a podpůrnými aktivy.	
nezavedeno	
Při hodnocení důležitosti primárních aktiv je posouzeno především: - rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství, - rozsah dotčených právních povinností nebo jiných závazků, - rozsah narušení vnitřních řídících a kontrolních činností, - poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty, - dopady na poskytování důležitých služeb, - rozsah narušení běžných činností, - dopady na zachování dobrého jména nebo ochranu dobré pověsti, - dopady na bezpečnost a zdraví osob, - dopady na mezinárodní vztahy, - dopady na uživatele informačního a komunikačního systému.	
částečně zavedeno	*Posouzena malá část z výše uvedeného.*

Asistované zhodnocení v plném rozsahu je k dispozici v **příloze č. 4**.

2.3.3 Výstup asistovaného zhodnocení

Na základě provedené analýzy bezpečnostních opatření byly zjištěny následující skutečnosti. Společnost z celkového počtu 144 požadavků splňuje 34, částečně splňuje 21, nesplňuje 86 a 3 požadavky jsou pro ni nerelevantní.



Graf č. 1: Grafický výstup asistovaného zhodnocení [Zdroj: Vlastní zpracování]

2.4 Souhrn asistovaného zhodnocení k opatřením ISMS

Asistované zhodnocení je převedeno na jednotlivá opatření ISMS, která jsou převzata z normy ČSN EN ISO/IEC 27001:2017. Níže uvedená tabulka představuje jednotlivá opatření a jejich stav plnění na základě zjištěných informací z asistovaného zhodnocení. Tímto dostáváme přesný popis současného stavu bezpečnostních opatření v souladu s ISMS ve společnosti.

Tabulka č. 1: Souhrn asistovaného zhodnocení k opatřením ISMS [Zdroj: Vlastní zpracování dle: 10]

A.5	**Politiky bezpečnosti informací**	
A.5.1	**Směřování bezpečnosti informací vedením organizace**	
A.5.1.1	Politiky pro bezpečnost informací	**nezavedeno**
A.5.1.2	Přezkoumávání politik pro bezpečnost informací	**nezavedeno**
A.6	**Organizace bezpečnosti informací**	
A.6.1	**Interní organizace**	
A.6.1.1	Role a odpovědnosti bezpečnosti informací	**nezavedeno**
A.6.1.2	Princip oddělení povinností	**nezavedeno**
A.6.1.3	Kontakt s příslušnými orgány a autoritami	**nezavedeno**
A.6.1.4	Kontakt se zájmovými skupinami	**nezavedeno**
A.6.1.5	Bezpečnost informací v řízení projektů	**nezavedeno**
A.6.2	**Mobilní zařízení a práce na dálku**	
A.6.2.1	Politika mobilních zařízení	**nezavedeno**
A.6.2.2	Práce na dálku	**částečně zavedeno**
A.7	**Bezpečnost lidských zdrojů**	
A.7.1	**Před vznikem pracovního vztahu**	
A.7.1.1	Prověřování	**částečně zavedeno**
A.7.1.2	Podmínky pracovního vztahu	**zavedeno**
A.7.2	**Během pracovního vztahu**	
A.7.2.1	Odpovědnost vedení organizace	**částečně zavedeno**
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	**nezavedeno**
A.7.2.3	Disciplinární řízení	**částečně zavedeno**
A.7.3	**Ukončení a změna pracovního vztahu**	
A.7.3.1	Odpovědnost při ukončení nebo změně pracovního vztahu	**zavedeno**
A.8	**Řízení aktiv**	
A.8.1	**Odpovědnost za aktiva**	
A.8.1.1	Seznam aktiv	**zavedeno**
A.8.1.2	Vlastnictví aktiv	**zavedeno**
A.8.1.3	Přípustné použití aktiv	**nezavedeno**
A.8.1.4	Navrácení aktiv	**zavedeno**
A.8.2	**Klasifikace informací**	
A.8.2.1	Klasifikace informací	**nezavedeno**
A.8.2.2	Označování informací	**nezavedeno**
A.8.2.3	Manipulace s aktivy	**nezavedeno**
A.8.3	**Manipulace s médii**	
A.8.3.1	Správa výměnných médií	**nezavedeno**
A.8.3.2	Likvidace médií	**nezavedeno**
A.8.3.3	Přeprava fyzických médií	**nezavedeno**
A.9	**Řízení přístupu**	
A.9.1	**Požadavky organizace na řízení přístupu**	
A.9.1.1	Politika řízení přístupu	**částečně zavedeno**
A.9.1.2	Přístup k sítím a síťovým službám	**zavedeno**
A.9.2	**Řízení přístupu uživatelů**	

A.9.2.1	Registrace a zrušení registrace uživatele	**zavedeno**
A.9.2.2	Správa uživatelských přístupů	**zavedeno**
A.9.2.3	Správa privilegovaných přístupových práv	**zavedeno**
A.9.2.4	Správa tajných autentizačních informací uživatelů	**zavedeno**
A.9.2.5	Přezkoumávání přístupových práv uživatelů	**částečně zavedeno**
A.9.2.6	Odebrání nebo úprava přístupových práv	**zavedeno**
A.9.3	**Odpovědnost uživatelů**	
A.9.3.1	Používání tajných autentizačních informací	**částečně zavedeno**
A.9.4	**Řízení přístupu k systémům a aplikacím**	
A.9.4.1	Omezení přístupu k informacím	**zavedeno**
A.9.4.2	Bezpečné postupy přihlášení	**zavedeno**
A.9.4.3	Systém správy hesel	**částečně zavedeno**
A.9.4.4	Použití privilegovaných programových nástrojů	**nezavedeno**
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	**zavedeno**
A.10	**Kryptografie**	
A.10.1	**Kryptografická opatření**	
A.10.1.1	Politiky pro použití kryptografických opatření	**nezavedeno**
A.10.1.2	Správa klíčů	**zavedeno**
A.11	**Fyzická bezpečnost a bezpečnost prostředí**	
A.11.1	**Bezpečné oblasti**	
A.11.1.1	Fyzický bezpečnostní perimetr	**zavedeno**
A.11.1.2	Fyzické kontroly vstupu	**zavedeno**
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	**zavedeno**
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	**zavedeno**
A.11.1.5	Práce v bezpečných oblastech	**zavedeno**
A.11.1.6	Oblasti pro nakládku a vykládku	**nerelevantní**
A.11.2	**Zařízení**	
A.11.2.1	Umístění zařízení a jeho ochrana	**částečně zavedeno**
A.11.2.2	Podpůrné služby	**nezavedeno**
A.11.2.3	Bezpečnost kabelových rozvodů	**zavedeno**
A.11.2.4	Údržba zařízení	**nezavedeno**
A.11.2.5	Přemístění aktiv	**nezavedeno**
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory	**částečně zavedeno**
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	**nezavedeno**
A.11.2.8	Uživatelská zařízení bez obsluhy	**nezavedeno**
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	**nezavedeno**
A.12	**Bezpečnost provozu**	
A.12.1	**Provozní postupy a odpovědnosti**	
A.12.1.1	Dokumentované provozní postupy	**částečně zavedeno**
A.12.1.2	Řízení změn	**částečně zavedeno**
A.12.1.3	Řízení kapacit	**zavedeno**
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	**zavedeno**
A.12.2	**Ochrana proti malwaru**	
A.12.2.1	Opatření proti malwaru	**nezavedeno**
A.12.3	**Zálohování**	

A.12.3.1	Zálohování informací	**částečně zavedeno**
A.12.4	**Zaznamenávání formou logů a monitorování**	
A.12.4.1	Zaznamenávání událostí formou logů	**zavedeno**
A.12.4.2	Ochrana logů	**částečně zavedeno**
A.12.4.3	Logy o činnosti administrátorů a operátorů	**částečně zavedeno**
A.12.4.4	Synchronizace hodin	**nezavedeno**
A.12.5	**Správa provozního softwaru**	
A.12.5.1	Instalace softwaru na provozní systémy	**částečně zavedeno**
A.12.6	**Řízení technických zranitelností**	
A.12.6.1	Řízení technických zranitelností	**částečně zavedeno**
A.12.6.2	Omezení instalace softwaru	**částečně zavedeno**
A.12.7	**Hlediska auditu informačních systémů**	
A.12.7.1	Opatření k auditu informačních systémů	**částečně zavedeno**
A.13	**Bezpečnost komunikací**	
A.13.1	**Správa bezpečnosti sítě**	
A.13.1.1	Opatření v sítích	**zavedeno**
A.13.1.2	Bezpečnost síťových služeb	**zavedeno**
A.13.1.3	Princip oddělení v sítích	**zavedeno**
A.13.2	**Přenos informací**	
A.13.2.1	Politiky a postupy při přenosu informací	**nezavedeno**
A.13.2.2	Dohody o přenosu informací	**nezavedeno**
A.13.2.3	Elektronické předávání zpráv	**nezavedeno**
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	**nezavedeno**
A.14	**Akvizice, vývoj a údržba systémů**	
A.14.1	**Bezpečnostní požadavky informačních systémů**	
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	**částečně zavedeno**
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	**částečně zavedeno**
A.14.1.3	Ochrana transakcí aplikačních služeb	**částečně zavedeno**
A.14.2	**Bezpečnost v procesech vývoje a podpory**	
A.14.2.1	Politika bezpečného vývoje	**nezavedeno**
A.14.2.2	Postupy řízení změn systémů	**částečně zavedeno**
A.14.2.3	Technické přezkoumávání aplikací po změnách provozní platformy	**částečně zavedeno**
A.14.2.4	Omezení změn softwarových balíků	
A.14.2.5	Principy budování bezpečných systémů	**částečně zavedeno**
A.14.2.6	Prostředí bezpečného vývoje	**částečně zavedeno**
A.14.2.7	Outsourcovaný vývoj	**částečně zavedeno**
A.14.2.8	Testování bezpečnosti systémů	**částečně zavedeno**
A.14.2.9	Testování akceptace systémů	**částečně zavedeno**
A.14.3	**Data pro testování**	
A.14.3.1	Ochrana dat pro testování	**částečně zavedeno**
A.15	**Dodavatelské vztahy**	
A.15.1	**Bezpečnost informací v dodavatelských vztazích**	
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	**nezavedeno**
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	**částečně zavedeno**

A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	**nezavedeno**
A.15.2	**Řízení dodávek služeb dodavatelů**	
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	**nezavedeno**
A.15.2.2	Řízení změn ve službách dodavatelů	**nezavedeno**
A.16	**Řízení incidentů bezpečnosti informací**	
A.16.1	**Řízení incidentů bezpečnosti informací a zlepšování**	
A.16.1.1	Odpovědnosti a postupy	**nezavedeno**
A.16.1.2	Hlášení událostí bezpečnosti informací	**nezavedeno**
A.16.1.3	Hlášení slabých míst bezpečnosti informací	**nezavedeno**
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	**nezavedeno**
A.16.1.5	Reakce na incidenty bezpečnosti informací	**nezavedeno**
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	**nezavedeno**
A.16.1.7	Shromažďování důkazů	**nezavedeno**
A.17	**Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací**	
A.17.1	**Kontinuita bezpečnosti informací**	
A.17.1.1	Plánování kontinuity bezpečnosti informací	**nezavedeno**
A.17.1.2	Implementace kontinuity bezpečnosti informací	**nezavedeno**
A.17.1.3	Verifikace, přezkoumávání a vyhodnocení kontinuity bezpečnosti informací	**nezavedeno**
A.17.2	**Redundance**	
A.17.2.1	Dostupnost vybavení pro zpracování informací	**nezavedeno**
A.18	**Soulad s požadavky**	
A.18.1	**Soulad s právními a smluvními požadavky**	
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	**zavedeno**
A.18.1.2	Ochrana duševního vlastnictví	**zavedeno**
A.18.1.3	Ochrana záznamů	**zavedeno**
A.18.1.4	Soukromí a ochrana osobních údajů	**zavedeno**
A.18.1.5	Regulace kryptografických opatření	**nezavedeno**
A.18.2	**Přezkoumávání bezpečnosti informací**	
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	**nezavedeno**
A.18.2.2	Shoda s bezpečnostními politikami a normami	**nezavedeno**
A.18.2.3	Přezkoumávání technické shody	**nezavedeno**

2.5 Požadavky společnosti

Vedení společnosti bylo seznámeno s výstupem asistovaného zhodnocení a souhrnem asistovaného zhodnocení k opatřením ISMS. Na základě těchto informací se vedení rozhodlo řešit aktuální situaci informační bezpečnosti ve společnosti a stanovilo následující požadavky:

- provést analýzu rizik,
- navrhnout bezpečnostní opatření jejichž stav plnění je „nezavedeno“,
- navrhnout bezpečnostní opatření pro zvládání největších rizik,
- zvýšit bezpečnostní povědomí u zaměstnanců,
- zvýšit informační bezpečnost ve společnosti.

2.6 Shrnutí analýzy

V kapitole týkající se analýzy současného stavu byla představena společnost, popsán její současný stav z pohledu bezpečnosti a ve spolupráci s vedením společnosti bylo vyplněno asistované zhodnocení. Vyplněné asistované zhodnocení bylo následně převedeno na jednotlivá opatření ISMS převzatá z normy ČSN EN ISO/IEC 27001:2017. Tímto postupem byl získán přesný popis současného stavu bezpečnostních opatření v souladu s ISMS ve společnosti. Výstup asistovaného zhodnocení včetně souhrnu asistovaného zhodnocení k opatřením ISMS bylo představeno vedení společnosti, které se na základě předložených materiálů rozhodlo řešit aktuální situaci informační bezpečnosti ve společnosti.

Z analýzy je zřejmé, že společnost nemá zavedený systém řízení informační bezpečnosti a neřídí systematicky informační bezpečnost. Existuje však několik směrnic zaměřující se na ochranu osobních údajů, bezpečnost komunikační sítě a fyzickou bezpečnost. Společnost splňuje požadavky vycházející z Obecného nařízení o ochraně osobních údajů (GDPR), které nabylo účinnosti 25. května 2018. Je jmenován tzv. pověřenec pro ochranu osobních údajů neboli DPO, který tuto pozici zastává externě.

I přesto, že se jedná o softwarovou společnost, která zaměstnává převážně vývojáře, aplikační administrátory, konzultanty, projektové manažery – tedy na první pohled počítačově gramotné osoby, je bezpečnostní povědomí zaměstnanců na nízké úrovni. Chybí pozice manažera informační bezpečnosti (CISO) včetně jeho zavedení do organizační struktury, který by řídil informační bezpečnost ve společnosti a měl na starosti budování bezpečnostního povědomí u zaměstnanců.

Cílem mé práce bude dodržet požadavky vedení společnosti a zpracovat návrh zavedení bezpečnostních opatření v souladu s ISMS. Vzhledem k počtu nezavedených bezpečnostních opatření se nabízí jako nejvýhodnější varianta rozdělit zavedení do dvou etap.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V této kapitole se budu zabývat samotným návrhem zavedení bezpečnostních opatření v souladu se systémem řízení informační bezpečnosti. Při návrhu vlastního řešení budu vycházet z teoretických východisek, z poznatků získaných z analýzy současného stavu a budu také brát v potaz požadavky vedení společnosti.

3.1 Rozsah a hranice

Na úvod je třeba říci, že společnost v dohledné době neplánuje zavádět v plném rozsahu ISMS ani usilovat o certifikaci. Z toho důvodu není nutné zavádět všechna bezpečnostní opatření normy ČSN EN ISO/IEC 27001:2017. Rozsah, který mimo jiné vyšel také z asistovaného hodnocení, je stanoven pouze na vybraná bezpečnostní opatření pro zvládání největších zjištěných rizik (těch s největším dopadem) a požadavků vedení společnosti.

3.2 Analýza rizik

Analýza rizik začíná identifikací aktiv a jejich ohodnocením. Následně jsou identifikovány hrozby a zranitelnosti. Na závěr je vypracována matice rizik a provedeno vyhodnocení analýzy rizik. Při analýze rizik budu vycházet z informací zjištěných při analýze současného stavu a také z dodatečných informací, které byly zjištěny po konzultacích s vedením společnosti, vlastníky (garanty) a uživateli daných aktiv.

Umístění analýzy rizik do návrhové části má své opodstatnění. Jelikož společnost v současné době neprovádí analýzu rizik, bude tato analýza zároveň sloužit jako návrh k politice řízení rizik.

3.2.1 Identifikace a ohodnocení aktiv

Aktiva je nejprve potřeba identifikovat a následně ohodnotit. Identifikace byla prováděna v součinnosti s vedením společnosti. Identifikovaná aktiva jsou rozdělena do čtyř skupin – informační, hardwarová, softwarová aktiva a služby. V rámci identifikace byly identifikováni i jednotliví vlastníci aktiv, kteří odpovídají za jejich stav a činnost. Nicméně vzhledem k povaze diplomové práce tyto informace nebudou uvedeny.

Ohodnocení aktiv je provedeno dle klasifikačního schématu pro hodnocení aktiv. Jednotlivá aktiva jsou hodnocena podle nákladů vzniklých v důsledku narušení tří hlavních atributů informační bezpečnosti – důvěrnosti, integrity a dostupnosti. Hodnotící škála jednotlivých atributů je vyjádřena na stupnici od 1 do 5. Význam ohodnocení je patrný z následující tabulky.

Tabulka č. 2: Klasifikační schéma pro hodnocení aktiv [Zdroj: Vlastní zpracování dle: 2]

Klasifikační stupeň	Klasifikační kritérium (dopad na organizaci)
1	žádný dopad
2	zanedbatelný dopad
3	potíže či finanční ztráty
4	vážné potíže či podstatné finanční ztráty
5	existenční potíže

Výsledná hodnota aktiva je vypočtena pomocí tzv. součtového algoritmu:

$$\boldsymbol{hodnota\ aktiva} = \frac{\boldsymbol{důvěrnost} + \boldsymbol{integrita} + \boldsymbol{dostupnost}}{\mathbf{3}}$$ [2].

Tabulka č. 3: Identifikace a ohodnocení aktiv [Zdroj: Vlastní zpracování]

Typ	Aktivum	Zdroj	C	I	A	H
INFORMAČNÍ AKTIVA	Data o zákaznících	*IS*	5	5	4	5
	Data o zaměstnancích	*IS*	5	4	3	4
	Interní data	*IS, servery*	5	5	4	5
	Zdrojové kódy	*servery (GitLab)*	4	5	4	4
	Zálohy dat	*servery*	4	4	4	4
		cloud	4	4	4	4
HARDWAROVÁ AKTIVA	Pracovní stanice		3	2	3	3
	Servery		4	5	5	5
	Tiskárny		1	1	2	1
	Notebooky		3	3	3	3
	Mobilní zařízení		2	2	2	2
	Síťová infrastruktura	*pasivní síťové prvky*	3	3	3	3
		aktivní síťové prvky	3	3	3	3
	Datové úložiště	*synology*	4	3	3	3
	Elektronické nosiče	*USB flash disky*	2	1	1	1
	Kamerový systém	*servery*	2	2	2	2
	Zabezpečovací systém (PZTS)	*servery*	2	2	2	2
SOFTWAROVÁ AKTIVA	Operační systémy	*servery*	3	3	4	3
		pracovní stanice	2	2	3	2
		notebooky	2	2	3	2
	Informační systém (IS)	*servery*	5	5	5	5
	JIRA (systém pro vývoj SW)	*servery*	4	4	4	4
	Confluence (intranet)	*servery*	4	4	3	4
	GitLab (verzování kódu)	*servery*	4	5	4	4
	Účetní software	*servery*	4	3	2	3
	PZTS software	*servery*	2	3	2	2
	Software IP kamer	*servery*	1	1	1	1
SLUŽBY	Internetové připojení	*cloud*	3	4	4	4
		pobočka	3	4	4	4
	Elektrická energie	*cloud*	4	4	4	4
		pobočka	4	4	4	4
	Elektronická pošta	*office 365*	3	3	3	3
	Webové stránky	*servery*	2	3	3	3
	Cloud computing		5	5	4	5
	Vzdálené připojení (VPN)		4	4	4	4
	Údržba, servis	*interní IT oddělení*	3	2	2	2

Aby bylo možné předložit tabulku v plném rozsahu, byly upraveny názvy atributů informační bezpečnosti na anglické zkratky: C – důvěrnost, I – integrita, A – dostupnost. Poslední sloupec tabulky představuje výslednou hodnotu aktiva.

Z identifikace a ohodnocení aktiv vyplývá, že pro společnost je nejdůležitějším aktivem interně vyvíjený informační systém, který v sobě uchovává data o zákaznících, zaměstnancích a také interní data společnosti.

Dalším neméně důležitým aktivem jsou servery, na nichž je provozován informační systém a další softwarové nástroje (JIRA, Confluence a GitLab), které jsou každodenně využívány při vývoji softwaru.

3.2.2 Identifikace hrozeb a zranitelností

Po identifikaci a ohodnocení aktiv je zapotřebí identifikovat hrozby, před kterými je třeba aktiva chránit, a určit pravděpodobnost jejich výskytu. Identifikace hrozeb i s příklady zranitelnosti je založena a vychází z normy ČSN ISO/IEC 27005:2013. Především byly vybrány hrozby s co největší pravděpodobností reálného výskytu v kontextu společnosti. Pravděpodobnost výskytu hrozby je provedeno dle klasifikačního schématu. Hodnotící škála jednotlivých pravděpodobností je vyjádřena na stupnici od 1 do 5. Význam jednotlivých klasifikačních stupňů je patrný z následující tabulky.

Tabulka č. 4: Klasifikační schéma pravděpodobnosti výskytu hrozby [Zdroj: Vlastní zpracování dle 2]

Klasifikační stupeň	Klasifikační kritérium (pravděpodobnost)
1	nahodilá
2	nepravděpodobná
3	pravděpodobná
4	velmi pravděpodobná
5	trvalá

Tabulka č. 5: Identifikace hrozeb [Zdroj: Vlastní zpracování]

Typ	Hrozba
FYZICKÉ POŠKOZENÍ	Požár
	Poškození vodou
	Znečištění
	Zničení zařízení nebo médií
PŘÍRODNÍ UDÁLOSTI	Povodeň
ZTRÁTA ZÁKLADNÍCH SLUŽEB	Selhání klimatizace nebo dodávky vody
	Přerušení dodávky elektřiny
	Selhání telekomunikačního zařízení
OHROŽENÍ INFORMACÍ	Vzdálená špionáž
	Krádež médií nebo dokumentů
	Krádež zařízení
	Zprovoznění recyklovaných nebo vyřazených médií
	Vyzrazení
	Data pocházející z nedůvěryhodných zdrojů
	Falšování pomocí technického vybavení
	Falšování pomocí aplikačního programového vybavení
	Odhalení pozice
TECHNICKÉ SELHÁNÍ	Selhání zařízení
	Chybné fungování zařízení
	Chybné fungování aplikačního programového vybavení
	Chyba údržby
NEOPRÁVNĚNÉ ČINNOSTI	Neoprávněné použití zařízení
	Podvodné kopírování aplikačního programového vybavení
	Poškození dat
	Nezákonné zpracování dat
OHROŽENÍ FUNKČNOSTI	Chyba v používání
	Zneužití oprávnění
	Odepření činností

Tabulka č. 6: Identifikace hrozeb s pravděpodobností a příkladem zranitelnosti [Zdroj: Vlastní zpracování]

Hrozba	P	Příklad zranitelnosti
Požár	2	Hořlavost kabelových spojení
Poškození vodou	1	Špatná těsnost střechy
Znečištění	3	Nedostatečná údržba
Zničení zařízení nebo médií	2	Nedodržení pravidelné výměny
Povodeň	1	Poloha v zátopové oblasti
Selhání klimatizace nebo dodávky vody	2	Bod totálního selhání
Přerušení dodávky elektřiny	3	Nestabilní elektrická síť
Selhání telekomunikačního zařízení	4	Nekvalitní kabelové spojení
Vzdálená špionáž	2	Přenos odkrytých hesel
Krádež médií nebo dokumentů	3	Nekontrolované kopírování
Krádež zařízení	3	Nedostatečné kontroly zařízení mimo lokalitu
Zprovoznění recyklovaných nebo vyřazených médií	1	Nedostatečné postupy likvidace
Vyzrazení	4	Nejasné odpovědnosti uživatelů
Data pocházející z nedůvěryhodných zdrojů	3	Nedostatky ve formálním procesu pro autorizaci veřejně přístupných informací
Falšování pomocí technického vybavení	4	Neřízený přístup k datové síti
Falšování pomocí aplikačního programového vybavení	4	Nekontrolované stahování a užívání programů
Odhalení pozice	2	Nedostatečná ochrana mobilních telefonů
Selhání zařízení	3	Nedostatky v plánech kontinuity
Chybné fungování zařízení	3	Neexistence dohledové služby, logování událostí
Chybné fungování aplikačního programového vybavení	3	Neodladěný nebo nový program
Chyba údržby	2	Nedostatečná odezva pracovníků údržby systému
Neoprávněné použití zařízení	3	Nechráněné připojení do veřejné sítě
Podvodné kopírování aplikačního programového vybavení	3	Nedostatečné zabezpečení programového vybavení
Poškození dat	3	Široce rozšířené programy
Nezákonné zpracování dat	1	Spuštění nepotřebných služeb
Chyba v používání	3	Nedostatečné bezpečnostní školení
Zneužití oprávnění	4	Chybné přiřazení přístupových práv
Odepření činností	3	Nedostatečné ověřování posílání a přijímání zpráv

3.2.3 Matice zranitelnosti

Matice zranitelnosti vychází z identifikovaných aktiv a hrozeb. Představuje zranitelnost každého z identifikovaných aktiv vůči identifikovaným hrozbám. Pro posouzení závažnosti zranitelnosti je využito klasifikační schéma. Hodnotící škála jednotlivých zranitelností je vyjádřena na stupnici od 1 do 5. Význam jednotlivých klasifikačních stupňů je patrný z následující tabulky.

Tabulka č. 7: Klasifikační schéma pro zranitelnost [Zdroj: Vlastní zpracování dle: 21]

Klasifikační stupeň	Klasifikační kritérium (zranitelnost)
1	velmi nízká
2	nízká
3	střední
4	vysoká
5	kritická

Vzhledem ke specifičnosti a velikosti matice zranitelnosti je na následující straně předložena pouze její část zaměřující se na informační aktiva. Matice zranitelnosti v plném rozsahu je k dispozici v **příloze č. 1**.

Tabulka č. 8: Matice zranitelnosti [Zdroj: Vlastní zpracování]

Zranitelnost [V]		INFORMAČNÍ AKTIVA					
	Zdroj	*IS*	*IS*	*IS, servery*	*servery (GitLab)*	*servery*	*cloud*
	Aktivum	Data o zákaznících	Data o zaměstnancích	Interní data	Zdrojové kódy	Zálohy dat	
	A	5	4	5	4	4	4
Hrozba	**T**						
Požár	2						
Poškození vodou	1						
Znečištění	3						
Zničení zařízení nebo médií	2						
Povodeň	1						
Selhání klimatizace nebo dodávky vody	2						
Přerušení dodávky elektřiny	3	4	4	4	4	4	2
Selhání telekomunikačního zařízení	4	4	4	4	4	3	2
Vzdálená špionáž	2	4	4	4	4	4	4
Krádež médií nebo dokumentů	3	4	4	4	4	2	3
Krádež zařízení	3						
Zprovoznění recyklovaných nebo vyřazených médií	1						
Vyzrazení	4	4	4	4	4	3	3
Data pocházející z nedůvěryhodných zdrojů	3						
Falšování pomocí technického vybavení	4					1	1
Falšování pomocí aplikačního programového vybavení	4					2	2
Odhalení pozice	2						
Selhání zařízení	3						
Chybné fungování zařízení	3						
Chybné fungování aplikačního programového vybavení	3					3	3
Chyba údržby	2						
Neoprávněné použití zařízení	3						
Podvodné kopírování aplikačního programového vybavení	3						
Poškození dat	3	3	3	3	3	4	3
Nezákonné zpracování dat	1	3	4	4	4	3	3
Chyba v používání	3	4	4	4	4	4	3
Zneužití oprávnění	4	3	3	3	3	3	3
Odepření činností	3						

3.2.4 Matice rizik

Matice rizik je sestavena na základě kombinace aktiv a hrozeb. Pro výpočet úrovně rizika je použita maticová metoda se třemi parametry (aktivum, hrozba a pravděpodobnost). Výpočet úrovně rizika vychází z následujícího vztahu:

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

Kde:

- R – úroveň rizika,
- A – hodnota aktiva,
- T – pravděpodobnost vzniku hrozby,
- V – zranitelnost aktiva.

Posouzení závažnosti úrovně jednotlivých rizik je provedeno dle níže uvedeného klasifikačního schématu.

Tabulka č. 9: Klasifikační schéma pro úroveň rizika [Zdroj: Vlastní zpracování dle: 2]

Klasifikační stupeň	Klasifikační kritérium (úroveň rizika)
0-10	bezvýznamné
11-20	akceptovatelné
21-30	nízké
31-60	nežádoucí
61 a více	nepřijatelné

Vzhledem ke specifičnosti a velikosti matice rizik je na následující straně předložena pouze její část zaměřující se na informační aktiva. Matice rizik v plném rozsahu je k dispozici v **příloze č. 2**.

Tabulka č. 10: Matice rizik [Zdroj: Vlastní zpracování]

Úroveň rizika [R]		INFORMAČNÍ AKTIVA					
	Zdroj	*IS*	*IS*	*IS, servery*	*servery (GitLab)*	*servery*	*cloud*
	Aktivum	Data o zákaznících	Data o zaměstnancích	Interní data	Zdrojové kódy	Zálohy dat	
	A	5	4	5	4	4	4
Hrozba	**T**						
Požár	2						
Poškození vodou	1						
Znečištění	3						
Zničení zařízení nebo médií	2						
Povodeň	1						
Selhání klimatizace nebo dodávky vody	2						
Přerušení dodávky elektřiny	3	60	48	60	48	48	24
Selhání telekomunikačního zařízení	4	80	64	80	64	48	32
Vzdálená špionáž	2	40	32	40	32	32	32
Krádež médií nebo dokumentů	3	60	48	60	48	24	36
Krádež zařízení	3						
Zprovoznění recyklovaných nebo vyřazených médií	1						
Vyzrazení	4	80	64	80	64	48	48
Data pocházející z nedůvěryhodných zdrojů	3						
Falšování pomocí technického vybavení	4					16	16
Falšování pomocí aplikačního programového vybavení	4					32	32
Odhalení pozice	2						
Selhání zařízení	3						
Chybné fungování zařízení	3						
Chybné fungování aplikačního programového vybavení	3					36	36
Chyba údržby	2						
Neoprávněné použití zařízení	3						
Podvodné kopírování aplikačního programového vybavení	3						
Poškození dat	3	45	36	45	36	48	36
Nezákonné zpracování dat	1	15	16	20	16	12	12
Chyba v používání	3	60	48	60	48	48	36
Zneužití oprávnění	4	60	48	60	48	48	48
Odepření činností	3						

3.2.5 Vyhodnocení analýzy rizik

Tabulka č. 11: Nepřijatelná rizika [Zdroj: Vlastní zpracování]

Hrozba	Úroveň rizika	Aktivum	Zdroj
Selhání telekomunikačního zařízení	80	Data o zákaznících	*IS*
	64	Data o zaměstnancích	*IS*
	80	Interní data	*IS, servery*
	64	Zdrojové kódy	*servery (GitLab)*
	64	Internetové připojení	*cloud*
	80		*pobočka*
	80	Cloud computing	
	64	Vzdálené připojení (VPN)	
Vyzrazení	80	Data o zákaznících	*IS*
	64	Data o zaměstnancích	*IS*
	80	Interní data	*IS, servery*
	64	Zdrojové kódy	*servery (GitLab)*
Chybné fungování aplikačního programového vybavení	75	Informační systém (IS)	*servery*
Zneužití oprávnění	80	Informační systém (IS)	*servery*
	64	JIRA (systém pro vývoj SW)	*servery*
	64	Confluence (intranet)	*servery*
	64	GitLab (verzování kódu)	*servery*

Z provedené analýzy rizik je patrné, že nejvíce ohrožena jsou informační aktiva společnosti. Převážná většina informačních aktiv je zdigitalizována a uložena v informačním systému, který v sobě uchovává právě data o zákaznících, zaměstnancích a také interní data společnosti. Další část infomačních aktiv, mezi ně patří také zdrojové kódy, je uložena v softwarových nástrojích JIRA, Confluence a GitLab, které jsou každodenně využívány při vývoji softwaru.

Největší riziko představuje selhání telekomunikačního zařízení tedy selhání internetového připojení. Je to logické vyústění, neboť produkční servery, na nichž běží informační systém a softwarové nástroje, jsou provozovány v cloudu v rámci služeb cloud computingu. Nedostupnost, tedy nemožnost se připojit k těmto serverům, negativně

ovlivňuje chod celé společnosti. Část softwarových nástrojů je dostupná pouze z interní sítě, z toho důvodu je důležité mít dostupné vzdálené připojení (VPN).

Dalšími největšími riziky je zneužití oprávnění a vyzrazení informací. Tato rizika záměrně uvádím pospolu neboť do určité míry spolu souvisejí. Pokud dojde, a tato situace reálně může nastat, k chybnému přiřazení přístupových práv do informačního systému nebo softwarových nástrojů, tak s daným uživatelem jsou sdílena data, ke kterým by neměl mít přístup. Získaná data můžou být následně daným uživatelem vyzrazena. Tato rizika souvisejí s lidským faktorem, který se nachází všude a nelze se mu zcela vyhnout.

Posledním závažným rizikem je chybné fungování aplikačního programového vybavení. V kontextu společnosti je toto riziko spojeno s interně vyvíjeným informačním systémem, o jehož vývoj se stará interní tým vývojářů, kteří mají za úkol rozšiřovat stávající systém o nové funkce. Pochybení při jejich vývoji může mít vliv na poskytované informace manažerům, kteří na základě nich provádějí svá rozhodnutí. Chyba při vývoji systému může ovlivnit chod celé společnosti.

V matici rizik si lze všimnout velkého množství rizik s úrovní rizika 60. Tato rizika sice spadají do kategorie nežádoucích rizik, ale dělí je pouze jeden bod od kategorie nepřijatelných. Z toho důvodu je potřeba uvést i tato nežádoucí rizika (viz Tabulka č. 12).

Při pohledu na tabulku s nežádoucími riziky je zřejmé, že nejvíce ohrožena jsou stejně jako v předcházejícím případě u nepřijatelných rizik informační aktiva společnosti. Navíc je ohrožena také zbylá část serverů běžící ve virtuálním prostředí na fyzických serverech umístěných v prostoru budovy. Na zmíněná aktiva působí hrozby přerušení dodávky elektřiny, selhání telekomunikačního zařízení, krádež médií nebo dokumentů, chybné fungování zařízení, chyba v používání a zneužití oprávnění.

Tabulka č. 12: Nežádoucí rizika [Zdroj: Vlastní zpracování]

Hrozba	Úroveň rizika	Aktivum	Zdroj
Přerušení dodávky elektřiny	60	Data o zákaznících	*IS*
	60	Interní data	*IS, servery*
	60	Servery	
	60	Internetové připojení	*pobočka*
	60	Elektrická energie	*pobočka*
Selhání telekomunikačního zařízení	60	Servery	
Krádež médií nebo dokumentů	60	Data o zákaznících	*IS*
	60	Interní data	*IS, servery*
Chybné fungování zařízení	60	Servery	
Chyba v používání	60	Data o zákaznících	*IS*
	60	Interní data	*IS, servery*
	60	Informační systém (IS)	*servery*
Zneužití oprávnění	60	Data o zákaznících	*IS*
	60	Interní data	*IS, servery*
	60	Servery	

3.3 Bezpečnostní opatření

Vzhledem k tomu, že společnost v dohledné době neplánuje zavádět v plném rozsahu ISMS ani usilovat o certifikaci, nebudu navrhovat zavedení všech dostupných bezpečnostních opatření. Dle požadavků vedení společnosti a výsledků analýzy rizik jsou vybrána pouze ta bezpečnostní opatření, která vedou ke snížení největších rizik a která ještě nejsou ve společnosti zavedena. Vybraná bezpečnostní opatření jsou v souladu s normou ČSN EN ISO/IEC 27001:2017 s přílohou A. Následující tabulka zobrazuje cílené navržení bezpečnostních opatření k jednotlivým rizikům, která budou zavedena v rámci první etapy.

Tabulka č. 13: Výběr bezpečnostních opatření pro zvládání největších rizik [Zdroj: Vlastní zpracování]

Hrozba	Bezpečnostní opatření
Přerušení dodávky elektřiny	A.11.2.2, A.11.2.4, A.17.2.1
Selhání telekomunikačního zařízení	A.11.2.2, A.11.2.4, A.17.2.1
Krádež médií nebo dokumentů	A.6.2.1, A.8.2.3, A.10.1.1, A.11.2.5, A.11.2.8, A.11.2.9, A.12.2.1, A.12.4.4, A.13.2.1, A.13.2.2, A.13.2.3
Vyzrazení	A.6.2.1, A.8.2.1, A.8.2.2, A.10.1.1, A.11.2.9, A.12.2.1, A.13.2.1
Chybné fungování zařízení	A.11.2.4, A.11.2.5, A.11.2.8, A.17.2.1
Chybné fungování aplikačního programového vybavení	A.12.2.1, A.12.4.4
Chyba v používání	A.6.2.1, A.7.2.2, A.8.1.3, A.8.2.3, A.11.2.5, A.11.2.8, A.11.2.9
Zneužití oprávnění	A.12.4.4

Pro splnění požadavku zvýšení informační bezpečnosti ve společnosti navrhuji v rámci první etapy také zavést bezpečnostní opatření spadající do oblasti organizace bezpečnosti informací (A.6.1.1 - A.6.1.5), která přímo nevyplývají z provedené analýzy rizik, avšak je vhodné je zavést z důvodu jejich obecné působnosti v oblasti informační bezpečnosti.

3.3.1 Plán zavedení bezpečnostních opatření

Jak již bylo zmíněno v předcházející kapitole 3.3, zavádění bezpečnostních opatření bude rozděleno na dvě etapy.

V **první etapě** budou zavedena bezpečnostní opatření, která vedou ke snížení největších rizik a která ještě nejsou ve společnosti zavedena. V první etapě navrhuji také zavést bezpečnostní opatření spadající do oblasti organizace bezpečnosti informací (A.6.1.1 - A.6.1.5), která přímo nevyplývají z provedené analýzy rizik, avšak je vhodné je zavést z důvodu jejich obecné působnosti v oblasti informační bezpečnosti.

V **druhé etapě** budou zavedena všechna zbývající bezpečnostní opatření, která nejsou ve společnosti zavedena (viz kapitola 2.4 – bezpečnostní opatření jejichž stav plnění je „nezavedeno“).

3.4 Návrh zavedení bezpečnostních opatření

V této kapitole bude popsán návrh zavedení bezpečnostních opatření, která jsou uvedena v Tabulce č. 13. U každé kategorie opatření je uveden cíl podle normy ČSN ISO/IEC 27002:2017, jehož má být dosaženo. Všechna zaváděná bezpečnostní opatření vychází z doporučení téže normy. Pro potřeby společnosti jsou některá doporučení částečně upravena.

3.4.1 A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: „*Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace*“ [11, s. 11].

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Opatření: Definovat a přidělit všechny odpovědnosti za bezpečnost informací.

Implementace: Zavést role a odpovědnosti za bezpečnost v souladu s politikami bezpečnosti informací. Provést identifikaci odpovědnosti za ochranu jednotlivých aktiv a za provádění specifických postupů v oblasti bezpečnosti informací. Identifikovat a definovat aktiva a procesy bezpečnosti informací. Určit vlastníky aktiv, kteří za dané aktivum budou zodpovědní. Vlastníci aktiva by měli být v dané oblasti kompetentní a měli by dostat možnost udržovat krok s vývojem, aby byli schopni zastávat dané odpovědnosti.

Časová náročnost: 16 hodin

A.6.1.2 Princip oddělení povinností

Opatření: Oddělit konfliktní povinnosti a oblasti působnosti z důvodu omezení příležitosti pro neúmyslné nebo neoprávněné změny nebo zneužití aktiv organizace.

Implementace: Zabezpečit, aby žádná jednotlivá osoba nemohla k aktivům přistupovat, upravovat je nebo používat je bez oprávnění nebo detekce. V případě, kdy nelze povinnosti dostatečně oddělit, je nutné zajistit alespoň monitorování činností, které jsou s aktivem prováděny.

Ve společnosti existuje dokument s popisem pracovních pozic, který však není aktuální. Navrhuji tento dokument aktualizovat a doplnit role, práva, povinnosti a odpovědnosti osob, které tyto pracovní pozice zastávají. Na základě tohoto dokumentu budou nastavena jednotlivá oprávnění v adresářové službě Active Directory.

Časová náročnost: 6 hodin

A.6.1.3 Kontakt s autoritami

Opatření: Udržovat přiměřené vztahy s příslušnými orgány a autoritami.

Implementace: Zavést postupy, které stanoví, kdo a kdy by měl kontaktovat autority (např. orgány vymáhající právo) a jak by měly být identifikované incidenty bezpečnosti informací včas hlášeny (např. existuje-li podezření, že došlo k porušení zákona). Doporučuje se také udržovat kontakty s dalšími autoritami jako např. s poskytovateli telekomunikačních služeb.

Časová náročnost: 4 hodiny

A.6.1.4 Kontakt se zvláštními zájmovými skupinami

Opatření: Udržovat přiměřené kontakty se zvláštními zájmovými skupinami nebo dalšími fóry specialistů na bezpečnost a profesními sdruženími.

Implementace: Členství ve zvláštních zájmových skupinách či fórech by měla vést k:

a) zlepšování znalostí o doporučených postupech a sledování aktuálního vývoje v kompetentní oblasti bezpečnosti informací,
b) ujištění, že chápání bezpečnosti informací v prostředí organizace je aktuální a kompletní,
c) obdržení včasných varování, doporučení a oprav týkajících se útoků a zranitelností,
d) získání přístupu k doporučením specialistů bezpečnosti informací,
e) sdílení a výměně informací o nových technologiích, produktech, hrozbách nebo zranitelnostech,
f) zajištění vhodných styčných míst při řešení bezpečnostních incidentech.

Časová náročnost: 2 hodiny

A.6.1.5 Bezpečnost informací v řízení projektů

Opatření: Řešit bezpečnosti informací v rámci řízení projektů, bez ohledu na typ projektu.

Implementace: Začlenit bezpečnost informací do metod řízení projektů za účelem identifikovat rizika bezpečnosti informací a řešit je jako součást projektu. Dopady bezpečnosti informací by měly být řešeny a pravidelně přezkoumávány ve všech projektech. Metody řízení projektů by měly vyžadovat, aby:

a) cíle bezpečnosti informací byly zahrnuty do projektových cílů,
b) posuzování rizik bezpečnosti informací se provádělo již v rané fázi projektu z důvodu identifikování nezbytných opatření,
c) bezpečnost informací byla součástí všech fází použité projektové metodiky.

Časová náročnost: 6 hodin

A.6.2 Mobilní zařízení a práce na dálku

Cíl: „*Zajistit bezpečnost práce na dálku a bezpečnost použití mobilních zařízení*“ [11, s. 13].

A.6.2.1 Politika mobilních zařízení

Opatření: Přijmout politiku a podpůrná bezpečnostní opatření k řízení rizik zavedených používáním mobilních zařízení.

Implementace: Zavést politiku pro používání mobilních zařízení, aby nemohly být kompromitovány informace týkající se činnosti organizace. Politika by měla brát v úvahu rizika práce s mobilními zařízeními v nechráněných oblastech. Politika mobilních zařízení by se měla věnovat:

a) registraci mobilních zařízení,
b) požadavkům na fyzickou ochranu,
c) omezení instalace softwaru,
d) požadavkům na nejnovější verze operačního systému a aplikací,
e) řízení přístupu,
f) kryptografickým technikám,
g) ochraně před malwarem,
h) vzdálené deaktivaci, výmazu nebo zablokování,
i) zálohování.

Časová náročnost: 4 hodiny

3.4.2 A.7 Bezpečnost lidských zdrojů

A.7.2 Během pracovního poměru

Cíl: „*Zajistit, aby si zaměstnanci a smluvní strany byli vědomi svých povinností, a zajistit, aby je plnili*“ [11, s. 17].

A.7.2.2 Povědomí, vzdělávání a školení o bezpečnosti informací

Opatření: Všichni zaměstnanci organizace, smluvní strany a tam, kde je to vhodné, by měli získat odpovídající povědomí o bezpečnosti informací formou vzdělávání a školení a pravidelných aktualizací politik a postupů organizace, dle významu pro zastávanou pracovní funkci.

Implementace: Program budování bezpečnostního povědomí by se měl zaměřit na to, aby byli všichni zaměstnanci, a tam, kde je to vhodné, i smluvní strany, vědomi své odpovědnosti za bezpečnost informací a způsobů, jímž jsou tyto odpovědnosti plněny. Program budování bezpečnostního povědomí by měl být v souladu s politikami organizace v oblasti bezpečnosti informací a příslušnými postupy. Měl by brát v úvahu

informace organizace, které mají být chráněny, a opatření, která byla na ochranu informací zavedena. Měl by být naplánován s přihlédnutím k rolím zaměstnanců v organizaci. Činnosti v rámci programu budování bezpečnostního povědomí by měly být naplánovány v průběhu času, nejlépe pravidelně, tak aby se činnosti opakovaly a zahrnovaly nové zaměstnance a smluvní strany. Měl by být také pravidelně aktualizován.

Časová náročnost: 24 hodin

3.4.3 A.8 Řízení aktiv

A.8.1 Odpovědnost za aktiva

Cíl: „*Identifikovat aktiva organizace a definovat odpovědnosti za přiměřenou ochranu*“ [11, s. 19].

A.8.1.3 Přípustné použití aktiv

Opatření: Identifikovat, dokumentovat a implementovat pravidla pro přípustné používání informací a aktiv spojených s informacemi a vybavením pro zpracování informací.

Implementace: Uvědomit všechny zaměstnance a uživatele z externích stran používající nebo mající přístup k aktivům organizace o požadavcích bezpečnosti informací na aktiva organizace spojené s informacemi a vybavením pro zpracování informací a zdroji. Na zaměstnance a uživatele z externích stran používající nebo mající přístup k aktivům organizace by se měla přenášet odpovědnost za použití jakýchkoliv zdrojů pro zpracování informací a jakéhokoliv podobného použití provedeného v rámci své odpovědnosti.

Časová náročnost: 4 hodiny

A.8.2 Klasifikace informací

Cíl: „*Zajistit, aby informace získala odpovídající úroveň ochrany v souladu s jejím významem pro organizaci*“ [11, s. 21].

A.8.2.1 Klasifikace informací

Opatření: Klasifikovat informace z hlediska právních požadavků, hodnoty, kritičnosti a citlivosti ve vztahu k neoprávněnému prozrazení nebo modifikaci.

Implementace: Klasifikace informací musí být vykonávána tak, aby byla určena důležitost a stupeň ochrany pro dané informace. Klasifikována můžou být i jiná aktiva než pouze informace, v souladu s klasifikací informací, která jsou v aktivech uložena, zpracovávána nebo jsou aktivem chráněna. Za jejich klasifikaci by měli být odpovědni jednotliví vlastníci aktiv. Klasifikaci je důležité provádět s ohledem na právní požadavky, kritičnost a citlivost daných informací. Po určité době, např. po zveřejnění, mohou přestat být informace citlivé a kritické. Je potřeba s těmito aspekty počítat, neboť přehnaná klasifikace může vést k neúměrným administrativním nákladům. Při klasifikaci by se měl brát zřetel na škodu, která může nastat při prozrazení nebo zveřejnění některých informací. Příklad klasifikačního schématu důvěrnosti:

a) únik informací nezpůsobí žádnou škodu,
b) únik informací způsobí menší nepříjemnosti nebo menší provozní obtíže,
c) únik informací má významný krátkodobý dopad na provozní činnosti nebo taktické cíle,
d) únik informací má vážný dopad na dlouhodobé strategické cíle nebo ohrožuje samotný chod organizace.

Časová náročnost: 10 hodin

A.8.2.2 Označování informací

Opatření: Vypracovat a implementovat vhodné soubory postupů, v souladu se schématem klasifikace informací přijatým organizací.

Implementace: Na základě vytvořeného klasifikačního schématu (viz A.8.2.1) je potřeba vypracovat postupy pro označování těchto informací. Veškeré informace a související aktiva, ať už ve fyzické nebo elektronické podobě, musí být značeny. Výjimku tvoří informace, které jsou klasifikovány jako veřejné, ty označovány být nemusí. Označení musí být lehce rozeznatelné. O postupech označování by měli být obeznámeni zaměstnanci a smluvní strany.

Časová náročnost: 4 hodiny

A.8.2.3 Manipulace s aktivy

Opatření: Vyvinout a zavést postupy v souladu se schématem klasifikace informací přijatým organizací.

Implementace: Vypracovat postupy pro zacházení, zpracování, ukládání a předávání informací, které budou v souladu s jejich klasifikací (viz A.8.2.1). Je třeba brát v potaz následující položky:

a) omezení přístupu podporující požadavky na ochranu na každé úrovni klasifikace,
b) udržování formálního záznamu o oprávněných příjemcích aktiv,
c) ochrana dočasných nebo trvalých kopií informace na úrovni odpovídající ochraně původní informace,
d) skladování IT aktiv v souladu se specifikacemi výrobce,
e) zřetelné označení kopií médií pro upoutání pozornosti oprávněného příjemce.

Časová náročnost: 4 hodiny

3.4.4 A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: „*Zajistit správné a efektivní využití kryptografie na ochranu důvěrnosti, autenticity a/nebo integrity informací*“ [11, s. 31].

A.10.1.1 Politika použití kryptografických opatření

Opatření: Vypracovat a realizovat politiku použití kryptografických opatření na ochranu informací.

Implementace: Vypracovat politiku v oblasti kryptografie. Při jejím vypracovávání by mělo být zváženo následující:

a) manažerský přístup ve vztahu k používání kryptografických opatření v rámci celé organizace, včetně obecných zásad, podle nichž by měly být informace chráněny,
b) na základě posuzování rizik by měla být určena vyžadovaná úroveň ochrany s ohledem na typ, sílu a kvalitu požadovaného šifrovaného algoritmu,
c) použití šifrování pro ochranu informací přenášených prostřednictvím mobilních zařízení nebo zařízení s výměnnými médii,
d) přístup ke správě klíčů, včetně metod zabývajících se ochranou kryptografických klíčů a obnovením zašifrované informace v případě ztráty, kompromitace nebo poškození klíčů,
e) role a zodpovědnosti (implementace politiky, správa klíčů včetně generování klíčů),
f) dopad použití šifrované informace na opatření, která se spoléhají na kontrolu obsahu.

Kryptografická opatření mají své uplatnění také při dosahování různých cílů v oblasti bezpečnosti informací, například:

a) důvěrnosti – pomocí šifrování informací k ochraně citlivých nebo kritických informací,
b) integrity/autenticity – např. pomocí digitálních podpisů,
c) nepopiratelnosti – použití kryptografických technik za účelem poskytnutí důkazu o výskytu nebo absenci výskytu události nebo činnosti,
d) autentizace – použití kryptografických technik k autentizaci uživatelů.

Časová náročnost: 4 hodiny

3.4.5 A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.2 Zařízení

Cíl: „*Zabránit ztrátě, poškození, odcizení nebo kompromitaci aktiv a přerušení provozu organizace*“ [11, s. 36].

A.11.2.2 Podpůrné služby

Opatření: Chránit zařízení před výpadkem napájení a dalšími poruchami způsobenými selháním podpůrných služeb.

Implementace: Pro zajištění bezproblémové funkčnosti podpůrných služeb (např. elektřina, telekomunikace) je dobré:

a) pravidelně posuzovat a testovat vybavení zajišťující podpůrné služby,
b) včasně upozornit na detekci závady,
c) implementovat redundance (vícenásobné přívody s odlišnými fyzickými trasami a od více než jednoho poskytovatele služeb).

Časová náročnost: 6 hodin

A.11.2.4 Údržba zařízení

Opatření: Správně udržovat zařízení pro zajištění jeho stálé dostupnosti a integrity.

Implementace: Všechna zařízení by měla být udržována dle doporučených servisních intervalů a specifikací výrobce. Opravy a servis zařízení by měli provádět pouze autorizovaní pracovníci údržby. V případě provádění opravy nebo servisu zařízení mimo organizaci, je nutné zkontrolovat, zda zařízení obsahuje důvěrné informace, které by měly být před servisem ze zařízení odstraněny. Pevný disk by měl být vyjmut ze zařízení, a to i přesto, že data nacházející se disku jsou šifrována. Před opětovným uvedením zařízení do provozu po servisu by mělo být zařízení zkontrolováno s cílem ujistit se, že se zařízením nebylo manipulováno a že jeho funkčnost je správná.

Časová náročnost: 2 hodiny

A.11.2.5 Přemístění aktiv

Opatření: Bez předchozího povolení by neměly být mimo organizaci přemístěny zařízení, informace nebo software.

Implementace: Vedení organizace musí schválit přemísťování aktiv. Každé jednotlivé přemístění aktiva musí být zdokumentováno a odůvodněno. Vedení organizace může zavést namátkové kontroly zaměřující se na vnášení nebo vynášení aktiv.

Časová náročnost: 2 hodiny.

A.11.2.8 Neobsluhovaná uživatelská zařízení

Opatření: Zajistit přiměřenou ochranu neobsluhovaného zařízení.

Implementace: Informovat všechny uživatele o bezpečnostních požadavcích a postupech pro ochranu neobsluhovaného zařízení včetně jejich odpovědnosti za realizaci této ochrany. Poučit uživatele o tom, aby:

a) ukončili aktivní relace po dokončení činnosti,
b) se odhlásili z aplikací nebo síťových služeb, pokud již nejsou dále potřeba,
c) zabezpečili počítače nebo mobilní zařízení před neoprávněným použitím.

Časová náročnost: 2 hodiny

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Opatření: Přijat zásadu prázdného stolu, týkající se papírových dokumentů a vyměnitelných paměťových médií, a zásadu prázdné obrazovky.

Implementace: Zásada prázdného stolu a prázdné obrazovky monitoru by měla brát v úvahu následující:

a) citlivé nebo kritické informace organizace, ať už v papírové nebo elektronické formě, by měly být uzamčeny, pokud nejsou využívány (např. ve skříni nebo v jiném zabezpečeném vybavení),
b) počítače by měly být ponechávány s odhlášenými uživateli nebo chráněny mechanismem zamykajícím obrazovku nebo klávesnici, který je kontrolován heslem,
c) zabránit neoprávněnému používání reprodukčních technologií (např. kopírek, skenerů),
d) média obsahující citlivé či klasifikované informace by měla být ihned odebrána z tiskáren.

Časová náročnost: 2 hodiny

3.4.6 A.12 Bezpečnost provozu

A.12.2 Ochrana před malwarem

Cíl: „*Zajistit, že informace a vybavení pro zpracování informací jsou před malwarem chráněny*“ [11, s. 42].

A.12.2.1 Opatření na ochranu proti malwaru

Opatření: Implementovat opatření pro detekci, prevenci a zotavení na ochranu před malwarem, v kombinaci s vhodným zvyšováním povědomí uživatelů.

Implementace: Ochrana před malwarem by měla být postavena na detekci malwaru a opravných programech, na povědomí o bezpečnosti informací a odpovídajících opatření v oblasti přístupu k systému a řízení změn. Je potřeba posoudit následující pokyny:

a) stanovení formální politiky zakazující používání neautorizovaného softwaru,
b) realizace opatření, která zabraňují nebo detekují použití neautorizovaného softwaru a známých nebo podezřelých škodlivých webových stránek,
c) instalace a pravidelná aktualizace softwaru pro detekci malwaru a opravných programů pro skenování počítače a médií,
d) stanovení postupů a odpovědnosti zabývajících se ochranou před malwarem,
e) definování plánu kontinuity podnikaní pro zotavení se z útoku vyvolaného malwarem,
f) zavedení izolovaného prostředí, ve kterém mohou nastat katastrofické účinky.

Poznámka: Efektivita ochrany před malwarem může být zvýšena použitím dvou nebo více softwarových produktů chránící před malwarem od různých dodavatelů a s různou technologií.

Časová náročnost: 8 hodin

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: „*Zaznamenávat události a generovat důkazy*“ [11, s. 44].

A.12.4.4 Synchronizace hodin

Opatření: Všechny významné systémy pro zpracování informací v rámci organizace by měly mít zdroje času synchronizovány s jedním referenčním zdrojem času.

Implementace: Definovat standardní referenční čas pro použití v rámci organizace. Jeho důležitost spočívá v zajištění přesnosti auditních záznamů, které mohou být vyžadovány například pro vyšetřování nebo jako důkazy v soudním či disciplinárním řízení.

Časová náročnost: 1 hodina

3.4.7 A.13 Bezpečnost komunikací

A.13.2 Přenos informací

Cíl: „*Zachovat bezpečnost informací přenášených v rámci organizace a s jakýmkoli externím subjektem*“ [11, s. 50].

A.13.2.1 Politiky a postupy při přenosu informací

Opatření: Zavést formální politiky, postupy a opatření vedoucí k ochraně přenosu informací prostřednictvím všech druhů komunikačních zařízení.

Implementace: Při používání komunikačních zařízení pro přenos informací je potřeba se držet postupů a kontrol, které by měly zvážit následující opatření:

a) postupy navrhnuté k ochraně přenášených informací před odposlouchávánim, kopírováním, pozměněním, chybným směrováním a zničením,

b) postupy pro detekci a ochranu před malwarem,
c) postupy pro ochranu citlivých elektronických informací, které jsou ve formě přílohy,
d) politika či směrnice vymezující přípustné použití komunikačních zařízení,
e) použití kryptografických technik,
f) směrnice obsahující informace o uchovávání a likvidaci veškeré podnikové korespondence,
g) doporučení zaměstnancům o přijetí vhodných preventivních opatření proti prozrazení důvěrných informací.

Upozornit zaměstnance, že by neměli vést důvěrné rozhovory na veřejných místech nebo prostřednictvím nezabezpečených komunikačních kanálů, v otevřených kancelářích a zasedacích místnostech.

Časová náročnost: 4 hodiny

A.13.2.2 Dohody o přenosu informací

Opatření: Ustanovit dohody, které povedou k bezpečnému přenosu obchodních informací mezi organizací a externími stranami.

Implementace: Dohody o přenosu informací by měly obsahovat následující:

a) odpovědnosti managementu za řízení a oznamování přenosu, odesílání a přijímání,
b) kroky k zajištění dohledatelnosti a nepopiratelnosti,
c) dohody o uložení zdrojových kódů programů u nezávislé třetí strany,
d) odpovědnosti a povinnosti v případě incidentů bezpečnosti informací (např. ztráta dat),
e) jakákoliv speciální opatření, která jsou nutná k ochraně citlivých položek,
f) akceptovatelné úrovně řízení přístupu.

Časová náročnost: 2 hodiny

A.13.2.3 Elektronické předávání zpráv

Opatření: Přiměřeně chránit informace zahrnuté v elektronicky předávaných zprávách.

Implementace: V elektronicky předávaných zprávách by měly být zváženy následující aspekty:

a) ochrana zpráv před neoprávněným přístupem,
b) zajištění správného adresování a přepravy zprávy,
c) spolehlivost a dostupnost služby,
d) zákonná kritéria (např. požadavky na elektronické podpisy),
e) získání povolení k užívání externích veřejných služeb,
f) silnější úroveň autentizace řídící přístup z veřejně přístupných sítí.

Časová náročnost: 1 hodina

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

A.17.2 Redundance

Cíl: „*Zajistit dostupnost vybavení pro zpracování informací*“ [11, s. 68].

A.17.2.1 Dostupnost vybavení pro zpracování informací

Opatření: Vybavení pro zpracování informací by mělo být zaváděno s dostatečnou redundancí, aby byly splněny požadavky na dostupnost.

Implementace: Identifikovat požadavky na dostupnost informačních systémů. V případě, že dostupnost nelze zajistit pomocí stávající architektury systémů, měly by být zvažovány redundantní komponenty nebo architektury.

Časová náročnost: 2 hodiny

3.5 Budování bezpečnostního povědomí

Budování bezpečnostního povědomí neboli SAE (Security Awareness Education) je nikdy nekončící proces, stejně tak jako je tomu u informační bezpečnosti. Cíl tohoto procesu je neustále vzdělávat všechny zaměstnance a budovat u nich bezpečnostní povědomí. Budování bezpečnostního povědomí je nezávislé na zavedení bezpečnostních opatření a ISMS. Při budování bezpečnostního povědomí rozdělujeme uživatele do skupin a vzděláváme je na několika úrovních dle potřeby organizace. Neodmyslitelným prvkem pro úspěšné budování bezpečnostního povědomí je stanovení SAE plánu, který se skládá z několika na sebe navazujících činností.

Role a odpovědnosti

Pro budování bezpečnostního povědomí bude stanovena jedna role a to tzv. CISO. Osoba zastávající tuto roli bude odpovědná za budování bezpečnostního povědomí v organizaci. Z důvodu zastupitelnosti rolí bude stanovena druhá osoba, a to vedoucí IT oddělení, který bude moci se podílet v případě nutnosti na budování bezpečnostního povědomí. Náplní práce této role bude dohlížet na dodržení SAE plánu a na základě zpětné vazby jej vylepšovat a upravovat k zajištění co nejvyšší efektivity budování bezpečnostního povědomí.

Rozdělení uživatelů

Zaměstnanci budou rozděleni do skupin podle zkušeností a druhu využití ICT:

a) běžný uživatel – pouze základní znalosti o ICT, ICT používá pouze pro nutné činnosti,
b) pokročilý uživatel – pokročilé znalosti ICT, jeho pracovní náplní je práce s ICT,
c) specialista – podílí se na zvyšování informační bezpečnosti v organizaci.

Tabulka č. 14: Srovnávací rámec bezpečnostního vzdělávání [Zdroj: Vlastní zpracování dle: 22]

Srovnávací rámec bezpečnostního vzdělávání			
	Povědomí	**Školení**	**Vzdělávání**
Atribut	"Co"	"Jak"	"Proč"
Úroveň	Informativní	Znalost	Pochopení
Cíl vzdělávání	Rozpoznání a zapamatování	Dovednost	Porozumění
Cílová skupina	Běžný uživatel, pokročilý uživatel, specialista	Pokročilý uživatel, specialista	Specialista
Příklad vzdělávací metody	Výukové videa, prospekty, bezpečnostní brožura	Případové studie, praktické ukázky	Semináře a diskuze, čtení a studium, výzkum
Způsob testování vzdělání	Test Ano/Ne, výběr z více možností	Řešení problémů (praktická cvičení)	Esej
Časová náročnost	Krátkodobá	Střednědobá	Dlouhodobá

Po ověření vstupních znalostí jednotlivých zaměstnanců a rozdělení do skupin je možné blíže specifikovat cíle a rozsah bezpečnostního vzdělávání. Podle zjištěných skutečností je dále nutné navázat s následujícími činnostmi:

a) stanovení cílů pro každou úroveň vzdělávání,
b) vytvoření školících materiálů dle skupin uživatelů,
c) určení cíle pro každou skupinu uživatelů,
d) témata, která je třeba řešit v každé relaci nebo kurzu,
e) metody nasazení pro každý aspekt programu,
f) dokumentace, zpětná vazba a doložení výuky,
g) vyhodnocení a aktualizace výukových materiálů,
h) četnost opakování včetně updatů materiálů,
i) kalkulace.

3.6 Postup zavedení bezpečnostních opatření první etapy

V kapitole 3.4 byla popsána bezpečnostní opatření, která budou zavedena v rámci první etapy. Tato opatření jsou seřazena dle pořadí v normě ČSN EN ISO/IEC 27001:2017 příloze A. Při jejich zavádění je však důležité postupovat dle odlišného pořadí. Je nutné zavádět opatření dle jejich důležitosti a dle závažnosti rizik, která tato opatření minimalizují.

Z provedené analýzy rizik je patrné, že největší riziko představuje selhání telekomunikačního zařízení, vyzrazení, chybné fungování aplikačního programového vybavení, zneužití oprávnění, přerušení dodávky elektřiny, krádež médií nebo dokumentů, chybné fungování zařízení a chyba v používání. Všechny tyto hrozby ohrožují informační aktiva společnosti.

Navrhuji proto začít se zaváděním opatření ze skupiny A.11 Fyzická bezpečnost a bezpečnost prostředí. Tato opatření zabrání neoprávněnému přístupu, poškození a narušování informací. Následně zavést opatření ze skupiny A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací. Dále zavést opatření ze skupiny A.8 Řízení aktiv. Cílem těchto opatření je identifikovat aktiva a definovat odpovědnosti za přiměřenou ochranu. Následovat bude opatření ze skupiny A.10 Kryptografie, které zajistí vypracování politik pro použití kryptografických opatření na

ochranu informací. Dalšími opatřeními budou opatření ze skupiny A.12 Bezpečnost provozu. Opatření v těchto skupině zajistí správné a bezpečné provozování vybavení pro zpracovávání informací. Další skupinou opatření, která bude zavedena, je A.13 Bezpečnost komunikací. Tato opatření zajistí ochranu informací v sítích. Po zavedení výše uvedených opatření je možné pokračovat se zavedením opatření ze skupiny A.6 Organizace bezpečnosti informací. Při aplikaci opatření z této skupiny jsou definovány role a odpovědnosti pro nakládání s informacemi. Poslední skupinou opatření, která bude v první etapě zavedena, je A.7 Bezpečnost lidských zdrojů. Toto opatření slouží pro vypracování programu pro seznámení zaměstnanců s bezpečnostními pravidly a pro budování bezpečnostního povědomí, které je považováno za klíčový prvek v systému řízení informační bezpečnosti.

V Tabulce č. 15 je nastíněn postup zavedení bezpečnostních opatření první etapy včetně časové náročnosti, která je potřeba pro jejich zavedení a pro každoroční kontrolu.

Tabulka č. 15: Postup zavedení opatření včetně časové náročnosti [Zdroj: Vlastní zpracování]

Opatření	Název opatření	Časová náročnost zavedení opatření [h]	
		Jednorázově	Každoročně
A.11	Fyzická bezpečnost a bezpečnost prostředí	14	5
A.17	Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	2	1
A.8	Řízení aktiv	22	8
A.10	Kryptografie	4	1
A.12	Bezpečnost provozu	9	2
A.13	Bezpečnost komunikací	7	3
A.6	Organizace bezpečnosti informací	38	6
A.7	Bezpečnost lidských zdrojů	24	10
Celková časová náročnost		**120**	**36**

3.6.1 Časový plán

Vedení společnosti se rozhodlo na zavádění bezpečnostních opatření první etapy vyhradit jeden celý měsíc. Práce na zavádění začne 1. července 2019 a skončí v pondělí 22. července 2019. Práce bude probíhat od pondělí do pátku s osmihodinovou pracovní dobou. Ve 27. týdnu je jeden státní svátek, kdy je zavádění na jeden den pozastaveno. Zbytek 30. týdne a polovina 31. týdne je vyhrazen pro případnou časovou rezervu. Níže uvedená tabulka zobrazuje detailní časový plán zavádění bezpečnostních opatření první etapy.

Na základě zkušeností a časových možností společnosti bude rozhodnuto o termínu a způsobu zavádění bezpečnostních opatření druhé etapy.

Tabulka č. 16: Časový plán [Zdroj: Vlastní zpracování]

Opatření	Časová náročnost [h]	27. týden					28. týden					29. týden					30. týden				
		Po	Út	St	Čt	Pá	Po	Út	St	Čt	Pá	Po	Út	St	Čt	Pá	Po	Út	St	Čt	Pá
A.11.2.2	6	6																			
A.11.2.4	2	2																			
A.11.2.5	2		2																		
A.11.2.8	2		2																		
A.11.2.9	2		2																		
A.17.2.1	2		2																		
A.8.1.3	4			4																	
A.8.2.1	10			4	6																
A.8.2.2	4				2		2														
A.8.2.3	4						4														
A.10.1.1	4						2	2													
A.12.2.1	8							6	2												
A.12.4.4	1								1												
A.13.2.1	4								4												
A.13.2.2	2								1	1											
A.13.2.3	1									1											
A.6.1.1	16									6	8	2									
A.6.1.2	6											6									
A.6.1.3	4												4								
A.6.1.4	2												2								
A.6.1.5	6												2	4							
A.6.2.1	4													4							
A.7.2.2	24														8	8	8				

3.7 Ekonomické zhodnocení

Vedení společnosti se rozhodlo zavádět bezpečnostní opatření ve dvou etapách, a to z toho důvodu, že si nemůže dovolit plně alokovat zaměstnance na delší dobu. V první etapě tvoří náklady na zavádění pouze mzda zaměstnance. Na základě konzultací s vedením společnosti byla stanovena mzda zaměstnance pracujícího na jejich zavádění na 500 Kč/hod. Zaměstnanci bude po dobu zavádění vyhrazena 100% alokace (tj. 40 hodin týdně). V případě, že by se vedení společnosti rozhodlo využít služeb externího specialisty, byla by výše mzdy stanovena minimálně na 1 000 Kč/hod.

3.7.1 Náklady na návrh bezpečnostních opatření

Náklady na návrh bezpečnostních opatření se skládají z pěti činností, které na sebe chronologicky navazují. Jedná se o asistované zhodnocení, stanovení rozsahu a hranic, analýzu rizik, výběr bezpečnostních opatření a návrh zavedení bezpečnostních opatření. Časová náročnost návrhu bezpečnostních opatření byla 184 hodin, z čehož vyplývají celkové náklady ve výši 92 000 Kč.

Tabulka č. 17: Náklady na návrh bezpečnostních opatření [Zdroj: Vlastní zpracování]

	Časová náročnost [h]	**Celkové náklady**
Asistované zhodnocení	56	28 000 Kč
Rozsah a hranice	8	4 000 Kč
Analýza rizik	56	28 000 Kč
Výběr bezpečnostních opatření	16	8 000 Kč
Návrh zavedení bezpečnostních opatření	48	24 000 Kč
Celkem	**184**	**92 000 Kč**

3.7.2 Náklady na zavedení bezpečnostních opatření

Celková předpokládaná časová náročnost na zavedení bezpečnostních opatření vychází na 120 hodin. Při mzdě zaměstnance 500 Kč/hod. jsou celkové náklady na zavedení bezpečnostních opatření ve výši 60 000 Kč. ISMS je však nikdy nekončící proces, který vyžaduje neustále udržování a zlepšování. Odhadl jsem proto také časovou náročnost a náklady na údržbu bezpečnostních opatření, které budou zavedeny v první etapě. Časová náročnost roční údržby je přibližně 36 hodin, z čehož vyplývají roční náklady 18 000 Kč.

Tabulka č. 18: Náklady na zavedení bezpečnostních opatření [Zdroj: Vlastní zpracování]

Opatření	Časová náročnost [h]		Náklady	
	Zavedení	Ročně	Zavedení	Ročně
A.6.1.1	16	1	8 000 Kč	500 Kč
A.6.1.2	6	1	3 000 Kč	500 Kč
A.6.1.3	4	1	2 000 Kč	500 Kč
A.6.1.4	2	1	1 000 Kč	500 Kč
A.6.1.5	6	1	3 000 Kč	500 Kč
A.6.2.1	4	1	2 000 Kč	500 Kč
A.7.2.2	24	10	12 000 Kč	5 000 Kč
A.8.1.3	4	1	2 000 Kč	500 Kč
A.8.2.1	10	4	5 000 Kč	2 000 Kč
A.8.2.2	4	2	2 000 Kč	1 000 Kč
A.8.2.3	4	1	2 000 Kč	500 Kč
A.10.1.1	4	1	2 000 Kč	500 Kč
A.11.2.2	6	1	3 000 Kč	500 Kč
A.11.2.4	2	1	1 000 Kč	500 Kč
A.11.2.5	2	1	1 000 Kč	500 Kč
A.11.2.8	2	1	1 000 Kč	500 Kč
A.11.2.9	2	1	1 000 Kč	500 Kč
A.12.2.1	8	1	4 000 Kč	500 Kč
A.12.4.4	1	1	500 Kč	500 Kč
A.13.2.1	4	1	2 000 Kč	500 Kč
A.13.2.2	2	1	1 000 Kč	500 Kč
A.13.2.3	1	1	500 Kč	500 Kč
A.17.2.1	2	1	1 000 Kč	500 Kč
Celkem	**120**	**36**	**60 000 Kč**	**18 000 Kč**

3.7.3 Celkové náklady na návrh a zavedení bezpečnostních opatření

Celkové náklady na návrh a zavedení bezpečnostních opatření první etapy jsou ve výši 152 000 Kč. Celkové náklady se však můžou měnit v závislosti na časové náročnosti průběhu zavádění.

Tabulka č. 19: Celkové náklady na návrh a zavedení opatření [Zdroj: Vlastní zpracování]

	Časová náročnost [h]	Celkové náklady
Návrh bezpečnostních opatření	184	92 000 Kč
Zavedení bezpečnostních opatření	120	60 000 Kč
Celkem	**304**	**152 000 Kč**

3.8 Přínos práce

Hlavní přínosem práce je zvýšení informační bezpečnosti ve společnosti. Vedení společnosti si na základě provedené analýzy uvědomilo možná rizika a jejich dopad při nepřiměřeném zabezpečení. I přesto, že společnost v dohledné době neplánuje usilovat o certifikaci ISMS, má zavedení bezpečnostních opatření v souladu s ISMS velký přínos ve zvýšení informační bezpečnosti ve společnosti. Pokud by se vedení rozhodlo v budoucnu zavést ISMS v plném rozsahu, bylo by možné usilovat o certifikaci. Výhodou certifikace je zvýšení důvěryhodnosti v očích zákazníků a případně rozšíření zákazníků o státní instituce nebo soukromé subjekty, které spadají do kritické informační infrastruktury. Společnosti, které budou chtít dodávat produkty nebo služby do kritické infrastruktury, jsou povinny mít certifikát systému řízení informační bezpečnosti.

Dalším přínosem práce je splnění požadavků, které vedení společnosti stanovilo. Práce představuje základ pro řízení rizik, který by měla společnost správně uchopit a dále provozovat. Po zavedení mnou navrhnutých bezpečnostních opatření dojde k výraznému snížení největších (nepřijatelných) rizik a společnost tak dosáhne přiměřené bezpečnosti za akceptovatelné náklady, které ve srovnání s ročním obratem nejsou nijak výrazné.

I samotná analýza současného stavu, která byla provedena za pomoci podpůrného materiálu (Pomůcky k auditu bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.), je pro organizaci přínosem, protože bylo poukázáno na značné nedostatky z pohledu informační bezpečnosti. K samotné bezpečnosti však nejvíce přispívá budování bezpečnostního povědomí u zaměstnanců a jejich motivace k dodržování daných bezpečnostních pravidel. Budování bezpečnostního povědomí musí probíhat pravidelně, stejně jako kontrola, udržování a zlepšování samotného systému řízení informační bezpečnosti. Pokud bude takto činěno, je velice pravděpodobné, že úroveň bezpečnosti bude neustále zvyšována.

Dle mého názoru je pro společnost největším přínosem pochopení komplexnosti řešení informační bezpečnosti. Vedení si uvědomilo, že v dnešní době je nutné zabudovávat prvky bezpečnosti téměř do všech činností, které jsou ve společnosti prováděny.

ZÁVĚR

Cílem mé diplomové práce bylo zpracovat návrh zavedení bezpečnostních opatření v souladu s ISMS pro softwarovou společnost. Vedení společnosti se pro zpracování návrhu rozhodlo z důvodu zvýšení informační bezpečnosti ve společnosti. Společnost v dohledné době neplánuje usilovat o certifikaci ISMS, jde ji pouze o zlepšení současného stavu. Z toho důvodu jsem zavádění bezpečnostních opatření rozdělil na dvě etapy, tak aby byla přednostně zavedena opatření, která snižují největší rizika.

Základem práce bylo důkladně provést analýzu současného stavu ve společnosti. Ve spolupráci s vedením společnosti bylo vyplněno asistované zhodnocení, které bylo následně převedeno na jednotlivá opatření ISMS převzatá z normy ČSN EN ISO/IEC 27001:2017. Tímto postupem byl získán přesný popis současného stavu bezpečnostních opatření v souladu s ISMS ve společnosti. Výstup asistovaného zhodnocení včetně souhrnu asistovaného zhodnocení k opatřením ISMS bylo představeno vedení společnosti, které se na základě předložených materiálů rozhodlo řešit aktuální situaci informační bezpečnosti ve společnosti.

Na základě analýzy a teoretických východisek práce jsem následně zpracoval návrh. Nejprve jsem určil rozsah a hranice, a vypracoval analýzu rizik, ze které vychází návrh bezpečnostních opatření, která jednotlivá rizika snižuje na akceptovatelnou úroveň. Bezpečnostní opatření jsou navrhnuta dle normy ČSN EN ISO/IEC 27001:2017 a pokynů z normy ČSN ISO/IEC 27002:2017. Všechny záležitosti týkající se návrhu a zavedení bezpečnostních opatření jsem konzultoval s vedením společnosti tak, aby výsledné řešení bylo reálně použitelné.

Vedení společnosti od této práce očekávalo analýzu rizik, návrh bezpečnostních opatření pro zvládání největších rizik, zvýšení bezpečnostního povědomí u zaměstnanců a celkové zvýšení informační bezpečnosti ve společnosti.

Naplnil jsem cíl práce, který byl na začátku stanoven. Byl zpracován návrh zavedení bezpečnostních opatření v souladu s ISMS, ve kterém byly dodrženy všechny požadavky vedení společnosti.

SEZNAM POUŽITÝCH ZDROJŮ

[1] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 9788073802769.

[2] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[3] BÉBR, Richard. *Informační systémy pro podporu manažerské práce*. Praha: Professional Publishing, 2005. ISBN 978-80-8641-979-4.

[4] ČSN ISO/IEC 27000. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018.

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

[6] SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi*. 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN 9788025128787.

[7] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[8] SEDLÁK, P. *Management informační bezpečnosti* (přednáška). Brno: VUT, 2018.

[9] ONDRÁK, V. *Management informační bezpečnosti* (skripta). Brno: VUT, 2013.

[10] ČSN EN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

[11] ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

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

[13] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978–80–7251–397–0.

[14] NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. ©2019 [cit. 2019-02-09]. Dostupné z: https://nukib.cz/

[15] NCKB. *Národní centrum kybernetické bezpečnosti* [online]. ©2019 [cit. 2019-02-09]. Dostupné z: https://www.govcert.cz/

[16] Řízení rizik: Jemný úvod do řízení rizik. *CleverAndSmart* [online]. ©2019 [cit. 2019-02-10]. Dostupné z: https://www.cleverandsmart.cz/rizeni-rizik-jemny-uvod-do-rizeni-rizik/

[17] ISO. *International Organization for Standardization* [online]. ©2019 [cit. 2019-02-01]. Dostupné z: https://www.iso.org

[18] IEC. *International Electrotechnical Commission* [online]. ©2019 [cit. 2019-02-01]. Dostupné z: https://www.iec.ch

[19] ITU. *Český telekomunikační úřad* [online]. ©2019 [cit. 2019-02-02]. Dostupné z: https://www.ctu.cz/mezinarodni-aktivity/itu

[20] O Úřadu. *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví* [online]. ©2019 [cit. 2019-02-03]. Dostupné z: http://www.unmz.cz/urad/o-uradu

[21] Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) ze dne 21. května 2018.

[22] Building an Information Technology Security Awareness and Training Program: Computer security. Gaithersburg, U.S.: National Institute of Standards and Technology, 2003.

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and related Technology
CRAMM	CCTA Risk Analysis and Management Method
CSIRT	Computer Security Incident Response Team
ČSN	Česká technická norma
DPO	Data Protection Officer
EU	Evropská unie
GDPR	General Data Protection Regulation
HW	Hardware
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDCA	Plan, Do, Check, Act
PZTS	Poplachový zabezpečovací a tísňový systém
SAE	Security Awareness Education
SLA	Service Level Agreement
SW	Software
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
VPN	Virtual Private Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

Příloha 1: Matice zranitelnosti

Zranitelnost [V]		INFORMAČNÍ AKTIVA						HARDWAROVÁ AKTIVA										SOFTWAROVÁ AKTIVA										SLUŽBY								
	Zdroj	*IS*	*IS*	*IS, servery*	*servery (GitLab)*	*servery*	*cloud*						*pasivní síťové prvky*	*aktivní síťové prvky*	*synology*	*USB flash disky*	*servery*	*servery*	*servery*	*pracovní stanice*	*notebooky*	*servery*	*servery*	*servery*	*servery*	*servery*	*servery*	*servery*	*servery*	*cloud*	*pobočka*	*cloud*	*pobočka*	*office 365*	*servery*			*interní IT oddělení*
	Aktivum	Data o zákaznících	Data o zaměstnancích	Interní data	Zdrojové kódy	Zálohy dat		Pracovní stanice	Servery	Tiskárny	Notebooky	Mobilní zařízení	Síťová infrastruktura		Datové úložiště	Elektronické nosiče	Kamerový systém	Zabezpečovací systém (PZTS)	Operační systémy			Informační systém (IS)	JIRA (systém pro vývoj SW)	Confluence (intranet)	GitLab (verzování kódu)	Účetní software	PZTS software	Software IP kamer	Internetové připojení		Elektrická energie		Elektronická pošta	Webové stránky	Cloud computing	Vzdálené připojení (VPN)	Údržba, servis
	A	5	4	5	4	4	4	3	5	1	3	2	3	3	3	1	2	2	3	2	2	5	4	4	4	3	2	1	4	4	4	4	3	3	5	4	2
Hrozba	**T**																																				
Požár	2							4	3	2	4	2	4	3	3	4	2	2											2	3	2	3					1
Poškození vodou	1							3	2	2	4	3	2	2	2	3	1	1											1	2	1	3					2
Znečištění	3							3	2	3	3	2	1	1	2	3	1	1																			3
Zničení zařízení nebo médií	2							3	3	2	4	3	2	2	3	4	2	2											1	2	1	1					2
Povodeň	1							5	2	3	5	4	5	3	2	5	5	5											3	4	4	5					
Selhání klimatizace nebo dodávky vody	2								4				2	4	4																					2
Přerušení dodávky elektřiny	3	4	4	4	4	4	2	2	4	1	2	1	4	4	4		4	4											4	5	4	5					4
Selhání telekomunikačního zařízení	4	4	4	4	4	3	2	3	3	2	3	3	2	2	3		2	2											4	5					4	4	
Vzdálená špionáž	2	4	4	4	4	4	4	2		1	3	2	1	3					2	2	2	5	4	4	4	2	2	2					4	2	4	2	
Krádež médií nebo dokumentů	3	4	4	4	4	2	3																														
Krádež zařízení	3							3	1	2	4	4		1	1	4	1	1																			
Zprovoznění recyklovaných nebo vyřazených médií	1															4																					
Vyzrazení	4	4	4	4	4	3	3																														
Data pocházející z nedůvěryhodných zdrojů	3							1			1	1										1	1	1	1	1											
Falšování pomocí technického vybavení	4					1	1	2	2	1	3	2		2	2		1	1											2	3							2
Falšování pomocí aplikačního programového vybavení	4					2	2												1	1	1	2	2	2	2	1	1	1									
Odhalení pozice	2										3	3																									
Selhání zařízení	3							2	3	1	2	1	1	3	3	2	2	2																			
Chybné fungování zařízení	3							2	4	1	2	1	2	4	4	3	2	2																			
Chybné fungování aplikačního programového vybavení	3					3	3												3	3	3	5	2	2	2	2	1	1	1	1			1	2	1	2	
Chyba údržby	2							3	3	2	3	2	2	3	3	3	1	1	3	2	2	3	2	2	2	2	1	1	1	1	1	1			2		5
Neoprávněné použití zařízení	3							3	2	1	4	1	3	2	2	3	1	1																			
Podvodné kopírování aplikačního programového vybavení	3																		1	2	2	3	3	3	3	1	1	1									
Poškození dat	3	3	3	3	3	4	3												1	2	2	3	3	3	3	2	1	1									
Nezákonné zpracování dat	1	3	4	4	4	3	3															4				4		3					2	1	1		
Chyba v používání	3	4	4	4	4	4	3	3	3	2	3	2	4	3	3	3	2	2	3	3	3	4	3	3	3	3	2	2	2	2	2	2	2		2		
Zneužití oprávnění	4	3	3	3	3	3	3	3	3	2	3	2		3	3		2	2	2	3	3	4	4	4	4	3	1	1	2	2							
Odepření činností	3							2	3	1	2	1		3	3		2	2	2	3	3	3	3	3	3	3	2	2	3	3				1	3	4	

Příloha 2: Matice rizik

Úroveň rizika [R]		INFORMAČNÍ AKTIVA						HARDWAROVÁ AKTIVA										SOFTWAROVÁ AKTIVA									SLUŽBY							
	Zdroj	*IS*	*IS*	*IS, servery*	*servery (GitLab)*	*servery*	*cloud*						*pasivní síťové prvky*	*aktivní síťové prvky*	*synology*	*USB flash disky*	*servery*	*servery*	*servery*	*pracovní stanice*	*notebooky*	*servery*	*servery*	*servery*	*servery*	*servery*	*servery*	*servery*	*servery*	*cloud*	*pobočka*	*cloud*	*pobočka*	*office 365*	*servery*			*interní IT oddělení*
	Aktivum	Data o zákaznících	Data o zaměstnancích	Interní data	Zdrojové kódy	Zálohy dat		Pracovní stanice	Servery	Tiskárny	Notebooky	Mobilní zařízení	Síťová infrastruktura		Datové úložiště	Elektronické nosiče	Kamerový systém	Zabezpečovací systém (PZTS)	Operační systémy			Informační systém (IS)	JIRA (systém pro vývoj SW)	Confluence (intranet)	GitLab (verzování kódu)	Účetní software	PZTS software	Software IP kamer	Internetové připojení		Elektrická energie		Elektronická pošta	Webové stránky	Cloud computing	Vzdálené připojení (VPN)	Údržba, servis
	A	5	4	5	4	4	4	3	5	1	3	2	3	3	3	1	2	2	3	2	2	5	4	4	4	3	2	1	4	4	4	4	3	3	5	4	2
Hrozba	**T**																																				
Požár	2							24	30	4	24	8	24	18	18	8	8	8											16	24	16	24					4
Poškození vodou	1							9	10	2	12	6	6	6	6	3	2	2											4	8	4	12					4
Znečištění	3							27	30	9	27	12	9	9	18	9	6	6																			18
Zničení zařízení nebo médií	2							18	30	4	24	12	12	12	18	8	8	8											8	16	8	8					8
Povodeň	1							15	10	3	15	8	15	9	6	5	10	10											12	16	16	20					
Selhání klimatizace nebo dodávky vody	2								40				12	24	24																					8
Přerušení dodávky elektřiny	3	60	48	60	48	48	24	18	60	3	18	6	36	36	36		24	24											48	60	48	60					24
Selhání telekomunikačního zařízení	4	80	64	80	64	48	32	36	60	8	36	24	24	24	36		16	16											64	80					80	64	
Vzdálená špionáž	2	40	32	40	32	32	32	12		2	18	8	6	18					12	8	8	50	32	32	32	12	8	4					24	12	40	16	
Krádež médií nebo dokumentů	3	60	48	60	48	24	36																														
Krádež zařízení	3							27	15	6	36	24		9	9	12	6	6																		
Zprovoznění recyklovaných nebo vyřazených médií	1															4																					
Vyzrazení	4	80	64	80	64	48	48																														
Data pocházející z nedůvěryhodných zdrojů	3							9			9	6										15	12	12	12	9											
Falšování pomocí technického vybavení	4					16	16	24	40	4	36	16		24	24		8	8											32	48							16
Falšování pomocí aplikačního programového vybavení	4					32	32												12	8	8	40	32	32	32	12	8	4								
Odhalení pozice	2										18	12																									
Selhání zařízení	3							18	45	3	18	6	9	27	27	6	12	12																			
Chybné fungování zařízení	3							18	60	3	18	6	18	36	36	9	12	12																			
Chybné fungování aplikačního programového vybavení	3					36	36												27	18	18	75	24	24	24	18	6	3	12	12			9	18	15	24	
Chyba údržby	2							18	30	4	18	8	12	18	18	6	4	4	18	8	8	30	16	16	16	12	4	2	8	8	8	8			20		20
Neoprávněné použití zařízení	3							27	30	3	36	6	27	18	18	9	6	6																			
Podvodné kopírování aplikačního programového vybavení	3																		9	12	12	45	36	36	36	9	6	3									
Poškození dat	3	45	36	45	36	48	36												9	12	12	45	36	36	36	18	6	3									
Nezákonné zpracování dat	1	15	16	20	16	12	12															20				12		3					6	3	5		
Chyba v používání	3	60	48	60	48	48	36	27	45	6	27	12	36	27	27	9	12	12	27	18	18	60	36	36	36	27	12	6	24	24	24	24	18		30		
Zneužití oprávnění	4	60	48	60	48	48	48	36	60	8	36	16		36	36		16	16	24	24	24	80	64	64	64	36	8	4	32	32							
Odepření činností	3							18	45	3	18	6		27	27		12	12	18	18	18	45	36	36	36	27	12	6	36	36				9	45	48	

Příloha 3: Prohlášení o aplikovatelnosti první etapy

A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Ustanovit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci.

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Vyloučeno	Ne
Způsob plnění požadavku	Definování a přidělení odpovědností vedením organizace

A.6.1.2 Princip oddělení povinností

Vyloučeno	Ne
Způsob plnění požadavku	Aktualizace dokumentu s popisem pracovních pozic (role, práva, povinnosti a odpovědnosti) a následné nastavení v Active Directory

A.6.1.3 Kontakt s příslušnými orgány a autoritami

Vyloučeno	Ne
Způsob plnění požadavku	Sledování novinek na webových stránkách Národního centra kybernetické bezpečnosti a Národního CSIRT České republiky

A.6.1.4 Kontakt se zájmovými skupinami

Vyloučeno	Ne
Způsob plnění požadavku	Členství v odborných fórech nebo účast na konferencích o bezpečnosti

A.6.1.5 Bezpečnost informací v řízení projektů

Vyloučeno	Ne

Způsob plnění požadavku	Zajištění požadavků na informační bezpečnost a její implementace do řízení projektů nezávisle na typu projektu

A.6.2 Mobilní zařízení a práce na dálku

Cíl: Zajistit bezpečnost při používání mobilních zařízení a pro práci na dálku.

A.6.2.1 Politika mobilních zařízení

Vyloučeno	Ne
Způsob plnění požadavku	Vytvoření politik a manuálu uživatele pro používání mobilních zařízení

A.7 Bezpečnost lidských zdrojů

A.7.2 Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti bezpečnosti informací.

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Vyloučeno	Ne
Způsob plnění požadavku	Vytvoření plánu vzdělávání zaměstnanců, pravidelná školení za účelem zvyšování kvalifikace zaměstnanců a jejich povědomí o informační bezpečnosti

A.8 Řízení aktiv

A.8.1 Odpovědnost za aktiva

Cíl: Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.

A.8.1.3 Přípustné použití aktiv

Vyloučeno	Ne

Způsob plnění požadavku	Vytvoření dokumentu definující přípustné použití aktiv

A.8.2. Klasifikace informací

Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.

A.8.2.1 Klasifikace informací

Vyloučeno	Ne
Způsob plnění požadavku	Na základě dokumentace ISMS

A.8.2.2 Označování informací

Vyloučeno	Ne
Způsob plnění požadavku	Na základě dokumentace ISMS

A.8.2.3 Manipulace s aktivy

Vyloučeno	Ne
Způsob plnění požadavku	Na základě dokumentace ISMS

A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a / nebo integrity informací.

A.10.1.1 Politika pro použití kryptografických opatření

Vyloučeno	Ne
Způsob plnění požadavku	Vytvoření dokument definující postupy pro kryptografii

A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.2 Zařízení

Cíl: Přecházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.

A.11.2.2 Podpůrné služby

Vyloučeno	Ne
Způsob plnění požadavku	Zajištění redundantního internetového připojení, údržba již implementovaného záložního zdroje nepřerušovaného napájení

A.11.2.4 Údržba zařízení

Vyloučeno	Ne
Způsob plnění požadavku	Definování povinností související s údržbou zařízení (SLA)

A.11.2.5 Přemístění aktiv

Vyloučeno	Ne
Způsob plnění požadavku	Definování přemisťování aktiv mimo organizaci

A.11.2.8 Uživatelská zařízení bez obsluhy

Vyloučeno	Ne
Způsob plnění požadavku	Vytvoření směrnice pro správnou obsluhu zařízení

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Vyloučeno	Ne
Způsob plnění požadavku	Vytvoření směrnice věnující se zásadě prázdného stolu a prázdného monitoru

A.12 Bezpečnost provozu

A.12.2 Ochrana proti malwaru

Cíl: Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru.

A.12.2.1 Opatření proti malwaru

Vyloučeno	Ne

Způsob plnění požadavku	Instalace antiviru a firewallu, pravidelné zálohování dat s pravidlem 3-2-1

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a vytvářet záznamy.

A.12.4.4 Synchronizace hodin

Vyloučeno	Ne
Způsob plnění požadavku	Synchronizace hodin všech důležitých systémů podle externího zdroje (atomové hodiny)

A.13 Bezpečnost komunikací

A.13.2 Přenos informací

Cíl: Zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty.

A.13.2.1 Politiky a postupy při přenosu informací

Vyloučeno	Ne
Způsob plnění požadavku	Vytvoření dokument definující postupy při přenosu informací

A.13.2.2 Dohody o přenosu informací

Vyloučeno	Ne
Způsob plnění požadavku	Do dohod se zákazníky zanést informaci o přenosu informací

A.13.2.3 Elektronické předávání zpráv

Vyloučeno	Ne
Způsob plnění požadavku	Vytvoření směrnice věnující se elektronickému předávání zpráv

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

A.17.2 Redundance

Cíl: Zajistit dostupnost vybavení pro zpracování informací

A.17.2.1 Dostupnost vybavení pro zpracování informací

Vyloučeno	Ne
Způsob plnění požadavku	Zajistit redundanci informačních systémů, které jsou důležité pro chod organizace

Příloha 4: Asistované zhodnocení

ISMS

Je stanoven rozsah ISMS.
nezavedeno
Jsou stanoveny cíle ISMS.
nezavedeno
Je zaveden proces řízení rizik.
nezavedeno
Jsou vytvořeny, schváleny a zavedeny bezpečnostní politiky v oblasti ISMS, zavedena příslušná bezpečnostní opatření.
nezavedeno
Je prováděn audit kybernetické bezpečnosti u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti“).
nezavedeno
Zajištěno pravidelné vyhodnocení účinnosti ISMS, které obsahuje hodnocení stavu ISMS včetně revize hodnocení rizik, posouzeny výsledky provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na ISMS.
nezavedeno
Je prováděna aktualizace ISMS a související dokumentace na základě zjištění auditů kybernetické bezpečnosti, výsledků hodnocení účinnosti ISMS a v souvislosti s prováděnými významnými změnami.
nezavedeno
Řízen provoz a zdroje ISMS, zaznamenávány činnosti spojené s ISMS a řízením rizik.
nezavedeno

Řízení aktiv

Jsou identifikována a evidována aktiva.
zavedeno
Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za aktiva.
zavedeno

Je hodnocena důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a tato aktiva jsou zařazena do jednotlivých úrovní.	
částečně zavedeno	*Aktiva jsou pouze hodnocena, rozřazení chybí.*
Jsou určeny a evidovány vazby mezi primárními a podpůrnými aktivy a hodnoceny důsledky závislostí mezi primárními a podpůrnými aktivy.	
nezavedeno	
Při hodnocení důležitosti primárních aktiv je posouzeno především: - rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství, - rozsah dotčených právních povinností nebo jiných závazků, - rozsah narušení vnitřních řídících a kontrolních činností, - poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty, - dopady na poskytování důležitých služeb, - rozsah narušení běžných činností, - dopady na zachování dobrého jména nebo ochranu dobré pověsti, - dopady na bezpečnost a zdraví osob, - dopady na mezinárodní vztahy, - dopady na uživatele informačního a komunikačního systému.	
částečně zavedeno	*Posouzena malá část z výše uvedeného.*
Jsou stanovena pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že: - jsou určeny způsoby rozlišování jednotlivých úrovní aktiv, - jsou stanovena pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv, - jsou stanoveny přípustné způsoby používání aktiv, - jsou zavedena pravidla ochrany odpovídající úrovni aktiv, - jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.	
nezavedeno	

Řízení rizik

Stanoveny metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro akceptovatelnost rizik.	
nezavedeno	
Prováděno hodnocení rizik v pravidelných intervalech a při významných změnách.	
nezavedeno	

Prováděna identifikace a hodnocení důležitosti aktiv, která patří do rozsahu ISMS. Výstupy jsou zapracovány do zprávy o hodnocení aktiv a rizik.
nezavedeno
Prováděna identifikace rizik, při kterých jsou zohledňovány hrozby a zranitelnosti, posuzovány možné dopady na aktiva.
nezavedeno
Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováváno prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření.
nezavedeno
Je zpracovaný a zavedený plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik, určení osoby odpovědné za prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.
nezavedeno
Zváženy zranitelnosti, související s: - nedostatečnou údržbou informačního a komunikačního systému, - zastaralostí informačního a komunikačního systému, - nedostatečnou ochranou vnějšího perimetru, - nedostatečným bezpečnostním povědomím uživatelů a administrátorů, - nevhodným nastavením přístupových oprávnění, - nedostatečnými postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, - nedostatečným monitorováním činností uživatelů a administrátorů a neschopností odhalit jejich nevhodné nebo závadné způsoby chování, - nedostatečným stanovením bezpečnostních pravidel, nepřesným nebo nejednoznačným vymezením práv a povinností uživatelů, administrátorů a bezpečnostních rolí, - nedostatečnou ochranou aktiv, - nevhodnou bezpečnostní architekturou, - nedostatečnou mírou nezávislé kontroly, - neschopností včasného odhalení pochybení ze strany zaměstnanců.
nezavedeno
Zváženy hrozby, související s/se: - porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany uživatelů a administrátorů, - poškozením nebo selháním technického anebo programového vybavení, - zneužití identity,

- užíváním programového vybavení v rozporu s licenčními podmínkami, - škodlivým kódem (například viry, spyware, trojské koně), - narušením fyzické bezpečnosti, - přerušením poskytování služeb elektronických komunikací nebo dodávek elektrické energie, - zneužitím nebo neoprávněnou modifikací údajů, - ztrátou, odcizením nebo poškozením aktiva, - nedodržením smluvního závazku ze strany dodavatele, - pochybením ze strany zaměstnanců, - zneužitím vnitřních prostředků, sabotáží, - dlouhodobým přerušením poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb, - nedostatkem zaměstnanců s potřebnou odbornou úrovní, - cíleným kybernetickým útokem pomocí sociálního inženýrství, použitím špionážních technik, - napadením elektronické komunikace (odposlech, modifikace).
nezavedeno

Organizační bezpečnost

Zajištěna dostupnost zdrojů potřebných pro ISMS.	
nezavedeno	
Informování zaměstnanců o významu ISMS a významu dosažení shody s jeho požadavky se všemi dotčenými stranami.	
nezavedeno	
Zajištěna podpora k dosažení zamýšlených výstupů ISMS.	
nezavedeno	
Zaměstnanci jsou vedeni a podporování k rozvíjení efektivity ISMS.	
nezavedeno	
Je prosazováno neustálé zlepšování ISMS.	
nezavedeno	
Stanovena pravidla pro určení administrátorů a osob, které budou zastávat bezpečnostní role.	
nezavedeno	
Zajištěna mlčenlivost administrátorů a osob zastávajících bezpečnostní role.	
zavedeno	*Etablováno v pracovní smlouvě.*

Určen výbor pro řízení kybernetické bezpečnosti.	
nerelevantní	*Vzhledem k velikosti organizace není potřeba.*
Určena bezpečnostní role: manažer kybernetické bezpečnosti.	
nezavedeno	
Určena bezpečnostní role: architekt kybernetické bezpečnosti.	
nerelevantní	*Vzhledem k velikosti organizace není potřeba.*
Určena bezpečnostní role: auditor kybernetické bezpečnosti.	
nerelevantní	*Vzhledem k velikosti organizace není potřeba.*
Určena bezpečnostní role: garant aktiva.	
nezavedeno	

Řízení dodavatelů

Jsou stanovena pravidla pro dodavatele, která zohledňují požadavky ISMS.	
nezavedeno	
Je vedena evidence svých významných dodavatelů a ti jsou písemně informování o evidenci.	
částečně zavedeno	*Dodavatelé jsou evidováni v interním IS.*
U dodavatelů je před uzavřením smlouvy prováděno hodnocení rizik, která jsou spojena s podstatnými dodávkami.	
nezavedeno	
U dodavatelů uzavírá smlouvu o úrovni služeb, která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.	
zavedeno	*S dodavateli služeb je uzavírána dohoda o úrovni poskytovaných služeb (SLA).*
U dodavatelů provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb a zjištěné nedostatky odstraňuje nebo po dohodě s dodavatelem zajistí jejich odstranění.	
nezavedeno	

Bezpečnost lidských zdrojů

Je stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a jsou určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny.	
nezavedeno	
V souladu s plánem rozvoje bezpečnostního povědomí je zajištěno poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení.	
nezavedeno	
O školení jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.	
nezavedeno	
Je zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.	
částečně zavedeno	*Kontrola je prováděna náhodně.*
Je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.	
zavedeno	*Prováděno i zdokumentováno.*
Jsou stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.	
částečně nezavedeno	*Pravidla jsou stanovena, ale nejsou sepsána.*
Je hodnocena účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí.	
nezavedeno	
Jsou určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.	
částečně nezavedeno	*Pravidla jsou stanovena, ale nejsou sepsána.*

Řízení provozu a komunikací

Zajištěn bezpečný provoz informačního a komunikačního systému. Za tímto účelem jsou stanoveny provozní pravidla a postupy.	
částečně zavedeno	*Je stanoveno několik provozních pravidel a postupů.*
Provozní pravidla a postupy orgánu a osoby obsahují:	

- práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů.	
částečně zavedeno	*Pravidla jsou stanovena, ale nejsou sepsána.*
Provozní pravidla a postupy orgánu a osoby obsahují: - postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů.	
zavedeno	*Ano, je i zdokumentováno.*
Provozní pravidla a postupy orgánu a osoby obsahují: - postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech.	
nezavedeno	
Provozní pravidla a postupy orgánu a osoby obsahují: - pravidla a postupy pro ochranu před škodlivým kódem.	
nezavedeno	
Provozní pravidla a postupy orgánu a osoby obsahují: - řízení technických zranitelností.	
nezavedeno	
Provozní pravidla a postupy orgánu a osoby obsahují: - spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.	
zavedeno	*Ano, je i zdokumentováno.*
Provozní pravidla a postupy orgánu a osoby obsahují: - postupy řízení a schvalování provozních změn.	
zavedeno	*Ano, je i zdokumentováno.*
Provozní pravidla a postupy orgánu a osoby obsahují: - postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.	
zavedeno	*Ano, zaznamenáno v interním IS.*
Provozní pravidla a postupy orgánu a osoby obsahují: - pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu.	
nezavedeno	
Provozní pravidla a postupy orgánu a osoby obsahují: - pravidla a postupy pro instalaci technických aktiv.	
zavedeno	*Ano, je i zdokumentováno. Zajišťuje interní IT oddělení.*
Provozní pravidla a postupy orgánu a osoby obsahují: - provádění pravidelného zálohování a kontroly použitelnosti provedených záloh.	

částečně zavedeno	*Nejsou prováděny kontroly použitelnosti záloh.*
Je zajištěno oddělení vývojového, testovacího a produkčního prostředí.	
zavedeno	
Výměna a předávání informací je prováděna na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla jsou dokumentována.	
nezavedeno	
S ohledem na klasifikaci aktiv je prováděna výměna a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.	
nezavedeno	

Řízení změn

V rámci řízení změn u informačního a komunikačního systému jsou přezkoumávány možné dopady změn a určeny významné změny.	
částečně zavedeno	*Jsou přezkoumávány možné dopady.*
U významných změn se: - dokumentuje jejich řízení, - provádí analýza rizik, - přijímají opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, - aktualizuje bezpečnostní politika a bezpečnostní dokumentace, - zajistí jejich testování, - zajistí možnost navrácení do původního stavu.	
částečně zavedeno	*Je zavedena malá část z výše uvedených požadavků.*

Řízení přístupu a bezpečné chování uživatelů

Na základě provozních a bezpečnostních potřeb je řízen přístup k informačnímu a komunikačnímu systému a každému uživateli je přiřazen jednoznačný identifikátor.	
zavedeno	*Každý uživatel se do IS přihlašuje pomocí svého účtu (uživatelského jména a hesla).*
Přístup je řízen na základě skupin a rolí.	
zavedeno	

Každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému jsou přidělena přístupová práva a oprávnění a jedinečný identifikátor.	
zavedeno	
Jsou zavedena bezpečnostní opatření pro řízení přístupu zařízení k prostředkům informačního a komunikačního systému.	
nezavedeno	
Jsou zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými povinná osoba nedisponuje.	
nezavedeno	
Je omezeno přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce.	
zavedeno	
Přidělování a odebírání přístupových oprávnění je prováděno v souladu s politikou řízení přístupu.	
nezavedeno	
Je prováděno pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí.	
částečně zavedeno	*Přezkoumávání probíhá nepravidelně.*
Je využíván nástroj pro ověřování identity uživatelů podle: Nástroj pro ověřování identity uživatelů (VKB § 18) a nástroj pro řízení přístupových oprávnění podle Nástroj pro řízení přístupových oprávnění (VKB § 19).	
zavedeno	*Adresářová služba Active Directory.*
Zajištěna změna přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.	
zavedeno	
Zajištěno odebrání nebo změna přístupových oprávnění při ukončení nebo změně smluvního vztahu.	
zavedeno	
Dokumentace přidělování a odebírání přístupových oprávnění.	
nezavedeno	

Akvizice, vývoj a údržba

Jsou stanoveny bezpečnostní požadavky na změny informačního a komunikačního systému spojené s jejich akvizicí, vývojem a údržbou a jsou zahrnuty do projektu akvizice, vývoje a údržby systému.
nezavedeno
Jsou identifikována, hodnocena a řízena rizika související s akvizicí, vývojem a údržbou informačního a komunikačního systému.
nezavedeno
Je zajištěna bezpečnost vývojového prostředí a testovacího prostředí a zároveň je zajištěna ochrana používaných testovacích dat.
nezavedeno
Je prováděno bezpečnostní testování změn před jejich zavedením do provozu.
nezavedeno

Řízení kontinuity činností

Jsou stanoveny práva a povinnosti administrátorů a osob zastávajících bezpečnostní role.
nezavedeno
Jsou vyhodnocovány a dokumentovány možné dopady kybernetických bezpečnostních incidentů a posouzena možná rizika související s ohrožením kontinuity činností.
nezavedeno
Jsou stanoveny cíle řízení kontinuity činností formou určení: - minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému.
nezavedeno
Jsou stanoveny cíle řízení kontinuity činností formou určení: - doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému.
nezavedeno
Jsou stanoveny cíle řízení kontinuity činností formou určení: - bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.
nezavedeno

Jsou stanoveny, aktualizovány a pravidelně testovány plány kontinuity činností a havarijní plány související s provozováním informačního a komunikačního systému a souvisejících služeb.
nezavedeno
Jsou realizována opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom z požadavků podle § 27.
nezavedeno

Fyzická bezpečnost

Je předcházeno poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému.	
částečně zavedeno	
Je stanoven fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovány informace a umístěna technická aktiva informačního a komunikačního systému.	
zavedeno	*Prostor je chráněn řadou fyzických bariér (např. bránou, zdmi, recepcí)*
U fyzického bezpečnostního perimetru jsou přijata nezbytná opatření a uplatněny prostředky fyzické bezpečnosti: - k zamezení neoprávněného vstupu, - k zamezení poškození a neoprávněným zásahům, - pro zajištění ochrany na úrovni objekt a v rámci objektů.	
částečně zavedeno	

Bezpečnost komunikačních sítí

Pro ochranu bezpečnosti komunikační sítě je zajištěna její segmentace.	
zavedeno	*Dělena dle geografické lokality a funkce. Je používána virtuální LAN (VLAN).*
Segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí.	
zavedeno	*DMZ zavedena a používána.*

Pomocí kryptografie zajistit důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo pří přístupu do komunikační sítě pomocí bezdrátových technologií.	
zavedeno	*OpenVPN, přístup k interní bezdrátové síti řešen pomocí protokolu IEEE 802.1x a RADIUS serveru.*
Aktivně je blokována nežádoucí komunikace.	
zavedeno	*Řešeno firewallem.*
Jsou využívány nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.	
zavedeno	*Řešeno pomocí VLAN.*

Správa a ověřování identit

Jsou používány nástroje pro správu a ověření identity uživatelů, administrátorů a aplikací informačního a komunikačního systému.	
zavedeno	*Adresářová služba Active Directory.*
Nástroj pro správu a ověřování identity uživatelů, administrátorů a aplikací zajišťuje: - ověření identity před zahájením aktivit v informačním a komunikačním systému, - řízení počtu možných neúspěšných pokusů o přihlášení, - odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití, - ukládání autentizačních údajů ve formě odolné proti offline útokům, - opětovné ověření identity po určené době nečinnosti, - dodržení důvěrnosti autentizačních údajů při obnově přístupu, - centralizovanou správu identit.	
zavedeno	*Zajišťuje adresářová služba Active Directory.*
Pro ověření identity uživatelů, administrátorů a aplikací je využíván autentizační mechanizmus, který není založený pouze na použití identifikátoru účtu a hesla, nýbrž na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů.	
nezavedeno	
Nástroj pro ověřování identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, musí vynucovat pravidla: - délku hesla alespoň 12 znaků u uživatelů a 17 znaků u administrátorů a aplikací, - umožňující zadat heslo o délce alespoň 64 znaků, - neomezující použití malých a velkých písmen, číslic a speciálních znaků,	

- umožňující uživatelům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut, - pro povinnou změnu hesla v intervalu maximálně po 18 měsících.	
částečně zavedeno	*Část nastavena pomocí skupinových politik (Group Policy)*
Nástroj pro ověřování identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, musí vynucovat pravidla **neumožňující** uživatelům a administrátorům: - zvolit si nejčastěji používaná hesla, - tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému, - opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.	
nezavedeno	
Nástroj pro ověřování identity uživatelů, administrátorů a aplikací, který používá k autentizaci pouze účet a heslo, musí vynucovat bezodkladnou změnu výchozího hesla po jejím prvním použití.	
nezavedeno	*Active Directory umožňuje vynucovat změnu výchozího hesla, ale to není zavedeno. Uživatelé si výchozí heslo mění přes interní portál.*

Řízení přístupových oprávnění

Je používán centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění: - pro přístup k jednotlivým aktivům informačního a komunikačního systému.	
zavedeno	*Řešeno na základě skupin v Active Directory.*
Je používán centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění: - pro čtení dat, pro zápis dat a pro změnu oprávnění.	
zavedeno	

Ochrana před škodlivým kódem

Je používán nástroj pro nepřetržitou automatickou ochranu: - koncových stanic.	
částečně zavedeno	*Antivirový program Windows Defender pouze na koncových stanicích s operačním systémem Windows.*

Je používán nástroj pro nepřetržitou automatickou ochranu: - mobilních zařízení.	
nezavedeno	
Je používán nástroj pro nepřetržitou automatickou ochranu: - serverů, datových úložišť a výměnných datových nosičů.	
částečně zavedeno	*U virtuálních privátních serverů (VPS) a cloud computingu (Google Cloud Platform) řeší ochranu poskytoval.*
Je používán nástroj pro nepřetržitou automatickou ochranu: - komunikační sítě a prvků komunikační sítě.	
částečně zavedeno	*Firewall, spam filter v rámci služby Office 356.*
Je prováděna pravidelná aktualizace nástroje pro ochranu před škodlivým kódem.	
částečně zavedeno	*Pouze u serverů a datových úložišť, jejichž ochranu řeší poskytovatel, je prováděna pravidelná aktualizace.*

Zaznamenávání událostí informačního a komunikačního systému

Jsou zaznamenávány bezpečnostní a potřebné provozní události důležitých aktiv informačního a komunikačního systému.	
zavedeno	*Každé technické aktivum má svůj log.*
Je prováděn sběr informací o bezpečnostních a provozních událostech, zaznamenává se zejména: - datum a čas, - typ činnosti, - identifikace technického aktiva, které činnost zaznamenalo, - jednoznačnou identifikaci účtu, pod kterým byla činnost provedena, - úspěšnost nebo neúspěšnost činnosti.	
nezavedeno	
Je prováděn sběr informací před neoprávněným čtením a jakoukoli změnou, zaznamenává se zejména: - přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů, - činnosti provedené administrátory, - úspěšná i neúspěšná manipulace s účty, oprávněními a právy, - neprovedení činností v důsledku nedostatku přístupových práv a oprávnění, - činnosti uživatelů, kteří mohou mít vliv na bezpečnost informačního a komunikačního systému, - zahájení a ukončení činností technických aktiv, - kritická a chybová hlášení technických aktiv.	
nezavedeno	

Nejméně jednou za 24 hodin je prováděna synchronizace jednotného systémového času technických aktiv patřících do informačního a komunikačního systému.	
nezavedeno	
Záznamy událostí jsou uchovávány nejméně po dobu 12 měsíců.	
nezavedeno	

Detekce kybernetických bezpečnostních událostí

Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí: - ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi.	
nezavedeno	
Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí: - ověření a kontrolu přenášených dat na perimetru komunikační sítě.	
nezavedeno	
Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí: - blokování nežádoucí komunikace.	
nezavedeno	

Aplikační bezpečnost

Jsou prováděny penetrační testy informačního a komunikačního systému se zaměřením na důležitá aktiva, a to před jejich uvedením do provozu a po každé zásadní změně.	
nezavedeno	
Je zajištěna trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností.	
zavedeno	*Řešeno proxy serverem.*

Kryptografické prostředky

Jsou používány aktuálně odolné kryptografické algoritmy a kryptografické klíče.	
nezavedeno	

Je používán systém správy klíčů a certifikátů, který: 1. zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů 2. umožní kontrolu a audit.	
zavedeno	*Používána firemní certifikační autorita.*
Jsou zohledňována doporučení v oblasti kryptografických prostředků vydaná Úřadem, zveřejněná na jeho internetových stránkách.	
nezavedeno	

Zajišťování úrovně dostupnosti informací

Jsou zavedena opatření pro zajišťování úrovně dostupnosti, kterými zajistí: - dostupnost informačního a komunikačního systému pro splnění cílů řízení kontinuity činností, - dostupnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, - dostupnost důležitých technických aktiv informačního a komunikačního systému, - redundanci aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému.	
nezavedeno	

Bezpečnostní politika

Politika systému řízení bezpečnosti informací
nezavedeno
Politika řízení aktiv
nezavedeno
Politika organizační bezpečnosti
nezavedeno
Politika řízení dodavatelů
nezavedeno
Politika bezpečnosti lidských zdrojů
nezavedeno

Bezpečnost lidských zdrojů	
nezavedeno	
Politika řízení přístupu	
částečně zavedeno	*Politika existuje, ale neobsahuje všechny náležitosti.*
Politika zálohování a obnovy a dlouhodobého ukládání	
částečně zavedeno	*Existuje pouze politika zálohování.*
Politika bezpečného předávání a výměny informací	
nezavedeno	
Politika řízení technických zranitelností	
nezavedeno	
Politika bezpečného používání mobilních zařízení	
nezavedeno	
Politika akvizice, vývoje a údržby	
nezavedeno	
Politika ochrany osobních údajů	
zavedeno	
Politika fyzické bezpečnosti	
zavedeno	
Politika bezpečnosti komunikační sítě	
zavedeno	
Politika ochrany před škodlivým kódem	
nezavedeno	
Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí	
nezavedeno	
Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí	
nezavedeno	
Politika bezpečného používání kryptografické ochrany	
nezavedeno	
Politika řízení změn	
nezavedeno	
Politika zvládání kybernetických bezpečnostních incidentů	

nezavedeno	
Politika řízení kontinuity činností	
nezavedeno	