Návrh bezpečnostní politiky vybraného subjektu

Lukáš Korytar

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš Korytar**
Osobní číslo:	**L15175**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Návrh bezpečnostní politiky vybraného subjektu**

Zásady pro vypracování:

1. **Seznamte se s problematikou bezpečnostní politiky firmy.**
2. **Proveďte analýzu rizik vybraného subjektu z pohledu bezpečnostní politiky informačních systémů.**
3. **Analyzujte možnosti implementace bezpečnostní politiky informačních systémů pro vybraný subjekt.**
4. **Diskutujte získané výsledky s cílem identifikace klíčových částí.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] JAŠEK, Roman. Ochrana znalostí a dat v podnikových informačních systémech. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 8073180952.

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

[3] SINGER, P. W. a Allan FRIEDMAN. Cybersecurity and cyberwar: what everyone needs to know. New York: Oxford University Press, c2014. ISBN 978-0-19-991-809-6.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **3. listopadu 2017**

Termín odevzdání bakalářské práce: **15. května 2018**

V Uherském Hradišti dne 15. listopadu 2017

doc. RNDr. Jiří Dostál, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské/diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1)];
- bakalářská/diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3[2)];
- podle § 60[3)] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60[3)] odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se bakalářská práce skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti 16. 4. 2018

.....
podpis studenta

---

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy. Vysoká škola disertační práce nezveřejňuje, byla-li již zveřejněna jiným způsobem.

(2) Bakalářské, diplomové, disertační a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

(4) Vysoká škola může odložit zveřejnění bakalářské, diplomové, disertační a rigorózní práce nebo jejich částí, a to po dobu trvání překážky pro zveřejnění, nejdéle však na dobu 3 let. Informace o odložení zveřejnění musí být spolu s odůvodněním zveřejněna na stejném místě, kde jsou

zveřejňovány bakalářské, diplomové, disertační a rigorózní práce, jíž se týká odklad zveřejnění podle věty první, jeden výtisk práce k uchování ministerstvu.

2) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Tématem této bakalářské práce je návrh zavedení managementu informační bezpečnosti ve fyzioterapeutické ordinaci. Práce je rozdělena na dvě části. V první části je uveden teoretický základ práce, který popisuje základy bezpečnosti informací a platnou legislativu České republiky. Druhá část je zaměřena na popis a analýzu daného subjektu, na návrh síťové infrastruktury a na návrh bezpečnostních opatření.

Klíčová slova: Informace, Bezpečnost, Infrastruktura, Opatření

ABSTRACT

The topic of this bachelor thesis is the proposal of information security management in the physiotherapy surgery. The thesis is divided into two parts. The first part presents the theoretical basis of the thesis which describes the basics of information security and valid legislation of the Czech Republic. The second part is focused on the description and analysis of the surgery subject, the design of the network infrastructure and the design of the security measures.

Keywords: Information, Security, Infrastructure, Measure

Rád bych tímto poděkoval vedoucímu mé bakalářské práce Ing. Petru Svobodovi za odborné rady, cenné připomínky a čas strávený při konzultaci této bakalářské práce. Dále panu Pavlu Vrbovi, DiS za poskytnuté informace. Rád bych poděkoval své rodině za toleranci a podporu při mém studiu.

OBSAH

ÚVOD

V dnešní době je každá organizace při výkonu svých činností plně závislá na svých pracovnících a jejich přístupu k hmotným a nehmotným aktivům. Součástí většiny organizací jsou plány, jakým způsobem chránit své pracovníky a aktiva. Často organizace požadují vytvoření systému, který by byl schopen řídit bezpečnost organizace. Organizace na základě takového systému stanovují cíle, strategii a politiku.

Ve většině podniků jsou téměř veškerá data ukládána do informačních systémů. Pokud tato data nejsou dostatečně zabezpečena, mohou být zneužita. To může mít v některých případech fatální následky. Touto problematikou se zabývá bezpečnostní politika, která definuje postupy, jak chránit informační aktiva organizace. Dodržování takové bezpečnostní politiky vede k eliminaci možného úniku, poškození či ztrátě dat. V roce 2018 vstoupilo v platnost nové nařízení o ochraně osobních údajů - GDPR, jež rozšiřuje definici osobních údajů například o e-mail, telefonní číslo, fotografický záznam, IP adresu či zdravotní stav. Při závažném porušení či odcizení osobních údajů je povinen správce tuto skutečnost ohlásit.

Práce je zaměřena na problematiku návrhu bezpečnostní politiky lékařského subjektu. Ten v rámci své denní činnosti přichází do kontaktu s citlivými informacemi, jako jsou rodná čísla, diagnózy pacientů aj. Důvěrná data jsou uložena v lékařském informačním systému. Lékařský subjekt musí ze zákona splňovat předpisy, jak nakládat s osobními údaji. Sám subjekt by rád zavedl samotnou bezpečnostní politiku. Bezpečnostní politika by měla jasně formulovat směrování řízení bezpečnosti informací. Pro realizaci bezpečnostní politiky jsou nutná připravit dvě opatření. První opatření představuje dokument, kterým majitel subjektu vyjádří cíl a význam bezpečnosti informací. Druhé opatření představuje pravidelnou revizi bezpečnostní politiky.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST INFORMACÍ

Bezpečnost informací je chápána jako zodpovědnost za chráněné informace během jejich životního cyklu, tedy vytvoření, zpracování, uložení, přenosu a konečné likvidace. Pro lepší pochopení bych v části bezpečnost informací vymezil několik základních pojmů této problematiky ve spojení s bezpečností. [1]

- Aktivum – jedná se o aktiva, která mají pro majitele informačního systému (dále také „IS“) hodnotový význam. Především se jedná o data, informace, které by při jejich ztrátě způsobili majiteli určitou škodu.
- Autentizace – proces, při kterém dochází k ověření identity uživatele.
- Autorizace – proces, který pověřuje uživatele k určité činnosti, je dán přístupovými právy, oprávněním.
- Citlivé informace – informace, které byly určeny odpovědnou autoritou, že se musí chránit
- Citlivá data – jsou data i informace, které vyžadují ochranu, protože existuje určitá pravděpodobnost působení hrozeb.
- Hrozba – jedná se o možné zdroje ohrožení informačních aktiv podniku. Může dojít k poškození, zničení, ztrátě důvěry nebo aktiva. Hrozba je nebezpečí reálné, potenciální, souvisí s rozvojem informačních technologií, které ohrožuje informační systém.
- Informační systém – jedná se o soubor technického a programového vybavení, dat a personálu, který působí v dané organizaci.
- Integrita – jedná se o vlastnost, která zaručuje nezměněná, neporušená data během jejich přenosu od zdroje k cíli.
- Útočník – osoba, která usiluje o nepovolený zásah do informačního systému, nebo o krádež, poškození dat.

1.1 Informační aktiva

Aktivy v oblasti IS/ICT se především rozumí: [2]

- Hmotná aktiva – do sekce hmotná aktiva spadá především technické vybavení - počítače, servery, kabelové rozvody, tiskárny.
- Nehmotná aktiva – je možné rozdělit do dalších 4 podkategorií
    - Pracovní postupy, které podnik využívá v IS/ICT.

- Data – vytvořená zaměstnanci podniku nebo převzaté datové soubory, které jsou podstatné pro fungování a provoz podniku.
- Programové vybavení – do této podkategorie spadají operační systémy, programové vybavené pro provoz počítačových sítí, aplikační vybavení.
- Služby – základní (světlo, teplo), počítačové, komunikační služby

1.2 Informační hrozby

Hrozba představuje možnost poškození informačního systému, jeho aktiv. Jedná se o možnost využít zranitelné místo IS k útoku na něj, způsobit škodu na aktivech. [3] Hrozby využívají zranitelností, možných chyb v programech či nastaveních, které umožní útočníkovi neoprávněný přístup k datům. [4]

Hrozby lze kategorizovat:

Tab. 1: Kategorizace hrozeb, Zdroj: [vlastní]

Kategorie	Druh	Příklad
Objektivní	Přírodní, fyzické Fyzikální Technické a logické	Požár, povodeň, výpadek napětí, porucha Elektromagnetické vyzařování Porucha paměti, špatné propojení komponent
Subjektivní	Neúmyslné Úmyslné	Působení neškoleného uživatele, správce IS Špioni, teroristé, hackeři, vnitřní útočníci (rozzlobený zaměstnanec)

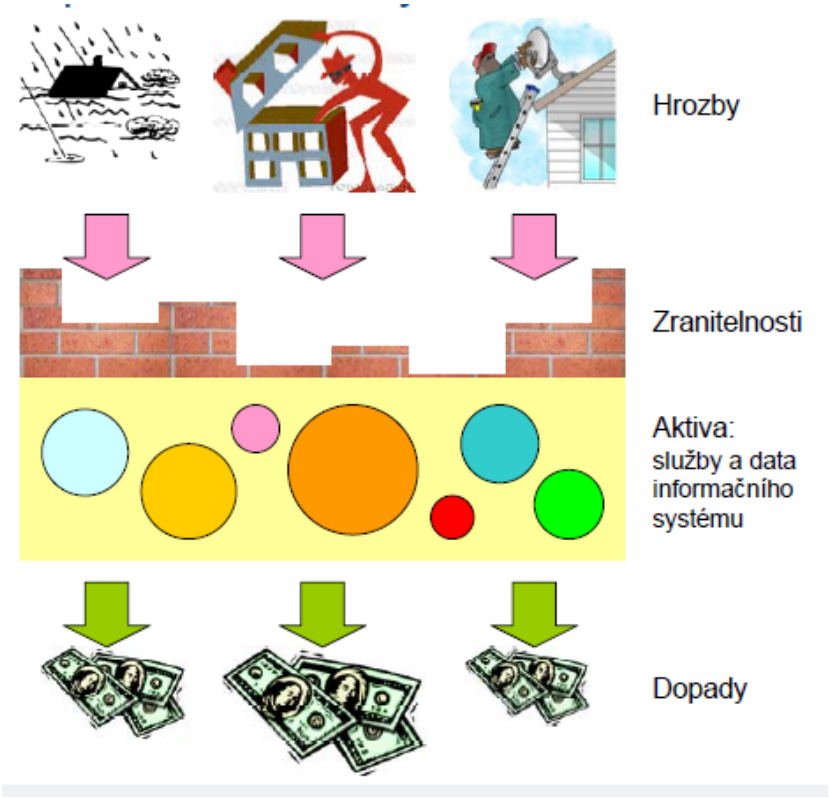
1.3 Informační zranitelnost

Zranitelností je nedostatek nebo slabá část celého bezpečnostního systému. Může dojít k poškození nebo zničení aktiv. Každý IS má zranitelná místa, prvky, které může útočník využít k získání či poškození dat. Slabinou může být aplikace, software, uživatelské chyby, podcenění bezpečnosti. [1]

Zranitelnost rozdělujeme na : [2]

- Fyzickou – součástí jsou budovy, počítačové místnosti.
- Technických programových prostředků – projevem bývá zpravidla chyba, porucha.
- Nosičů dat – nečitelnost nosiče, jeho selhání.
- Elektromagnetických záření – projevem je smazání obsahu nosiče při kontaktu s magnetickým polem.

- Komunikačních systémů a kabelových rozvodů – fyzické přerušení, případně možný odposlech.
- Personální – vyplývá z úmyslného nebo neúmyslného chování uživatelů, neznalosti nebo zanedbání plnění povinností.



Obr. 1: Zranitelnost [1]

1.4 Informační opatření

Rozumí se jakákoliv aktiva, technika, postup, který má schopnost snížit dopad hrozby, která působí na IS. Opatření může zcela zabránit účinku hrozby. Vhodným příkladem může být uzamykání objektů, používání přístupových hesel do systému.

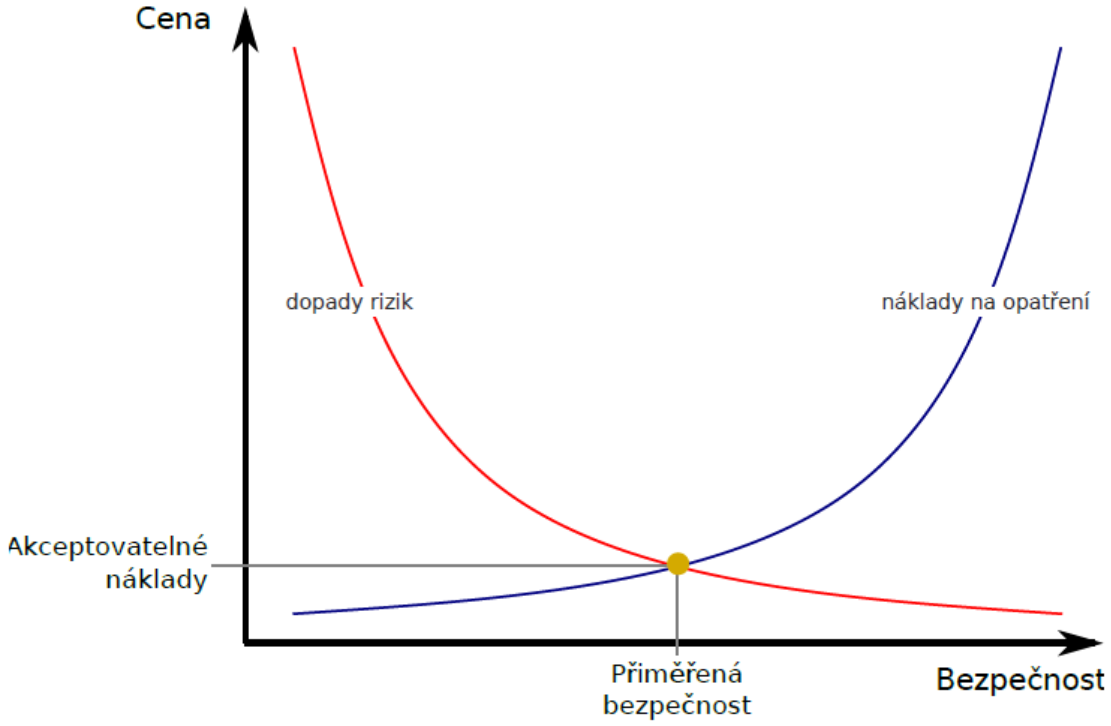
Opatření lze rozdělit podle charakteru: [2]

- Administrativní – opatření jako směrnice pro IS/ICT v organizaci. Směrnice pro postup autentizace, šifrování mailů, zálohování.
- Fyzická – používání zámků, trezorů, čipových karet pro přístup do režimových prostorů.
- Technický a technologický – autorizace a autentizace uživatelů k přístupu na IS/ICT. Ochrana přístupu pomocí hesel, biometrie.

2 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Pojem systém řízení bezpečnosti informací se zabývá zabezpečením sítě, fyzickými spoji, zabezpečením serveru, kódováním datových přenosů a jejich řešením, digitálními podpisy, firemními směrnicemi, autentizací, autorizací a autenticitou. Z toho lze odvodit, že se na informační bezpečnost nahlíží z několika úhlů pohledu. Systém řízení bezpečnosti informací (dále také „ISMS“) má za cíl zavedení a zajištění provozu, monitoringu a také údržby celého systému. ISMS je možné implementovat a používat v organizaci, která má alespoň deset pracovníků. Podrobněji je popsán v normě ISO/IEC 27001. ISMS používají organizace včetně veřejně právních institucí a orgánů státu. Důkazem o používání ISMS je spousta vládních organizací, které vyžadují implementaci ISMS. [2]

S pojmem ISMS souvisí takzvaná přiměřená bezpečnost. Přiměřená bezpečnost je definována jako střední hodnota mezi vynaloženými prostředky a získanou bezpečností. Jedná se o úkol managementu, který musí stanovit, jak velkou zabezpečovací úroveň potřebuje. Dále musí stanovit úroveň, kterou si může dovolit po stránce finanční. Větší váhu většinou mívá finanční rámec, neboť společnost má většinou omezené prostředky. [5]



Obr. 2: Graf přiměřené bezpečnosti [5]

2.1 Všeobecné požadavky

Základními požadavky na ISMS v podniku jsou:

- Ustanovení
- Zavedení
- Provozování
- Monitorování
- Přezkoumání
- Udržování
- Soustavné zlepšování

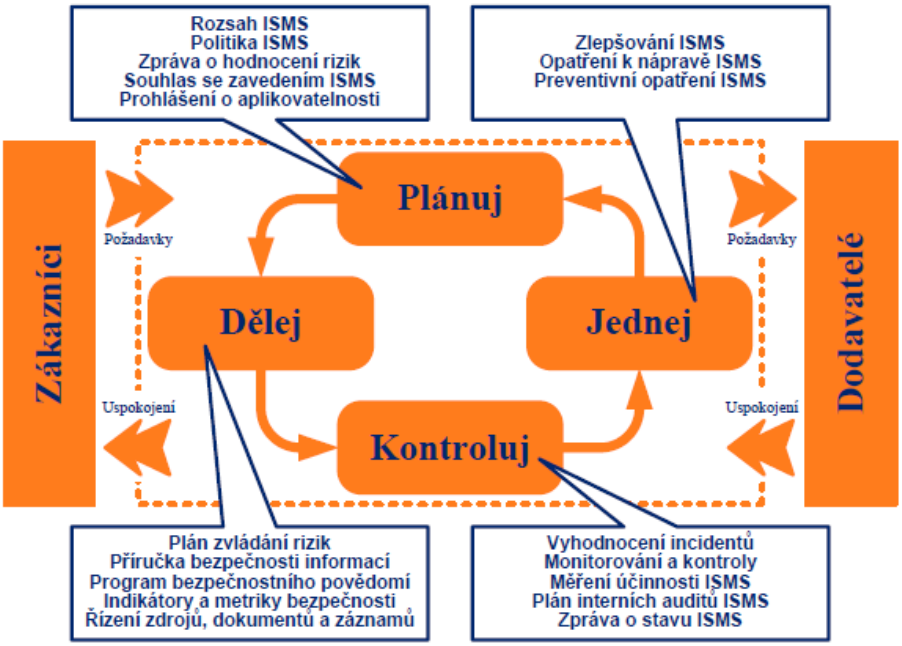
Všechny zmíněné požadavky musí být dokonale dokumentovány, a to v kontextu všech činností a identifikovaných rizik. Proces, který je použitý v normě, vychází z Demingova modelu PDCA.

2.2 Model PDCA

Model PDCA je interaktivní metoda postupného zlepšování systému. Použití je téměř neomezené a neustálým opakováním níže uvedených kroků dochází k neustálému zlepšování a rozvoji bezpečnosti. [5]

Model PDCA má 4 základní procesy:

- Plánuj (ustanovení ISMS) - první proces se zabývá vytvořením politiky ISMS, definuje cíle a postupy, které souvisí s řízením rizik. Nezbytnou částí je inovace ochrany informací tak, aby se splnil stanovený cíl, který je v politice ISMS.
- Dělej (zavedení a provozování ISMS) – zahrnuje zavedení a následné provedení politiky ISMS.
- Kontroluj (monitorování a přezkoumání ISMS) – v tomto procesu je zmíněno posouzení a případné měření výkonu. Zkoumá se, zda byly naplněny předem nadefinované cíle ISMS.
- Jednej (udržování a zlepšování ISMS) – poslední část definuje nezbytná opatření k nápravě vzniklých problémů a vytváří preventivních opatření. Všechny změny probíhají na základě interního podnikového auditu ISMS.



Obr. 3: Model pro řízení bezpečnosti informací [2]

Součástí PDCA modelu je dokumentace jednotlivých částí, která popisuje jednotlivé etapy. Jednou se o klíčovou dokumentaci zmíněného modelu. Pro práci s procesy v modelu PDCA je podstatné identifikace jednotlivých procesů. Druhou částí je popis a dokumentace procesů. Další částí je řízení procesů na základě dokumentace a finální optimalizace průběhu procesu. [5]

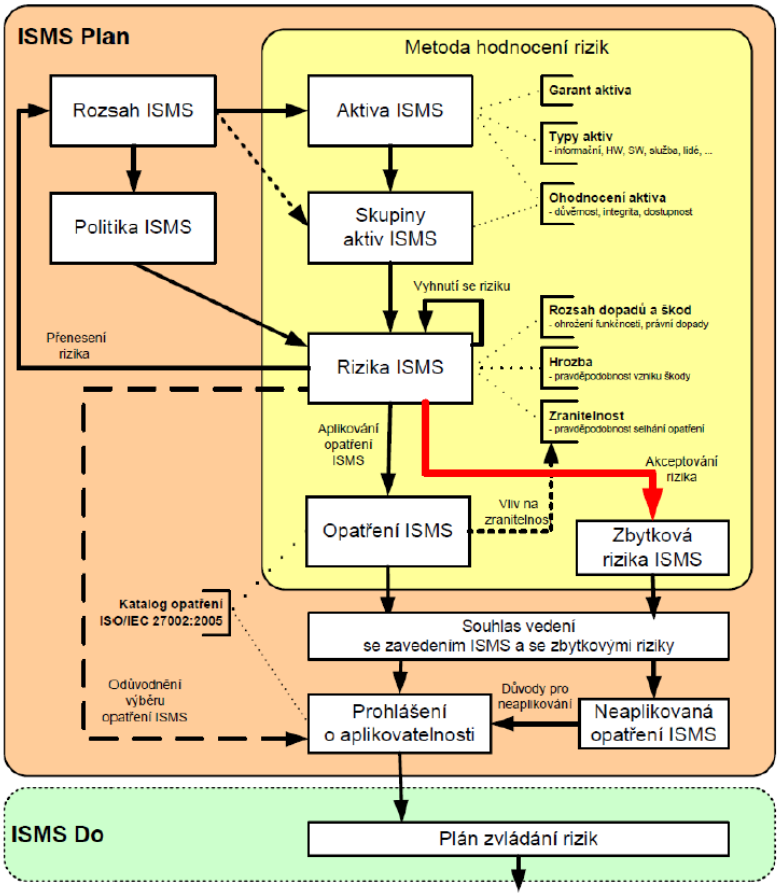
2.3 Ustanovení ISMS

První fází zavedení ISMS je jeho ustanovení. V této části jsou upřesněny správné formy řešení bezpečnosti informací, definován rozsah ISMS a odsouhlasení Prohlášení o politice ISMS. Do kritických činností spadá provedení analýzy rizik a dále výběr vhodných bezpečnostních opatření, která sníží vliv již existujících rizik. Etapa prosazování ISMS končí odsouhlasením vedení společnosti. [6]

Ustanovení ISMS je možné rozdělit:

- Definice rozsahu, hranic a vazeb.
- Definice a odsouhlasení politiky ISMS vedením organizace.
- Analýza a zvládání rizik.
- Příprava prohlášení o aplikovatelnosti.

Jedná se o nejdůležitější etapu budování ISMS, v této části jsou definovány základy celého systému řízení bezpečnosti informace. V případě, že by v této etapě vznikla chyba, promítnula by se i do dalších částí etap. [6]



Obr. 4 Přehled činností při ustanovení ISMS [2]

2.4 Zavádění a provoz ISMS

Ve fázi zavádění se soustředí pozornost na prosazení všech bezpečnostních opatření tak, jak bylo navrženo v předešlé části ustanovení ISMS. Příprava plánů s termíny a odpovědné osoby. Příručka bezpečnosti informací dokumentuje všechna bezpečnostní opatření.

V této etapě je nutné provést tyto činnosti: [2]

- Plánovací dokument zvládání rizik.
- Zavedení plánovaných bezpečnostních opatření, příprava příručky bezpečnosti informací, která upřesní pravidla a postupy opatření.
- Vytyčení programu budování bezpečnostního povědomí – zaškolení všech uživatelů, odborných pracovníků z úseku informatiky a oblasti řízení bezpečnosti.

- Upřesnění způsobů měření účinnosti bezpečnostních opatření.
- Zavedení procesu opatření pro detekci a reakci na bezpečnostní incident.
- Řízení zdrojů, dokumentů a záznamů ISMS.

2.5 Monitorování a přezkoumání ISMS

Cílem etapy monitorování a přezkoumání je zajištění zpětné vazby. Úkolem je prověření všech aplikovaných bezpečnostních opatření a také vzniklých důsledků těchto opatření na ISMS. Vlastní ověření provádí nadřízení pracovníci, případně bezpečnostní manažer s odpovědnými osobami formou přímé kontroly. Neméně podstatnou roli má interní audit ISMS, který posoudí fungování a následně účinnost ISMS. Jakmile jsou všechny zpětné vazby zaznamenány, připraví se dostatek podkladů o skutečném fungování ISMS. Poklady jsou dále předloženy vedení organizace, které posoudí, zda je ISMS realizováno v souladu s potřebami organizace. V této fázi jsou provedeny tyto činnosti: [2]

- Monitoring a ověření účinnosti prosazení bezpečnostních opatření - jedná se o zpětnou vazbu, která je nezbytná pro správné fungování ISMS. Součástí kontrol je schopnost včasné detekce chyb. Dále detekce úspěšných i neúspěšných pokusů o narušení bezpečnosti. Kontrolní činností je měření účinnosti ISMS a aplikovaných opatření.
- Provedení interního auditu ISMS – při plánování interního audit je důležité si uvědomit, že by měl být audit zaměřen rovnoměrně na celý rozsah ISMS. Samozřejmostí je zvážení cílů, priorit a rizikových oblastí ISMS. První částí, kterou audit prověřuje, jsou procesní pravidla, významným kritériem je naplnění požadavků ISO/IEC 27001. Druhou částí je prověření již implementovaných bezpečnostních opatření.
- Připravení zprávy o stavu ISMS – zpráva ISMS shrnuje vlastnosti ISMS, které fungují dobře. ISMS staví na zmíněných základních vlastnostech a zároveň stanovuje vlastnosti, které zatím nefungují. Tyto vlastnosti se musí postupně napravit.

Záměr každého auditu musí být naplánován s ohledem na stav a význam procesů, které jsou auditovány. Prováděný audit musí mít předem stanovená kritéria, rozsah a použité metody s ohledem na zaručení jejich opakovatelnosti. Auditoři provádí nestranný, objektivní audit, nesmí auditovat vlastní práci. Všechny výstupy auditu musí být dokumentovány.

Vedoucí pracovníci či bezpečnostní manažeři zodpovídají za svou oblast, která je předmětem auditu. V případě nedostatků musí zajistit jejich odstranění bez zbytečného odkladu. Nápravné kroky jsou dokumentovány a následně zpětně kontrolovány.

2.6 Údržba a zlepšování ISMS

Jedná se o poslední etapu prosazování ISMS. V této fázi dochází ke sběru žádostí, podnětů na zlepšení, nápravu ISMS. Během této fáze se provedou činnosti jako zavedení identifikované možnosti zlepšení ISMS. Druhou činností je provedení odpovídajícího opatření k nápravě. Možností jsou preventivní opatření pro odstranění nedostatků.

Zlepšování je řešeno formou zpětné vazby, která na jedné straně získává podněty, směřující k efektivnějšímu fungování ISMS. Zpětná vazby musí obsahovat nedostatky a jejich příčiny. [6]

2.7 Realizace bezpečnostních opatření

Východiskem pro realizaci ISMS je norma ISO/IEC 27002:2005 – Soubor postupů pro řízení bezpečnosti informací. Norma obsahuje zkušenost s řízením bezpečnosti informací, nahrazuje původní normu ISO/IEC 17799. Doporučení obsahuje 133 opatření týkající se bezpečnosti. Tato opatření jsou dále rozčleněna do 11 oblastí.

Obr. 5: Oblasti bezpečnosti informací [2]

Rozdělení jednotlivých skupin bezpečnostních opatření: [6]

- Bezpečnostní politika – uvádí základní pravidla pro správné fungování bezpečnosti informací. Obsahuje vyjádření podpory vedení organizace.
- Organizace bezpečnosti – rozděluje řízení bezpečnosti informací na dvě části. První je řízení bezpečnosti uvnitř organizace. Druhou částí je řízení bezpečnosti ve vztahu k externím subjektům mimo organizaci.
- Řízení aktiv – obsahuje přehled o existujících a vyřazených aktivech uvnitř organizace. Přehled existujících aktiv stanovuje odpovědnosti osob za udržování ochrany jednotlivých aktiv.
- Bezpečnost z hlediska lidských zdrojů – definuje povinnosti za ochranu informací všech pracovníků. Slouží jako zdroj informací pro bezpečnostní povědomí.
- Fyzická bezpečnost a bezpečnost prostředí – stanovuje pravidla pro povolené přístupy pracovníků do klíčových prostorů organizace. Zmíněna je ochrana zařízení, jako je zabezpečení prostředí serveru.
- Řízení komunikací a řízení provozu – zajišťuje spolehlivý a bezpečný chod produkčních informačních systémů a komunikačních systémů uvnitř organizace.
- Řízení přístupu – stanovuje pravidla pro přidělování přístupu k informačnímu a komunikačnímu systému. Pravidla pro sledování způsobu využívání dostupných prostředků.
- Akvizice, vývoj a údržba informačních systémů – pro projekty týkající se rozvoje ICT jsou prosazovány principy bezpečnosti informací.
- Zvládání bezpečnostních incidentů – stanovuje postupy a pravidla, která jsou určená pro řešení bezpečnostních incidentů.
- Řízení kontinuity činnosti organizace – definuje postupy prevence a minimalizace škod. Zaměřeno je na škody, které jsou způsobeny havárií, živelnou pohromou či jinou mimořádnou událostí.
- Soulad s požadavky – organizace vystavuje doklad o naplnění požadavků vyplývajících z právních, smluvních a jiných závazků.

Výhodou nové normy ISO/IEC 27002:2005 je její formální zobrazení. Původní doporučení byla zobrazována jako strukturovaný text, který nebyl uživatelsky přívětivý. V nové podobě jsou rozlišeny tři typy popisu opatření: [6]

- Definice opatření – specifikace bezpečnostních opatření definované v jedné větě. Vychází z normy ISO/IEC 27001:2005 příloha A.
- Směrnice pro zavedení – podrobně definuje jednotlivá opatření. Rozebírá myšlenku opatření, způsob jeho zavedení. Ne všechny informace jsou platné pro všechny případy nasazení, směrnice připouští aplikování i jiných metod.
- Další informace – jsou uvedeny specifické údaje spojené s implementací. Součástí jsou právní důsledky, odkazy na specifické bezpečnostní normy.

2.8 Bezpečnostní politika

- Při zavádění systému řízení bezpečnosti informací je bezpečnostní politika na vrcholu pyramidy všech úkonů. Samotná politika slouží jako výchozí dokument, který zavádí pravidla, určuje interní směrnice a také definuje postupy. Primární účel bezpečnostní politiky je řízení, ochrana informačních aktiv. Pro zavedení politiky je nutné jasně formulovat směrování řízení bezpečnosti informací v organizaci a vyjádřit zájem nejvyššího vedení organizace bezpečnost informací podporovat. Pro realizaci zmíněných cílů jsou definována dvě opatření: [2]

První opatření

Zabývá se potřebou nadefinovat dokument bezpečnostní politiky, kterému následně vedení organizace vymezí další požadavky.

- Vyjádření cílů, významu bezpečnosti informací
- Upřesnění základních bezpečnostních zásad, pravidel
- Určení odpovědnosti a pravomocí
- Vyjádření zájmu prohlubovat bezpečnost informací

Dokument se zmíněnými náležitostmi se stává hlavním východiskem pro prosazování bezpečnosti.

Druhé opatření

Má za cíl zajistit pravidelnou revizi bezpečnostní politiky. Revizi provádí vlastník bezpečnostní politiky na žádost vedení organizace. Přezkoumává se vhodnost, přiměřenost a efektivnost definovaných opatření.

Bezpečnostní politika obsahuje:

- Definici bezpečnosti informací, cíle, rozsah, význam a důležitost.
- Záměr vedení podniku podporovat cíle a principy bezpečnosti informací.
- Stručný výklad bezpečnostních zásad, principů standardů a případné speciální požadavky.
- Definice obecných a specifických odpovědností pro řízení bezpečnosti informací i pro hlášení případných bezpečnostních incidentů.
- Odkazy na dokumentaci, kde lze nalézt detailnější bezpečnostní politiku. Postupy specifické oblasti či bezpečnostní pravidla, která by měla být pracovníky dodržována.

Podle kritérií hodnocení bezpečnosti informačních systémů se zpracovávají tři úrovně politik:

- Celková – definuje cíle, jakým způsobem jsou zajištěny celkové bezpečnosti informačního systému.
- Systémová – má za cíl popsat způsob zajištění bezpečnosti informačního systému podniku. Dále zahrnuje popis vnitřních a vnějších vazeb informačního systému podniku. Popisuje bezpečnostní opatření informačního systému. Vyhodnocuje analýzu rizik IS.
- Technická – popisuje konkrétní opatření pro zajištění bezpečnosti při využívání zdrojů.

Bezpečnostní politika je základem funkčního systému řízení bezpečnosti organizace. Jde o základní část jistoty vedení organizace, které spoléhá, že aktiva organizace jsou perfektně zabezpečena proti škodám či jejich zničení.

3 ANALÝZA RIZIK

Při zavádění bezpečnostní politiky je analýza rizik jedním z nejdůležitějších kroků. Analýza rizik bývá většinou chápána jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva. Ve většině případů nebývá riziko izolované, ale bývá určitou kombinací rizik, které mohou představovat hrozbu pro organizaci. V úvahu je nutné určit priority z pohledu dopadu a pravděpodobnosti jejich výskytu a zaměření se na podstatné rizikové oblasti. Při analýze rizik se provede skupina kroků následujících za sebou. [7]

- Stanovení hranice analýzy rizik – vyberou se aktiva, která budou zahrnuta do analýzy. Ostatní aktiva budou vyloučena. Stanovení hranice analýzy vychází ze záměrů managementu organizace, z úvodní studie. Uvnitř hranice analýzy budou ležet aktiva, která mají vztah k cílům managementu v rámci procesu snižování rizik. Ostatní aktiva budou umístěna mimo. Stanovení pomyslné hranice říká, že uvnitř hranice budou ležet jednotlivá aktiva, ze kterých je subjekt složen, případně aktiva, která jsou z hlediska aktuálního záměru relevantní.
- Identifikace aktiv – vzniká se soupisem všech aktiv, které jsou uvnitř nadefinované hranice analýzy rizik.
- Stanovení hodnoty a seskupování aktiv – hodnota aktiva vzniká v závislosti na velikosti škody, která je způsobena zničením, ztrátou aktiva. Obvyklý způsob vychází z pořizovací ceny. Může ale vycházet i z výnosových charakteristik - za předpokladu, že aktivum přináší identifikovatelné zisky pro subjekt. Použijí se vždy ty charakteristiky, které mají vyšší hodnotu pro organizaci. Jako příklad lze uvést ochranné známky, patenty, průmyslové vzory, kvalifikace, know-how či nové technologie. Stanovení hodnoty bere v potaz, jak moc je podnik závislý na daném aktivu, jakým způsobem by byl podnik ovlivněn, pokud by se aktivum ztratilo, bylo nedostupné, případně by se zničilo. Vzhledem k tomu, že každá organizace může identifikovat velké množství aktiv, je doporučeno tato aktiva seskupovat do definovaných celků podle jejich povahy. Seskupují se ta, která mají stejnou nebo podobnou kvalitu, cenu či účel. Seskupený celek dále vystupuje jako jedno aktivum. Nutné je zabezpečit, aby případná protiopatření pro skupinu aktiv byla aplikována všem členům v seskupení aktiv.

- Identifikace hrozeb – tato část analýzy rizik říká, jak se hrozby identifikují. Vybrány jsou hrozby, které mají předpoklad ohrožení alespoň jedno z aktiv subjektu. V samotné identifikaci hrozeb se vychází ze seznamu hrozeb, který je běžně sestaven na základě literatury, vlastních zkušeností, průzkumů, případné předešlé analýzy. Samotnou hrozbu lze odvodit na základě statusu subjektu, jde-li o podnikatelský subjekt, orgán státu nebo neziskovou organizaci. Pro vytvoření seznamu je možné použít některou z metod jako brainstorming, diagram příbuznosti, strukturované rozhovory.
- Analýza hrozeb a zranitelností – všechny identifikované hrozby je nutné hodnotit vůči každému aktivu. U aktiv, u nichž se může hrozba uplatnit, je nutné stanovit úroveň této hrozby vůči tomuto aktivu a dále úroveň zranitelnosti aktiva vůči dané hrozbě. Faktory jako jsou nebezpečnost, motivace, přístup jsou použity k stanovení úrovně hrozby. Citlivost a kritičnost slouží ke stanovení úrovně zranitelnosti. Při použití této analýzy se musí brát v potaz případná protiopatření, neboť mohou snížit úroveň hrozeb ale i zranitelnosti.
- Pravděpodobnost jevu – v situacích, kdy nevíme, zda jev skutečně nastane, tak k popisu určitého jevu doplňujeme údaj s pravděpodobností, jakou může nastat. V prvé řadě je nutné definovat, zda je analyzovaný jev náhodný či nikoliv. Poté je možné daný jev vyloučit nebo zařadit do určitého intervalu pravděpodobnosti. Další vyskytující situací může být to, že daný jev bude podmíněn výskytem jevu jiného. Toto označujeme jako podmíněnou pravděpodobnost nebo závislý jev.
- Měření rizika – velikost rizika vyplývá z hodnoty aktiva, úrovně hrozby a zranitelnosti. Měření rizika není snadný úkol, protože riziko bývá často vyjádřeno veličinou, která není měřitelná. Měření bývá často hodnoceno specialistou na základě jeho zkušenosti. Často narazíme na pojmy vágní, malé, střední, vysoké riziko. Při měření rizika je nutné počítat s pravděpodobností výskytu jevu, kdy pravděpodobnější výskyt dostává vyšší hodnotu rizika.

4 CERTIFKACE A NORMY V OBLASTI BEZPEČNOSTI INFORMAČNÍCH TECHNOLOGIÍ

Certifikace a normy vznikají z důvodu neustále se opakujících procesů, které musí být beze změn. Pokud chceme v naší společnosti zavést určitý proces, bude zapotřebí norem a certifikací. Technická norma je dokument, který poskytuje uživateli pravidla, návody nebo definice pro určitý výrobek nebo postup. [8]Certifikace je akt, na základě kterého akreditovaný certifikační orgán potvrzuje, že daný systém, výrobek je ve shodě s požadavky příslušného normativního dokumentu. Dokladem o shodě je certifikát vydaný organizací certifikačním orgánem.

Tvorbou norem se zabývá velké množství organizací, které mohou mít úroveň působnosti národní nebo mezinárodní. Některé vybrané normy bývají přebírány českými úřady a můžeme se s nimi setkat i v české legislativě. Nejznámější normy z českého prostředí jsou: [9]

- IEC normy – tyto normy vydává instituce nazývaná International Electrotechnical Commision.
- ISO normy – tyto normy vydává instituce nazývaná Internation Organisation for Standardisation.
- IAB a IESG – tyto normy vydává instituce nazývaná Internet Architecture Board, Internet Engineering Steering Group

4.1 Legislativa v České republice

V legislativě České republiky je možné zmínit zákon o ochraně osobních údajů, který je neméně důležitý pro bezpečnosti informací.

V souvislosti s rokem 2017 vstoupily v účinnost dva zákony týkající se kybernetické bezpečnosti a informačních systémů veřejné správy.

4.1.1 Zákon č. 101/2000 Sb. o ochraně osobních údajů

Zákon se soustředí především na zpracování osobních údajů, citlivých údajů, práva a povinnosti subjektů zpracovávajících informace. Další pozornost je věnována Úřadu pro ochranu osobních údajů, kontrolní činnosti a problematice předávání osobních údajů do zahraničí. [10]

4.1.2 Zákon č. 104/2017 Sb. Novela o informačních systémech

Popisuje změny účinné od 1. 7. 2017, náhradou zákona 181/2014 Sb., kterým se mění zákon o informačních systémech veřejné správy, zákon o kybernetické bezpečnosti. Zákon č. 104/2017 Sb. přináší v rámci novely zákona o kybernetické bezpečnosti několik změn : [11]

- Nově je upravena definice provozovatele informačních a komunikačních systémů.
- Nově vytvořená kategorie povinného subjektu, kterým se stává provozovatel.
- Možnost hlášení bezpečnostního incidentu i provozovateli. Klasicky je incident hlášen správci.
- Povinnost provozovatele předat správci data, provozní údaje v případě hrozícího kybernetického incidentu.
- Zavedení pokut za porušení povinností provozovatele.

4.1.3 Zákon č. 205/2017 Sb. Novela zákona o kybernetické bezpečnosti

Novela 205/1017 přináší několik změn spojených především s implementací směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatření k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Evropské unii. Jedná se o směrnici NIS. Nejdůležitějšími změnami jsou: [12]

- Zavedení nových institutů, kterými jsou základní služby a digitální služby.
- Zavedení nových povinných orgánů a osob:
    - správce a provozovatel informačního systému základní služby.
    - Provozovatel základní služby
    - Poskytovatel digitální služby
- Systém zajištění kybernetické bezpečnosti – při výběru dodavatele služby, tedy správce a provozovatele informačních systémů základní služby musí být zohledněny požadavky vyplývající z bezpečnostních opatření. Změna spočívá v tom, že musí být zmíněné požadavky uvedeny ve smlouvě. Subjekty mají dále povinnost hlásit kybernetické bezpečnostní incidenty Úřadu, vládnímu CERT.

4.2 Normy z řady 27000

Vydávání norem má v České republice v působnosti Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Označení norem začíná zkratkou ČSN (československá

norma). V případě, že by byla norma převzata od některé z národních organizací, zůstává v názvu normy i název mezinárodní organizace. Zachovává se původní číslování.

ČSN ISO/IEC 27000:2014 / Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Norma položila základ pro zavedení managementu bezpečnosti informačních systémů. V platnost byla uvedena v roce 1995. Původně byla určena pro Britský normalizační institut. Postupně se začala uplatňovat i jiných zemí s označením ISMS. Norma se snaží komplexně řešit obranu proti možným hrozbám. Jedná se o hrozby, které byly v organizaci identifikované, oceněné a můžou mít rozsáhlé dopady. V roce 2000 byla norma přijatá jako standard ISO pod označením ISO 17799. V roce 2005 vydala mezinárodní organizace pro normalizaci sérii norem ISO/IEC 27000. Tato série norem zahrnuje i systém řízení informační bezpečnosti. Souhrn norem ISO/IEC se skládá z následujících částí: [2] [13]

ČSN ISO/IEC 27001:2014 / Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

Norma specifikuje požadavky na ustanovení, implementování, udržování a neustálé zlepšování ISMS. Součástí normy jsou i požadavky na posouzení a ošetření rizik bezpečnosti informací, které jsou přizpůsobené potřebám organizace. Norma prosazuje přijetí procesního přístupu k řešení ISMS a zavádí Demingův model PDCA. Neméně podstatná je příloha A této normy. Příloha obsahuje soupis cílů a jednotlivých opatření, které jsou propojeny s opatřeními v normě ISO/IEC 27002:2014. Druhá z příloh B uvádí vztah mezi principy OECD a fázemi Demingova modelu. Požadavky této normy je možné aplikovat ve všech organizacích bez ohledu na jejich typ, velikost a povahu. [14]

ČSN ISO/IEC 27002:2014 / Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

Norma je určena pro organizace jako doporučení pro výběr opatření v rámci ISMS. Jde o soubor postupů pro řízení bezpečnosti informací. Předchůdcem této normy byla ISO/IEC 17799:2005. Součástí je detailní rozbor vhodných opatření. Tato norma je také určena pro použití při vyvíjení směrnic pro řízení bezpečnosti informací se zaměřením na průmysl či

organizace. Norma přihlíží na konkrétní prostředí rizik pro bezpečnost informací. Bezpečnostní opatření podporující dosahování cílů, kdy odpovědnost za ně je možné přiřadit odpovědným osobám dle jejich funkcí. [15]

ČSN ISO/IEC 27003:2011 / Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací

Norma zprostředkovává doporučení pro ustanoven a implementaci ISMS v souladu s požadavky normy ISO/IEC 27000. Normu je možné použít pro všechny typy organizací. Obsahem normy je vysvětlení návrhu a implementace ISMS za pomocí popisu zahájení, definování a plánování projektu implementace ISMS. Norma obsahuje popis implementace ISMS v pěti krocích:

1. Souhlas vedení organizace se zahájením ISMS.
2. Definice rozsahu, hranic a politik ISMS.
3. Analýza požadavků bezpečnosti informací.
4. Provedení hodnocení rizik a plánování zvládání rizik.
5. Návrh ISMS.

V příloze této normy jsou uvedeny kontrolní seznamy činností potřebných k ustanovení a implementaci ISMS. Dále jsou popsány role a odpovědnosti bezpečnosti informací. Informace o postupu interního auditu, struktury politik a informace o monitorování a měření bezpečnosti informací. [16]

ČSN ISO/IEC 27004:2011/ Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření

Norma poskytuje doporučení pro vývoj a používání metrik, měření účinnosti zavedeného ISMS. Dále se norma zaměřuje na účinnost opatření nebo skupin opatření, jež se uvádí v ISO/IEC 27001. Měření bezpečnosti informací obsahuje procesy rozvoje metrik a měření, provádění měření, analýzy dat a hlášení výsledků měření. Dalšími kroky jsou proces vyhodnocení a zlepšování programu měření bezpečnosti informací. V příloze této normy jsou uvedeny koncepty měření pro určitá opatření nebo procesy ISMS. [17]

ČSN ISO/IEC 27005:2013 / Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

Norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace. V normě nejsou uvedeny přesné metodologie, jak přistupovat k řízení rizik nad bezpečností informací. Norma je určená manažerům a specialistům, kteří mají v rámci organizace odpovědnost za řízení rizik bezpečnosti informací. Aplikovatelnost normy je možná na všechny typy organizací. [18]

4.3 Bezpečnost zdravotnického prostředí

Bezpečností prostředí zdravotnictví se zabývá norma ISO/IEC 27799:2016 Zdravotnická informatika. Norma definuje soubor detailních kontrol, které se zabývají řízením bezpečnosti zdravotnických informací. Zavedením Této normy budou zdravotnické organizace schopny zajistit minimální úroveň zabezpečení. Zavedené zabezpečení by mělo odpovídat poměrům v organizaci, zachovat důvěrnost, integritu a dostupnost osobních zdravotnických informací. Zdravotnická norma se vztahuje na informace všech aspektů bez ohledu na jejich formu. Vztahuje se jak na slovní, písemnou formu informací ale i zvukové nahrávky, kresby, video. Prostředky k ukládání zmíněných informací mohou být papírové i elektronické. Zmíněny jsou i prostředky přenosu informací a to ruční, fax, počítačová síť, elektronická pošta. Nutností je ochrana přenášených informací.

Normy ISO/IEC 27002 a ISO/IEC 27799 společně určují požadavky bezpečnosti informací ve zdravotnictví. Normy ale nezmiňují, jakým způsobem by měly být požadavky na bezpečnost splněny. Normy tedy působí neutrálně ve vztahu k bezpečnosti informací ve zdravotnictví. Vzhledem k tomu, že normy by měly zůstat v platnost po dobu několika let a tempo vývoje nových technologií je velice rychlé, neutralita přichází vhod. [5]

5 CÍL PRÁCE A POUŽITÉ METODY

Cílem této práce jsou analýza současného stavu bezpečnosti informací v lékařském subjektu a návrh bezpečnostní politiky za využití ISO/IEC 27000:2014. Tato práce se soustředí na fyzioterapeutickou ordinaci, jejímž cílem je zavedení bezpečnostní politiky v rámci interního systému. Měla by navrhnout takovou politiku, která je vhodná pro lékařský subjekt. Tedy aby vyhovovala majiteli a byla finančně snesitelná. Hlavní cíl práce je tvořen následujícími dílčími cíli:

- Posouzení současného stavu bezpečnosti ve fyzioterapeutické ordinaci.
- Analýza rizik v prostředí fyzioterapeutické ordinace.
- Návrh opatření vycházející z ISO/IEC 27002:2014.

Při zpracování této práce bude čerpáno jednak z dostupných literárních zdrojů a dále z osobních zkušeností získaných při zaměstnání v oddělení informačních technologií. Teoretická část bude zpracována především metodou sběru dat a informací získaných konzultací se zadavatelem práce. Praktická část využije metody analýzy rizik. Na základě této analýzy budou navržena opatření vycházející z ISO/IEC 27002:2014, která vytvoří základ pro vypracování bakalářské práce.

II. PRAKTICKÁ ČÁST

6 SOUČASNÝ STAV BEZPEČNOSTI V ZAŘÍZENÍ

V praktické části této bakalářské práce bude popsán lékařský subjekt a také bude vypracována analýza současného stavu bezpečnosti. Na základě analýzy rizik budou navržena opatření zahrnující síťovou infrastrukturu a také opatření vycházející ze směrnice ČSN ISO/IEC 27001:2014, jež budou mít za cíl zlepšit zabezpečení informací.

6.1 Základní popis zdravotnického zařízení

Jedná se o nestátní zdravotnické zařízení založené v roce 1997. Zařízení nabízí služby v oboru rehabilitace a fyzikální terapie. V současné době jsou ve společnosti zaměstnáni tři fyzioterapeuti a jeden lékař. Společnost má v plánu do dvou let zaměstnat další 2 fyzioterapeuty.

6.2 Popis budovy

Jedná se o dvoupodlažní dům, který postupně prochází rekonstrukcí. Před otevřením ordinace se vlastník nemovitosti rozhodl částečně zrekonstruovat první podlaží tak, aby ordinace mohla fungovat co nejdříve. Další rekonstrukce budou následovat během roku. Provizorní ordinace je realizována v přízemí. První místností při vstupu do budovy je čekárna. Následuje recepce, která propojuje chodbou fyzioterapeutické místnosti a tělocvičnu. První patro slouží jako ubytovací zařízení pro vlastníka společnosti.

6.3 Infrastruktura

Strukturovaná kabeláž je vedena žlabem z prvního patra přes venkovní stranu budovy do přízemí. V přízemí budovy není kabel umístěn do žlabů. Je veden pod kobercem přímo do routeru, který je umístěn v recepci. Jedná se o jednoduchou intranetovou síť se čtyřmi PC, přičemž jeden z nich je nastaven jako server. Konektivita směrem k internetu je řešena pomocí ADSL s přenosovými rychlostmi 50/5 MBit. Jedná se o bezdrátové připojení s průměrnými přenosovými vlastnostmi.

Budova ordinace leží v blízkosti místního sídliště. Okolí budovy není zabezpečeno bezpečnostním oplocením. Objekt lze popsat z hlediska přístupových cest. Prvním možným vstupem je vchod do recepce, druhý vstup je umístěn v zadní části budovy. Třetí vstup je určen pro přístup do prvního patra. Na budově jsou instalovány venkovní bezpeč-

nostní rolety. Uvnitř budovy je umístěno signalizační zařízení, jehož úkolem je zjistit a signalizovat jakýkoliv pokus o vniknutí nepovolené osobě do objektu.

V objektu jsou používány čtyři notebooky, přičemž dva z nich běží pod operačním systémem (dále jen „OS“) Windows sedm. Třetí zařízení má nainstalován OS Windows osm a poslední zařízení je provozováno pod již nepodporovanými Windows XP.

Hlavní software, který ordinace používá, je program Wintropos. Jedná se o zdravotnický software, který primárně slouží k pořizování dávek dokladů předkládaných zdravotním pojišťovnám. Úlohou programu je vyúčtování práce zdravotnických subjektů. Další funkcionalitou zdravotnického softwaru je vedení kartotéky pacientů, tisk receptů a dalších dokumentů. Neméně podstatnou funkcí jsou přehledné statistiky s filtry. Program je možné nastavit do dvou rolí. První rolí je lékař, druhá role je určena pro sestru, která má omezený přístup k citlivým datům pacientů. Program umožňuje pravidelné zálohování dat. Pro práci s aktuálními daty je nastavena sdílená kartotéka „Data“, která obsahuje všechny informace. Ostatní počítače jsou připojeny k počítači, v němž je umístěna kartotéka.

6.4 Personální bezpečnost

Noví zaměstnanci jsou vybíráni standardním tří-kolovým přijímacím řízení. Přístup k zdravotnickému systému je umožněn až po podepsání pracovní smlouvy a seznámení se s ním. Práce se zdravotnickým systém je intuitivní a nevyžaduje žádné speciální školení. Po všech zaměstnancích je při opuštění PC vyžadováno zamykání účtu, čímž je zabráněno přístupu neoprávněným osobám.

6.5 Zhodnocení aktiv

Dle směrnice ISO 27001 je možné cíle informační bezpečnosti rozdělit na:

- Důvěrnost – zajištění, že informace jsou přístupně sděleny pouze uživatelům, kteří mají oprávnění.
- Dostupnost – zajištění, že informace jsou přístupné v okamžiku, kdy jsou potřebné oprávněnému uživateli.
- Integritu – zajištění správnosti a úplnosti informací.
- Výsledek – udává hodnotu aritmetického průměru hodnot důvěrnosti, dostupnosti a integrity, viz následující vzorec.

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

x_i = hodnota

n = počet hodnot

Identifikace aktiv bude nejdříve rozdělena do jednotlivých kategorií:

Hardware (dále jen „HW“) – Jedná se o veškeré fyzicky existující zařízení. V případě ordinace můžeme mezi aktiva zařadit síťové prvky, pracovní notebooky, routery a tiskárny.

Software (dále jen „SW“) – Softwarem označujeme veškeré programové zařízení. Pro případ ordinace hraje roli operační systém a zdravotnický systém.

Data – Podstatnou důležitost mají v ordinaci citlivé informace pacientů a lékařské zprávy. Tyto informace jsou částečně uchovávané v tištěné a digitální podobě.

Služby – Z pohledu aktiv je možné do služeb zařadit telefonní linku, připojení internetu, zdroj energie.

Tab. 2: Ohodnocení aktiv, Zdroj: [vlastní]

Typ	Aktivum	Důvěrnost	Dostupnost	Integrita	Výsledek
HW	Síťové prvky + kabeláž	5	5	5	5
	Notebooky	3	2	3	3
	Routery	5	4	4	4
	Síťová tiskárna	2	3	2	2
SW	Zdravotnický systém	4	3	4	4
Data	Databáze ZS	5	5	5	5
	Interní informace	3	4	3	3
	Lékařské zprávy	5	5	5	5
	Smlouvy	5	5	5	5
	www stránky organizace	4	4	4	4
Služby	Telefonní linka	3	2	2	2
	Připojení k internetu	5	4	5	5
	Zdroj elektrické energie	2	1	3	2

Výše uvedená aktiva organizace byla ohodnocena a byla u nich určena velikost dopadů na základě ohrožení důvěrnosti, dostupnosti nebo integrity. Velikost dopadů byla určena při konzultaci s vlastníkem organizace, který zmíněná aktiva spravuje.

6.6 Identifikace hrozeb

Dle ISO 27005 jsou v tabulce níže identifikovány hrozby a pravděpodobnosti výskytu hrozeb. Značení je ve formě stupnice „žádná“ – 0, „nízká“ – 1, „střední“ – 2, „vysoká“ – 3. Po konzultaci s vlastníkem ordinace byly vybrány nejdůležitější hrozby, které by mohly ovlivnit chod ordinace.

Tab. 3: Identifikace hrozeb, Zdroj: [vlastní]

Zkratka	Uvolnit popisky / Název	Hodnota	Poznámka
HROZBY - CELKEM		3	
FYZP	Fyzické poškození	2	
POZA	Požár	1	
POSV	Poškození Vodou	1	
ZNEC	Znečištění	2	
PRKZ	Prach, koroze, zamrznutí	2	
ZNZM	Zničení zařízení nebo médií	2	
ZTRS	Ztráta služeb	3	
PRDE	Přerušení dodávky elektřiny	2	
VYIP	Výpadek internetového připojení	2	
VYSW	Výpadek SW Wintropos	3	
OHRI	Ohrožení informací	3	
NEZI	Neoprávněné získání informací	3	
KRAZ	Krádež zařízení	3	
KRAM	Krádež médií nebo dokumentů	3	
NEOC	Neoprávněné činnosti	3	
NEOPZ	Neoprávněné použití zařízení	3	
ZNPP	Zneužití přístupových práv	2	
PODA	Poškození dat	3	
NEPB	Neoprávněný přístup do budovy	3	
LISE	Lidská selhání	2	
CHPO	Chyba použití	2	
NEDO	Nedostatečná dokumentace	1	
CHUD	Chyba údržby	2	

6.7 Analýza zranitelnosti

Tento bod popisuje tabulku, která porovnává závažnosti hrozeb a hodnoty aktiv. Každému aktivu se stanoví hodnota zranitelnosti při výskytu dané hrozby. Hodnoty jsou definovány stupnicí s hodnotami „žádná“ – 0, „nízká“ – 1, „střední“ – 2, „vysoká“ – 3.

Tab. 4: Matice zranitelnosti, Zdroj: [vlastní]

RISKAN RIZIKOVÝ KALKULÁTOR T-SOFT	Aktiva	AKTIVA - CELKEM	Hardware	Síťové prvky + kabeláž	Notebooky	Routery	Síťová tiskárna	Software	Zdravotnický systém	Data	Databáze ZS	Interní informace	Lékařské zprávy	www stránky organizace	Služby	Smlouvy	Telefonní linka	Připojení k internetu	Zdroj elektrické energie
			HW	SITP	NTBK	RTR	SITT	SW	ZDRS	DATA	DBS	INTI	LEKZ	WWW	SLUŽ	SMLO	TELL	PŘPI	ZDEE
	Hodnoty aktiv	5	5	5	3	4	2	4	4	5	5	3	5	4	5	5	2	5	2
		velmi vysoká	velmi vysoká	velmi vysoká	střední	vysoká	nízká	vysoká	vysoká	velmi vysoká	velmi vysoká	střední	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	nízká	velmi vysoká	nízká
Hrozby	Pravděpodobnost																		
HROZBY - CELKEM	3 Vysoká	3	3	3	3	3	3	3	3	3	3	3	3	1	2	2	1	2	2
FYZP Fyzické poškození	2 Střední	3	3	2	3	3	2	0	0	3	1	0	3	0	2	2	1	2	2
POZA Požár	1 Nízká	3	2	2	2	2	1	0	0	3	1	0	3	0	2	2	1	1	2
POSV Poškození Vodou	1 Nízká	3	1	1	1	1	1	0	0	3	1	0	3	0	2	1	1	1	2
ZNEC Znečištění	2 Střední	2	2	2	2	1	1	0	0	1	0	0	1	0	2	2	0	0	0
PRKZ Prach, koroze, zamrznutí	2 Střední	2	2	2	2	2	2	0	0	0	0	0	0	0	2	0	1	2	2
ZNZM Zničení zařízení nebo médií	2 Střední	3	3	2	3	3	2	0	0	2	0	0	2	0	0	0	0	0	0
ZTRS Ztráta služeb	3 Vysoká	3	3	0	3	3	3	3	3	0	0	0	0	0	0	0	0	0	0
PRDE Přerušení dodávky elektřiny	2 Střední	3	3	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0
VYIP Výpadek internetového připojení	2 Střední	3	0	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0
VYSW Výpadek SW Wintropos	3 Vysoká	3	0	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0
OHRI Ohrožení informací	3 Vysoká	3	3	3	3	2	0	3	3	3	3	3	3	1	2	2	0	0	0
NEZI Neoprávněné získání informací	3 Vysoká	3	0	0	0	0	0	3	3	3	3	1	3	1	2	2	0	0	0
KRAZ Krádež zařízení	3 Vysoká	3	3	3	3	2	0	3	3	3	3	2	3	1	1	1	0	0	0
KRAM Krádež médií nebo dokumentů	3 Vysoká	3	3	0	3	2	0	3	3	3	3	3	3	1	0	0	0	0	0
NEOC Neoprávněné činnosti	3 Vysoká	3	3	0	3	3	0	3	3	3	3	3	3	0	0	0	0	0	0
NEOPZ Neoprávněné použití zařízení	3 Vysoká	3	3	0	3	3	0	3	3	3	3	2	2	0	0	0	0	0	0
ZNPP Zneužití přístupových práv	2 Střední	3	3	0	3	3	0	1	1	3	3	1	1	0	0	0	0	0	0
PODA Poškození dat	3 Vysoká	3	3	0	3	2	0	3	3	3	3	3	3	0	0	0	0	0	0
NEPB Neoprávněný přístup do budovy	3 Vysoká	3	3	0	3	3	0	1	1	2	2	1	1	0	0	0	0	0	0
LISE Lidská selhání	2 Střední	3	3	0	3	2	1	3	3	3	3	1	1	1	0	0	0	0	0
CHPO Chyba použití	2 Střední	3	3	0	3	2	0	3	3	3	3	1	1	1	0	0	0	0	0
NEDO Nedostatečná dokumentace	1 Nízká	2	1	0	1	1	1	1	1	2	2	1	1	1	0	0	0	0	0
CHUD Chyba údržby	2 Střední	3	3	0	3	2	0	1	1	3	3	1	1	0	0	0	0	0	0

6.8 Analýza rizik

Vypracovaná matice se dále použije pro výpočet míry rizika. Pro tento výpočet rizika se používá vztah:

$$R = T * A * V.$$

kde:

R = míra rizika.

T = pravděpodobnost hrozby.

A = hodnota aktiva.

V = zranitelnost aktiva.

Pro výpočet analýzy rizik byl použit program Riskan, který urychlí proces analýzy. Jedná se o nástroj vyhledávající priority, jež jsou potřebné k získání rizikových výpočtů. Výstupem programu Riskan je jasný výsledek a dopady rozhodnutí pro následující návrh opatření.

Tab. 5: Matice rizik, Zdroj: [vlastní]

Riskan RIZIKOVÝ KALKULÁTOR T-SOFT		Aktiva	AKTIVA - CELKEM	Hardware	Síťové prvky + kabeláž	Notebooky	Routery	Síťová tiskárna	Software	Zdravotnický systém	Data	Databáze ZS	Interní informace	Lékařské zprávy	www stránky organizace	Služby	Smlouvy	Telefonní linka	Připojení k internetu	Zdroj elektrické energie
			HW	SITP	NTBK	RTR	SITT	SW	ZDRS	DATA	DBS	INTI	LEKZ	WWW	SLUŽ	SMLO	TELL	PŘPI	ZDEE	
		Hodnoty aktiv	5	5	5	3	4	2	4	4	5	5	3	5	4	5	5	2	5	2
			velmi vysoká	velmi vysoká	velmi vysoká	střední	vysoká	nízká	vysoká	vysoká	velmi vysoká	velmi vysoká	střední	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	nízká	velmi vysoká	nízká
Hrozby		Pravděpodobnost																		
HROZBY - CELKEM		3 Vysoká	45	45	45	27	36	12	36	36	45	45	27	45	12	30	30	4	20	8
FYZP	Fyzické poškození	2 Střední	24	24	20	18	24	8	0	0	20	5	0	20	0	20	20	4	20	8
POZA	Požár	1 Nízká	15	10	10	6	8	2	0	0	15	5	0	15	0	10	10	2	5	4
POSV	Poškození Vodou	1 Nízká	15	5	5	3	4	2	0	0	15	5	0	15	0	5	5	2	5	4
ZNEC	Znečištění	2 Střední	20	20	20	12	8	4	0	0	10	0	0	10	0	20	20	0	0	0
PRKZ	Prach, koroze, zamrznutí	2 Střední	20	20	20	12	16	8	0	0	0	0	0	0	0	20	0	4	20	8
ZNZM	Zničení zařízení nebo médií	2 Střední	24	24	20	18	24	8	0	0	20	0	0	20	0	0	0	0	0	0
ZTRS	Ztráta služeb	3 Vysoká	36	24	0	18	24	12	36	36	0	0	0	0	0	0	0	0	0	0
PRDE	Přerušení dodávky elektřiny	2 Střední	24	24	0	18	24	12	0	0	0	0	0	0	0	0	0	0	0	0
VYIP	Výpadek internetového připojení	2 Střední	24	0	0	0	0	0	24	24	0	0	0	0	0	0	0	0	0	0
VYSW	Výpadek SW Wintropos	3 Vysoká	36	0	0	0	0	0	36	36	0	0	0	0	0	0	0	0	0	0
OHRI	Ohrožení informací	3 Vysoká	45	45	45	27	24	0	36	36	45	45	27	45	12	30	30	0	0	0
NEZI	Neoprávněné získání informací	3 Vysoká	45	0	0	0	0	0	36	36	45	45	9	45	12	30	30	0	0	0
KRAZ	Krádež zařízení	3 Vysoká	45	45	45	27	24	0	36	36	45	45	18	45	12	15	15	0	0	0
KRAM	Krádež médií nebo dokumentů	3 Vysoká	45	27	0	27	24	0	36	36	45	45	27	45	12	0	0	0	0	0
NEOC	Neoprávněné činnosti	3 Vysoká	45	36	0	27	36	0	36	36	45	45	27	45	0	0	0	0	0	0
NEOPZ	Neoprávněné použití zařízení	3 Vysoká	45	36	0	27	36	0	36	36	45	45	18	30	0	0	0	0	0	0
ZNPP	Zneužití přístupových práv	2 Střední	30	24	0	18	24	0	8	8	30	30	6	10	0	0	0	0	0	0
PODA	Poškození dat	3 Vysoká	45	27	0	27	24	0	36	36	45	45	27	45	0	0	0	0	0	0
NEPB	Neoprávněný přístup do budovy	3 Vysoká	36	36	0	27	36	0	12	12	30	30	9	15	0	0	0	0	0	0
LISE	Lidská selhání	2 Střední	30	18	0	18	16	2	24	24	30	30	6	10	8	0	0	0	0	0
CHPO	Chyba použití	2 Střední	30	18	0	18	16	0	24	24	30	30	6	10	8	0	0	0	0	0
NEDO	Nedostatečná dokumentace	1 Nízká	10	4	0	3	4	2	4	4	10	10	3	5	4	0	0	0	0	0
CHUD	Chyba údržby	2 Střední	30	18	0	18	16	0	8	8	30	30	6	10	0	0	0	0	0	0

Jednotlivé úrovně byly následně klasifikovány do tří skupin. Podle toho, do které skupiny jsou daná rizika zařazena, budou k daným rizikům navrhnuta opatření. Pro klasifikaci rizik jsou nastaveny tři úrovně.

Tab. 6: Klasifikace rizik, Zdroj: [vlastní]

Hodnota rizika	Klasifikace rizika
0 až 15	Nízké
15 až 30	Střední
30 až 45	Vysoké

6.9 Zhodnocení analýzy rizik

Bylo identifikováno 18 rizik s vysokou úrovní rizika. Jedná se převážně o oblasti ohrožení informací, neoprávněná činnost a ztráta služeb. Proto bude v návrhu opatření vycházejícího z normy ISO/IEC 270001 přistoupeno zejména k těmto skupinám hrozeb. V rámci nastavení bezpečnostních opatření bude navržena počítačová síť, která by měla část hrozeb pokrýt.

Po dohodě s majitelem organizace byla sestavena tabulka s navrženými opatřeními. Všechna uvedená opatření byla akceptována ze strany vlastníka ordinace. V další části této práce budou navržena opatření, která eliminují analyzovaná rizika.

Tab. 7: Seznam navržených opatření, Zdroj: [vlastní]

Hrozba	Přijaté opatření
Fyzické poškození	
Požár	
Poškození vodou	
Znečištění	
Prach, koroze, zamrznutí	
Zničení zařízení nebo médií	
Ztráta služeb	
Přerušení dodávky elektřiny	
Výpadek internetového připojení	
Výpadek SW Wintropos	A.11.2.2
Ohrožení informací	
Neoprávněné získání informací	A.9.1.1
Krádež zařízení	A.6.1.1, A.11.1.1, A.11.1.3,A.11.2.1, A.11.2.3
Krádež médií nebo dokumentů	A.9.1.1, A.9.1.2, A.9.2.2, A.9.4.1, A.11.2.3, A.11.2.6, A.12.2.1, A.13.1.2
Neoprávněné činnosti	

Neoprávněné použití zařízení	A.9.1.2, A.9.4.1, A.9.4.2, A.11.1.1, A.11.1.2, A.11.1.3, A.11.2.1, A.11.2.6, A.11.2.8, A.12.2.1, A.13.1.2
Zneužití přístupových práv	A.7.2.3, A.9.1.1, A.9.2.2, A.9.2.3, A.9.4.1, A.9.4.3,
Poškození dat	A.9.1.2, A.9.4.1, A.12.2.1 A.11.2.8, A.12.3.1, A.12.6.2, A.14.1.3
Neoprávněný přístup do budovy	A.11.1.1, A.11.1.2
Lidské selhání	
Chyba použití	
Nedostatečná dokumentace	
Chyba údržby	

7 NÁVRH SÍŤOVÉ INFRASTRUKTURY

Tato kapitola se zabývá návrhem počítačové sítě organizace tak, aby splňovala bezpečnostní podmínky ISMS. Návrh zahrnuje výběr adekvátních síťových prvků a kabeláže. Důležitým úkolem je zajištění dostupnosti a kompatibility prvků.

7.1 Návrh sítě a uzlových bodů

Navrhnutá síť by měla splňovat několik zásadních požadavků zadavatele. Řešení by nemělo být zbytečně nákladné a nemělo by nijak finančně ohrozit chod ordinace. Přitom důraz by měl být kladen také na bezpečnost. Řešení návrhu sítě by mělo zabezpečit citlivá data, jako jsou rodná čísla či lékařské zprávy. Řešení by mělo být navrženo tak, aby v případě budoucích problémů neměl žádný IT pracovník problém se seznámením se se sítí a následnou opravou.

7.1.1 Pasivní vrstva

Mezi pasivní prvky lze zařadit kabeláž, která umožňuje fyzický přenos dat do PC.

Kabeláž

Kvůli vyšší stabilitě a rychlosti datových přenosů budou také použity síťové kabely vedeny z routeru do switche. Zvolen byl síťový kabel Datacom CAT6 UTP. Jedná se o kvalitní patch kabel UTP se čtyřmi páry a dvěma konektory RJ-45. Rychlost přenosu dat je až 1000 Mbit/s.

Vedení kabeláže venkovní částí budovy bude chráněno v kovových lištách. Zabrání se tím mechanickému poškození kabeláže zvenčí. Uvnitř budovy bude kabeláž vedena po stropní části v plastových lištách.

7.1.2 Výběr aktivních prvků

Výběr správných aktivních prvků pro ordinaci je velmi důležitý. Aktivní prvky budou vybírány se zaměřením na bezpečnost, kvalitu a efektivnost.

Přístupový bod

Přístupový bod musí splňovat možnost duálního vysílání. Z pohledu bezpečnosti je vyžadováno oddělení bezdrátového přenosu pro zaměstnance a pro pacienty. Zvoleno bylo zařízení ASUS RT-AC68U, na kterém může běžet VPN server a firewall. VPN server zajistí

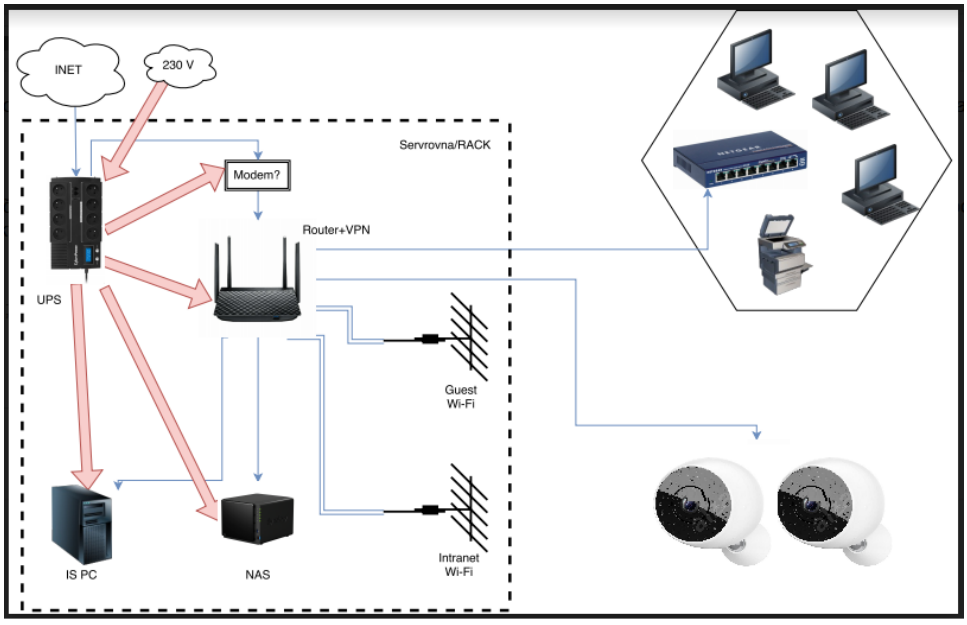
bezpečný vzdálený přístup. Po připojení bude moci uživatel přistupovat k datům přesně tak, jako by byl v kanceláři. Firewall bude zabezpečovat síť od vnějších útoků.

NAS

Uložiště dat by mělo splňovat několik základních podmínek. V případě citlivých lékařských dat je nutné dbát na jejich správnost a nemožnost ztráty dat. Pro potřeby ordinace se jeví jako ideální řešení NAS serveru o 4 discích splňující podmínku RAID 6. V tomto případě může dojít k výpadku až dvou disků. Možností je nastavení automatického šifrování dat, které je v plnění podmínek ISMS nutností. Zvoleno bylo zařízení Synology DS418play. Zařízení splňuje všechny podmínky. Dále nabízí kapacitu až 40 TB, což je pro potřeby ordinace dostačující.

Rozvod sítě

Rozvod sítě bude zajištěn pomocí kombinace Wi-fi a GLAN. Kabelové připojení bude sloužit jako primární. Pro účely kabelového připojení byl vybrán switch Netgear GS108GE, který je typický spolehlivostí a vysokou rychlostí připojení. Zajímavou funkcí je automatické vypnutí portů v případě, že nejsou využívány.



Obr. 6: Návrh počítačové sítě, Zdroj: [vlastní]

7.2 Návrh kritické části ISMS

Na základě analýzy rizik, která byla vypracována v předchozí části a po dohodě s vlastníkem ordinace byla vypracována tabulka s opatřeními. Seznam s opatřeními vychází z pří-

lohy A normy ISO/IEC 27001:2014. Níže vytvořená tabulka zahrnuje opatření z normy ISO/IEC 270002:2014. Všechna opatření budou nově zavedena případně revidována na základě informací z předešlé analýzy rizik.

7.2.1 Politiky bezpečnosti informací

Z důvodu, že se organizace dříve nezabývala bezpečnosti informací, je nezbytné, aby vlastník ordinace vyjádřil podporu. Podporu by měl vlastník vyjádřit dřív, než bude některé z opatření již zavedeno. Neméně důležité je stanovení odpovědné osoby, která bude zodpovědná za implementaci ISMS.

Politiky pro bezpečnost informací

Opatřením této části normy je vytvoření bezpečnostní politiky, která je v případě této organizace schválena majitelem. S bezpečnostní politikou jsou následně seznámeni všichni fyzioterapeuti, sestry a lékař. Povinností je podpis, který potvrzuje seznámení se s bezpečnostní politikou.

7.2.2 Organizace bezpečnosti informací

Úkolem této části je vytvoření řídicího rámce, který zodpovídá za zahájení a udržování bezpečnosti informací v ordinaci. Sekundárním úkolem řídícího rámce je zajištění bezpečnosti dat při jejich využívání na mobilních zařízeních. Neméně podstatná je bezpečnost při práci na dálku.

Aplikace níže uvedených opatření povede ke snížení hrozeb jako je krádež zařízení a neoprávněné získání informací.

Role a odpovědnost bezpečnosti informací

Cílem tohoto opatření je nastavení bezpečnosti aktiv. Každý zaměstnanec zodpovídá za bezpečnost aktiva, které používá. Zaměstnanci by měli být jednou ročně proškoleni z oblasti bezpečnosti informací. Pro tyto účely budou využity služby společnosti Eset, která nabízí bezpečnostní školení upravené na míru.

Práce na dálku

V případě potřeby práce na dálku je doporučeno použití předem zvoleného firemního zařízení. Vzdálené přihlášení bude probíhat přes VPN za použití dvou faktorové autentizace ESET Secure Authentication. Autentizace zahrnuje mobilní řešení, které používá dvou

faktorové řešení s ověřením s použití jednorázového náhodného hesla. Při přihlášení přijde na mobilní zařízení jednorázové heslo, které bude použito pro přihlášení. Použitím tohoto řešení se zvyšuje bezpečnost práce na dálku.

7.2.3 Bezpečnost lidských zdrojů

Bezpečnost lidských zdrojů se zabývá procesy jako prověřování příchozích zaměstnanců, ale také bezpečností informací během pracovního vztahu zaměstnanců.

Zavedením níže uvedeného opatření dojde ke snížení hrozby zneužití přístupových práv.

Disciplinární řízení

Disciplinární řízení bude vedeno se zaměstnanci, kteří nebudou dodržovat platné směrnice. Cílem opatření je motivace zaměstnanců nezneužívat přístupových práv. Nedodržováním směrnic se zaměstnanec dopouští přestupku, který bude řešen sankcí.

Sankci lze udělit zaměstnanci formou:

- Napomenutí – nejedná se o závažný přestupek.
- Udělení pokuty – uděluje se v případě, kdy ordinaci vznikne finanční ztráta.
- Ukončení pracovního poměru – předpokladem je vědomé spáchání přestupku nebo páchání přestupku opakovaně.

7.2.4 Řízení přístupu

Politika řízení přístupu se zabývá přidělováním a odebíráním uživatelských práv. Ve věci auditu ISMS je nutné zavést dokument s přidělenými a odebranými uživatelskými právy. Dokument je podepsán zodpovědnou osobou.

V případě zavedení níže uvedených opatření dojde k eliminaci níže uvedených hrozeb:

- Krádež médií nebo dokumentů.
- Neoprávněné použití zařízení.
- Zneužití přístupových práv.
- Poškození dat.

Politika řízení přístupu

Politika řízení přístupu má za cíl definovat role v rámci organizace. Definované role by měly odlišit přístup k informacím pro vlastníka, lékaře a fyzioterapeuta. Každý z nich bude mít zpřístupněny pouze ty informace, které potřebuje ke své práci.

Přístup k sítím a síťovým službám

Umístění serveru a PC s ordinačním softwarem je v oddělené místnosti, která je oddělena dveřmi se zámkem. Server je dále umístěn v RACK, který je chráněn heslem. Přístup má k dispozici pouze vlastník ordinace.

Registrace a zrušení registrace uživatele

Přihlašovací jméno a heslo vytvoří pověřený zaměstnanec ordinace. Společně s přístupovými právy se vytvoří nový uživatel. Dále je vytvořen účet s přístupem do programu Wintropos. Nově vytvoření uživatelé mají přidělena základní přístupová práva v závislosti na jejich pracovní náplni. V případě ukončení pracovního poměru zaměstnance je uživatelský účet zrušen.

Bezpečné postupy přihlášení

Pro bezpečné přihlášení k účtu do systému uživatel dostane jednorázové heslo, které je nutné po prvním přihlášení změnit. Samotné přihlášení do systému má svá pravidla.

- V přihlašovací části je zobrazeno minimum informací.
- Heslo ani počet znaků není zobrazeno.
- Nápověda není povolena.
- Pokud dojde k nezdařilé autentizace, nezobrazuje se chybná část hesla.
- Při překročení třech autentizačních pokusů je účet zablokován, vytvoří se bezpečnostní incident a informuje se odpovědná osoba.
- Není povoleno heslo posílat po síti v čitelném tvaru (nezabezpečeném).

Systém správy hesel

Systém správy hesel definuje postup při prvním přihlášení do systému a emailu. Při prvním přihlášení uživatel obdrží heslo, které musí být ihned změněno. Nové heslo nesmí být nikde zaznamenáno. Požadavky na vytvoření nového heslo jsou definovány níže:

- Délka hesla má minimálně 8 znaků.
- Heslo obsahuje číslici.
- Heslo obsahuje znak.

- Součástí hesla jsou velká a malá písmena.
- Heslo by nemělo být jméno, slovo.
- Nepoužívat stejná hesla pro více účtů.

Postup pro vytvoření silného hesla:

- Výběr vhodné pasáže z knihy nebo článku.
- Zkrácení pasáže na délku osmi znaků.
- Dosazení číslice, znaku a velkých písmen.
- Heslo nutné každé tři měsíce obměnit.

7.2.5 Fyzická bezpečnost a bezpečnost oblastí

Úkolem této části je zamezit neoprávněnému přístupu k datům. Dále je tato část zaměřena na ochranu proti poškození a narušování informací. Z pohledu zařízení je kladen důraz na jeho ochranu.

Navržená opatření mají za cíl eliminovat hrozby:

- Výpadek SW Wintropos.
- Krádež zařízení.
- Neoprávněné použití zařízení.
- Poškození dat.
- Neoprávněný přístup do budovy.

Fyzický a bezpečnostní perimetr

Pro nastavení fyzického a bezpečnostního perimetru bude po dohodě s vlastníkem střežení podniku použitím alarmu. Každý zaměstnanec dostane unikátní kód, kterým odkóduje alarm. Přístupy a odchody budou zaznamenávány pro případ potřeby. Vlastník ordinace dále souhlasí se zavedením kontroly oprávnění formou čipové karty. Implementovány bu-

dou bezpečnostní vstupní dveře a elektronicky stahovatelné žaluzie. Zaměstnanci budou moci vstoupit do předem nadefinovaných místností. Místnost se serverem nebude zpřístupněna žádnému zaměstnanci.

Další úrovní zabezpečení je instalace kamerového systému u vstupních dveří a v čekárně. Záznam z kamer bude ukládán po dobu dvou dnů, následně bude smazán.

Zabezpečení kanceláří, místností a vybavení

Kanceláře budou primárně zabezpečeny kontrolou oprávnění formou čipové karty. Sekundární zabezpečení bude nastaveno formou uzamykání místností po skončení pracovního dne. Při odchodu budou zaměstnanci povinni zkontrolovat všechny skříně, každá musí být uzamčena.

Notebooky budou uzamčeny pomocí ocelového lanka k pevně stojícímu nábytku. Zámek pro notebook disponuje rotačním kombinačním zámkem, který nabízí deset tisíc možných číselných variant.

Podpůrné služby

V rámci návrhu bezpečnosti sítě bylo doporučeno zařízení UPS, které při výpadku elektrické energie částečně zamezuje ztrátě rozpracovaných souborů.

Obr. 7: UPS - CyberPower [19]

UPS disponuje osmi výstupními zásuvkami. Může tedy zajistit přepěťovou ochranu pro sever, modem a PC. V případě výpadku energie pokryje UPS takovou dobu, aby mohli zaměstnanci uložit rozdělanou práci a mohli všechna zařízení bezpečně vypnout.

Bezpečnost kabelových rozvodů

Vedení kabeláže z prvního poschodí do přízemí je nutné zabezpečit ochrannými kovovými lištami. Tím se zamezí možnému poškození či odposlouchávání toku dat.

7.2.6 Bezpečnost provozu

Neméně podstatná část vycházející z analýzy rizik se zabývá bezpečným provozem na síti. Opatření se zaměřují na ochranu proti malwaru, oprávněním instalací softwaru a zálohováním dat.

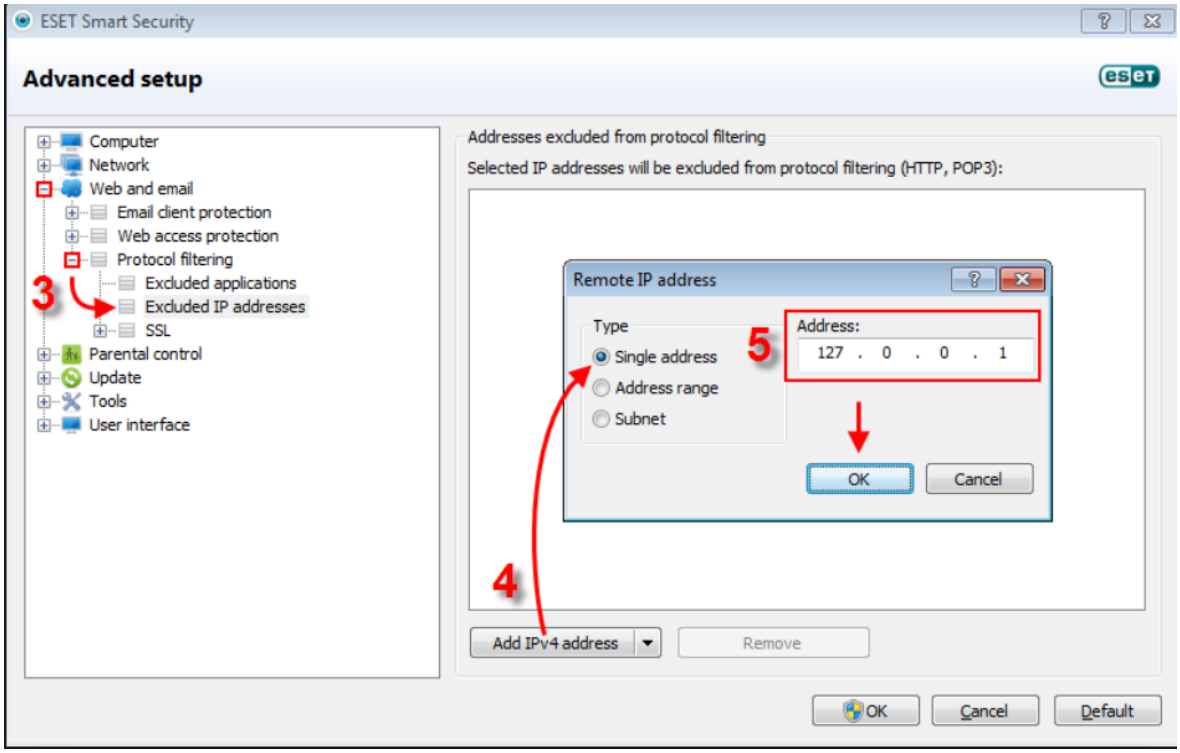
Navržená opatření mají za cíl snížit níže uvedené hrozby:

- Krádež médií nebo dokumentů.
- Neoprávněné použití zařízení.
- Poškození dat.

Opatření proti malwaru

Jedním z opatření je zákaz instalací programů ze strany zaměstnanců. Opatření je zajištěno úpravou v oprávnění. Oprávnění k instalaci má pouze vlastník ordinace. Dalším opatřením je zákaz používání jakýchkoliv datových médií. Povoleno je pouze použití firemního datového zařízení, pokud je nutné k firemnímu úkonu.

Dalším opatřením je zakoupení licencí na provoz antivirového programu od firmy Esset. Balíček Smart Security Premium nabízí řešení ochrany proti malware ve formě šifrování komunikace mezi klávesnicí a prohlížečem. Zamezí se tím získání a zneužití citlivých dat. Zajímavou funkcí je kontrola zabezpečení routeru a možnost kontroly připojených zařízení. Tento balíček nabízí navíc možnost šifrování dat, které je v případě citlivých dat v ordinaci žádoucí. [20]



Obr. 8: Kontrola připojených zařízení [20]

Zálohování

Zálohování dat bude probíhat na NAS serveru. Jedná se o zařízení, které je připojené síti, umožňující ukládání dat. Zálohování bude probíhat každý den ve 12 hodin, kdy je polední přestávka. PC nejsou v tuto dobu téměř vůbec využívány.

7.2.7 Bezpečnost komunikací

Opatření bezpečnosti komunikací má za cíl zajištění ochrany informací přenášených a používaných v sítích.

Opatření v oblasti bezpečnosti komunikací mají za cíl eliminaci níže uvedených hrozeb:

- Krádež médií nebo dokumentů.
- Neoprávněné použití zařízení.

Opatření v sítích

Síť bude spravována ze strany vlastníka ordinace. Doporučení z hlediska opatření v sítích je zavedení blokátorů na nevyužité porty. Dalším opatřením budou zámky nad připojenými kabely. Všechny kabely by měly být označeny štítkem pro větší přehlednost.

Obr. 9: Zámek portu RJ45 [21]

Bezpečnost síťových služeb

V rámci bezpečnosti síťových služeb bude zaveden hraniční firewall, který bude zabezpečovat síť od vnějších útoků. Ve spolupráci s majitelem bude vypracován seznam webových stránek, které budou povoleny. Další funkcí firewallu je sledování síťového provozu a vyhodnocování, zda neprobíhá pokus o útok na síť.

Druhým zabezpečením je VPN, které zaručí bezpečné spojení mezi ordinační sítí a koncovým zařízením. Vstup do sítě je umožněn na základě správně zadaného jména a hesla.

7.3 Ekonomické zhodnocení

Vzhledem k tomu, že fyzioterapeutická ordinace nemá zavedenou žádnou infrastrukturu, je nutné ji vybudovat od základu. Náklady na vybudování infrastruktury by neměly být vysoké. Navrhnuté řešení zahrnuje komponenty určené pro chod menších podniků. V případě použití průmyslového řešení by byly náklady několikanásobně vyšší. V rozpočtu jsou vedeny všechny nutné položky.

Tab. 8: Rozpočet návrhu sítě, zabezpečení, Zdroj: [vlastní]

číslo pol.	Položka	Množství	Cena/jednotku	Pořizovací cena
1	Datacom 1359 UTP CAT6 PE	100 m	10,49	1 049,00
2	Kovová lišta	20 m	104	2 080,00
3	Plastová lišta	80 m	58	4 640,00
4	ASUS RT-AC58U	1 ks	3309	3 309,00
5	Synology DiskStation DS418play	1 ks	12 330	12 330,00
6	Netgear GS108GE	1 ks	790	790,00
7	Seagate IronWolf - 2TB	4 ks	1790	7 160,00
8	CyberPower BR1200ELCD-FR	1 ks	3597	3 597,00
9	Esset Smart Security Premium pro 4 PC	1 ks	1890	1 890,00
10	Logitech Circle 2	2 ks	3760	7 520,00
11	Práce	35 hod	350	12 250,00

Cena celkem s DPH	56 615,00

Celkové náklady včetně nákladů na práci vychází na částku 56 615 Kč. Nejdražší položkou je server, ke kterému je nutné připočíst čtyři 2 TB disky. Hodnota za server je tedy rovna částce 19 490 Kč. Použitím těchto komponentů se podaří vybudovat kvalitní bezpečnou síť pro potřeby fyzioterapeutické ordinace.

ZÁVĚR

Cílem této práce bylo navrhnout bezpečnostní politiku pro fyzioterapeutickou ordinaci. Ordinace nemá v plánu získat certifikaci dle normy ISO/IEC 27001. Záměrem bylo použití ISMS jako standardu pro zavádění bezpečného systému.

První část této práce pojednává o teoretických východiscích a definuje obecné pojmy z oblasti bezpečnosti informací. Popisuje systém řízení bezpečnosti informací včetně Demingova modelu PDCA, kterým se celý systém řídí. Dále byla věnována pozornost také analýze rizik. Popsány jsou vybrané normy z řady ISO/IEC 27 000. Tyto normy budou sloužit pro následující vyhotovení praktické části. Teoretická část je uzavřena českou legislativou.

Druhá část je zaměřena na popis fyzioterapeutické ordinace z pohledu bezpečnosti objektu a síťové infastruktury. Byl zhodnocen aktuální stav informační bezpečnosti. Následně byly identifikovány a ohodnoceny důležitá aktiva, hrozby a zranitelnost aktiv. Vlastní analýza byla vyhotovena prostřednictvím programu Riskan, jehož výsledkem byla matice rizik. Na základě takto zjištěných rizik byla navrhnuta nová počítačová síť, která pokryje část zjištěných rizik. Zbývající rizika jsou eliminována aplikováním normy ISO/IEC 27001.

Tento návrh byl předložen majiteli ordinace, jež rozhodne, zda bude nový návrh realizován či nikoliv. Samozřejmě součástí práce je i ekonomické zhodnocení výdajů na zjištěná opatření. Výdaje za síťovou infrastrukturu byly odhadnuty na cca 60 000 Kč.

SEZNAM POUŽITÉ LITERATURY

[1] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových informačních systémech*. Vyd. 1. Zlín: Univerzita Tomáše Bati, 2002. ISBN 80-731-8095-2.

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

[3] HANÁČEK, Petr. a Jan. STAUDEK. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. 1. vyd. Praha: Úřad pro státní informační systém, 2000. ISBN 978-802-3854-008.

[4] SINGER, P. W. a Allan FRIEDMAN. *Cybersecurity and cyberwar: what everyone needs to know*. 1. New York: Oxford University Press, 2014. ISBN 978-0-19-991-809-6.

[5] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-807-2048-724.

[6] 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.

[7] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010. Expert (Grada). ISBN 978-80-247-3051-6.

[8] Technické normy a jejich využití v praxi. *Business info* [online]. Praha: BusinessInfo.cz, 2011 [cit. 2018-03-17]. Dostupné z: http://www.businessinfo.cz/cs/clanky/technicke-normy-a-jejich-vyuziti-v-praxi-4833.html

[9] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[10] *Zákon č. 101/2000 Sb. O ochraně osobních údajů*. In: . Praha: Úřad pro ochranu osobních údajů, 2000, ročník 2000, 101/2000. Dostupné také z: https://business.center.cz/business/pravo/zakony/oou/

[11] Národní centrum kybernetické bezpečnosti: Informace o změnách zákona č. 181/2014 Sb. *Www.govcert.cz* [online]. NÚKIB Brno: Národní úřad pro kybernetickou bezpečnost, 2017 [cit. 2018-02-02]. Dostupné z: https://www.govcert.cz/download/legislativa/2017/Zm%C4%9Bna_z%C3%A1kona_o_kybernetick%C3%A9_bezpe%C4%8Dnosti_velk%C3%A1_novela_v4.pdf

[12] Národní centrum kybernetické bezpečnosti: Informace o změnách zákona č. 181/2014 Sb. *Www.govcert.cz* [online]. NÚKIB Brno: Národní úřad pro kybernetickou bezpečnost, 2017 [cit. 2018-02-02]. Dostupné z: https://www.govcert.cz/download/legislativa/2017/Zm%C4%9Bna_z%C3%A1kona_o_kybernetick%C3%A9_bezpe%C4%8Dnosti_1_7_2017-final.pdf

[13] *ČSN ISO/IEC 27000: Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[14] *ČSN ISO/IEC 27001: Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[15] *ČSN ISO/IEC 27002: Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.* 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[16] *ČSN ISO/IEC 27003: Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací*. 2011. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.

[17] *ČSN ISO/IEC 27004: nformační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Měření.* 2011. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.

[18] *ČSN ISO/IEC 27006: nformační technologie - Bezpečnostní techniky - Požadavky na*

orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací. 2013. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[19] CyberPower: BRICs LCD Series BR1200ELCD. In: *Https://www.alza.cz/cyberpower-brics-lcd-series-br1200elcd-d4055353.htm* [online]. Praha: Alza.cz, 2018 [cit. 2018-04-07]. Dostupné z: https://www.alza.cz/cyberpower-brics-lcd-series-br1200elcd-d4055353.htm

[20] Antivir: Smart security premium. In: *Https://www.eset.com/cz/domacnosti/smart-security-premium/* [online]. Bratislava: Esset, 2018 [cit. 2018-04-08]. Dostupné z: https://www.eset.com/cz/domacnosti/smart-security-premium/

[21] Zámek portu: RJ45. In: *Https://shop.bechtle.cz/cs/product/z-225-mek-portu-rj45-sed-253-10-ks-1-kl-237-c--853816* [online]. Praha: Bechtle, 2018 [cit. 2018-04-08]. Dostupné z: https://shop.bechtle.cz/cs/product/z-225-mek-portu-rj45-sed-253-10-ks-1-kl-237-c--853816

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

HW	Hardware
IS	Information system
ISMS	Information security management system
LAN	Local area network
NAS	Network Attached Storage
OS	Operating system
PC	Personal computer
SW	Software
UPS	United Parcel Service
VPN	Virtual Private Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK