ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra biomedicínské informatiky

Řešení IT bezpečnosti v malé lékařské ordinaci

IT security solutions in a small doctor's office

Bakalářská práce

Studijní program:	Biomedicínská a klinická technika
Studijní obor:	Biomedicínská informatika

Autor bakalářské práce:	MDDr. Vojtěch Boček
Vedoucí bakalářské práce:	RNDr. Dagmar Brechlerová, Ph.D.

Kladno 2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Boček**	Jméno:	**Vojtěch**	Osobní číslo:	**491780**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra biomedicínské informatiky**				
Studijní program:	**Biomedicínská a klinická technika**				
Studijní obor:	**Biomedicínská informatika**				

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Řešení IT bezpečnosti v malé lékařské ordinaci

Název bakalářské práce anglicky:

IT security solutions in a small doctor's office

Pokyny pro vypracování:

V rešeršní části student shrne zákony, vyhlášky, normy a další předpisy, které se týkají vedení malé ordinace z hlediska IT bezpečnosti a zejména dodržení GDPR. V praktické části bude provedena analýza rizik ve vybraném zdravotnickém zařízení (malá ordinace), ze které vyplynou pro danou ordinaci doporučená bezpečností opatření. Také v této části vznikne řada doprovodných dokumentů, které jsou pro řešení bezpečnosti a v souvislosti s dodržením GDPR nezbytné. Jako další výstup vypracuje student vzorovou metodiku pro řešení IT bezpečnosti a dodržení GDPR pro malou ordinaci (max. 5 zaměstnanců), do které shrne své poznatky z předcházející práce.

Seznam doporučené literatury:

[1] TĚŠITELOVÁ, Vladimíra, Radek POLICAR, Milan BLAHA, Daniel KLIMEŠ a Ladislav DUŠEK. , Jak implementovat nařízení evropského parlamentu a rady (EU) 2016/679. , internet, ed. Ministerstvo zdravotnictví ČR, Ministerstvo zdravotnictví ČR, [Praha], 2018, [Revidováno 2018], ISBN ISBN 978-80-85047-55-4
[2] Zvárová, Jana - Lhotská, L. - Přibík, Vladimír - Adášková, Jana - Brechlerová, Dagmar - Hanzlíček, Petr - Huptych, M. - Kopecký, M. - Papíková, Vendula - Potůček, J. - Přečková, Petra - Říha, Antonín - Svátek, Vojtěch - Šárek, Milan - Zitová, Barbara - Zv, Biomedicínská informatika, 4, ed. Biomedicínská informatika, 4, ročník 2010, kapitola ---, 2010, Karolinum
[3] KOLOUCH, Jan a Pavel BAŠTA, Cyber Security, CZ.NIC, z.s.p.o., 2019, ISBN 978-80-88168-31-7
[4] Josef Požár, Informační bezpečnost, ed. vysokoškolská učebnice, Aleš Čeněk , 2005, ISBN 80-86898-38-5

Jméno a příjmení vedoucí(ho) bakalářské práce:

RNDr. Dagmar Brechlerová, Ph.D.

Jméno a příjmení konzultanta(ky) bakalářské práce:

Ing. Anna Schlenker, Ph.D.

Datum zadání bakalářské práce: **14.02.2022**
Platnost zadání bakalářské práce: **18.09.2023**

doc. Ing. Zoltán Szabó Ph.D.
vedoucí katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
děkan

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem „Řešení IT bezpečnosti v malé lékařské ordinaci“ vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k diplomové práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně …… …..……..……...

MDDr. Vojtěch Boček

PODĚKOVÁNÍ

Rád bych poděkoval paní RNDr. Dagmar Brechlerové, Ph.D. za vedení práce, připomínky, cenné rady a projevenou trpělivost.

ABSTRAKT

Řešení IT bezpečnosti v malé lékařské ordinaci

Hlavním tématem bakalářské práce je bezpečnost informací v malém zdravotnickém zařízení. Cílem práce je provést analýzu rizik v konkrétním malém zdravotnickém zařízení a doporučení bezpečnostních opatření ke snížení identifikovaných rizik. Teoretická část práce zpracovává úvod do problematiky informační bezpečnosti v malém zdravotnickém zařízení. Analýza rizik byla provedena na základě norem rodiny ISO/IEC 27xxx. K doporučeným bezpečnostním opatřením jsou vypracovány podpůrné materiály pro jejich implementaci.

Klíčová slova

ISMS, systém řízení bezpečnosti informací, zdravotnická dokumentace, GDPR, analýza rizik

ABSTRACT

IT security solutions in a small doctor's office

This thesis focus is the information security in a small health facility. The main goal is to conduct a risk analysis in one small health facility and make security recommendations to mitigate identified risks. First part is the introduction to base theory of information safety in a small health facility. Risk analysis was based on ISO/IEC 27xxx standard. There are prepared support materials for proposed security measures.

Keywords

ISMS, information security management system, medical record, GDPR, risk analysis

Obsah

Seznam symbolů a zkratek

Seznam symbolů

Symbol	Význam
A	Hodnota aktiva
R	Míra rizika
T	Pravděpodobnost hrozby
V	Úroveň zranitelnosti

Seznam zkratek

Zkratka	Význam
CD	Compact disc
GDPR	Obecné nařízení o ochraně osobních údajů (*General Data Protection Regulation*)
IKEM	Institut klinické a experimentální medicíny
IS	Informační systém
ISMS	Systém řízení bezpečnosti informací (*Information Security Management Systém*)
IT	Informační technologie
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDCA	Plánuj – Dělej – Kontroluj – Jednej (*Plan – Do – Check – Act*)
UPS	Zdroj nepřerušovaného napájení (*Uninterruptible power supply*)
ZZ	Zdravotnické zařízení

1 Úvod

Tato práce se zabývá informační bezpečností v malém zdravotnickém zařízení. Výběr tématu bakalářské práce byl motivován současným stavem bezpečnosti informací ve zdravotnictví. Je veřejným tajemstvím, že situace informační bezpečnosti ve zdravotnických zařízení obecně není příliš dobrá. Ve sdělovacích prostředcích se často setkáváme se zprávami o narušení informační bezpečnosti. Z poslední doby lze připomenout kybernetický útok na fakultní nemocnici Brno z roku 2020 nebo ransomwarový útok na Nemocnici Rudolfa a Stefanie Benešov. Tyto široce medializované bezpečnostní incidenty jsou pouze špičkou ledovce. V rámci informační bezpečnosti je třeba brát v úvahu i bezpečnostní incidenty malého rozsahu. O bezpečnostních incidentech malého rozsahu se obvykle veřejnost nedozví, ale to neznamená, že neexistují. Jako příklad lze uvést únik informací o zdravotním stavu Miloše Zemana z SMS konverzace mezi Andrejem Babišem a přednostou Kliniky hepatogastroenterologie IKEM Juliem Špičákem [1]. Tyto bezpečnostní incidenty se odehrály ve velkých zdravotnických zařízeních, které mají silné finanční, technologické i personální zázemí. Malá zdravotnická zařízení mají ke zdrojům potřebným k zajištění informační bezpečnosti obvykle výrazně ztížený přístup. V tomto světle se jeví situace malých zdravotnických zařízení v oblasti zajištění informační bezpečnosti velkou výzvou. Je potřeba této výzvě čelit na všech úrovních. Je potřeba provést opatření k zajištění bezpečnosti na úrovni státu, zdravotnictví, odborných společností, ale hlavně i na úrovni jednotlivých provozovatelů. Sám jsem provozovatel malého zdravotnického zařízení a zkušenosti z provozu bych chtěl promítnout do této práce.

Úkolem této bakalářské práce bude zhodnotit právní předpisy a normy upravující bezpečnost informací v malém zdravotnickém zařízení. V praktické části bude provedeno zhodnocení současného stavu informační bezpečnosti v konkrétním zdravotnickém zařízení, ohodnocení rizik a návrh opatření ke snížení rizika. Nakonec budou vypracovány doprovodné dokumenty k navrhovaným opatřením.

V první části práce bude proveden obecný přehled informační bezpečnosti ve zdravotnictví a bude provedena rešerše literatury týkající se zpracování osobních údajů, vedení zdravotnické dokumentace a řízení bezpečnosti informací. Bude zde vypracován krátký úvod do právních předpisů upravujících zacházení s osobními údaji a zdravotnickou dokumentací a přehled norem upravujících systém řízení bezpečnosti informací.

V druhé části zpracuji metodiku, podle které se bude řídit analýza rizika, která bude předmětem třetí části této práce. V rámci metodiky budou zpracovány postupy vyhodnocení analýzy a u jednotlivých postupů bude zdůvodněno, proč byl zvolen daný postup.

Třetí část bude vlastní analýza rizik. V této části bude nejdřív provedeno vlastní zhodnocení konkrétního zdravotnického zařízení a budou zpracovány vstupy pro vlastní analýzu rizik. V dalším kroku budou prezentovány výsledky analýzy a pro identifikovaná bezpečnostní rizika budou vypracovány návrhy bezpečnostních opatření. Na závěr budou pro navržená opatření zpracovány podklady potřebné k jejich zavedení do praxe.

2 Přehled současného stavu

Oblast zdravotnictví zahrnuje velké množství subjektů. V roce 2017 bylo evidováno 32 080 zdravotnických zařízení. Z převážné většiny jsou tato zdravotnická zařízení malého rozsahu a jsou tvořena jednotkami pracovníků. Jedná se o soukromé ordinace praktických lékařů, stomatologů, gynekologů a dalších lékařů specialistů. Jen těchto vyjmenovaných zařízení bylo v roce 2017 evidováno 21 975 [2]. Tato zařízení tvoří páteř ambulantní zdravotní péče. Zdravotnické zařízení, které je předmětem této práce, je typickým příkladem této kategorie. Jak je patrné z uvedených počtů, bezpečnost informací v malých zdravotnických zařízeních se může týkat velkého počtu subjektů.

Zdravotnictví je oblastí lidské činnosti postavené na informacích. A zároveň je ochrana zdraví jednou z hlavních priorit společnosti. Proto má oblast zdravotnictví specifické postavení ve vztahu k ochraně osobních údajů. Při poskytování zdravotních služeb je nutné sbírat, uchovávat a zpracovávat velké množství osobních údajů. Část informací získaných při tvorbě zdravotnické dokumentace získává na účelnosti až v kontextu budoucí péče, proto nelze použít princip minimalizace sběru osobních údajů. Tento fakt způsobuje, že část informací je potřebné sbírat preventivně. Z těchto důvodů je dáno oblasti zdravotnictví jisté privilegované postavení ve vztahu k ochraně osobních údajů. Toto postavení je kompenzováno poměrně složitým systémem právních předpisů, kterými se musí subjekty ve zdravotnictví řídit.

Informace ve zdravotnictví mohou mít různou formu. Historicky dominantní formou byla forma listinná, ale s postupující digitalizací ve společnosti se postupně digitalizuje i oblast zdravotnictví. České zdravotnictví lze pokládat za odvětví velmi konzervativní a s velmi pomalým postupem digitalizace. Důvodů lze identifikovat mnoho. Z nejvýznamnějších je nutno zmínit zejména nepřehlednou právní úpravu, požadavky na nízkou chybovost, nedostatek IT pracovníků, nedostatečné financování a odpor části lékařů ke změně pracovních procesů.

> *„Elektronizace ve zdravotnictví probíhá v ČR navzdory nedostatečné právní úpravě. Děje se tak živelně a bez centrálně stanovených pravidel, postupů, standardů. S ohledem na veřejný charakter výdajů ve zdravotnictví (převážná část zdravotní péče je hrazena z veřejného zdravotního pojištění) je nezbytné nastavit na centrální úrovni jasná pravidla, která povedou ke splnění třech faktorů: hospodárnosti, účelnosti a efektivity a umožní tak řízený a bezpečný rozvoj elektronizace zdravotnictví v ČR.” [3]*

Postupující digitalizace klade zvýšené nároky na bezpečnost informačních systémů (IS). Je veřejným tajemstvím, že v oblasti bezpečnosti IS má oblast zdravotnictví výrazné nedostatky.

> *„[v diskusích mezi zástupci nemocnic a NÚKIB] … je často skloňováno, že je [kybernetická bezpečnost] problém, který byl podceněn. Nevěnovalo se mu dostatek pozornosti a zdrojů a je potřeba s tím něco dělat. „ [4]*

Bezpečností informačního systému se obvykle rozumí bezpečnost jak hardwaru a softwaru, tak zabezpečení informací v něm zpracovávaných. Dále sem patří bezpečnost, komunikační, personální i fyzická, ochrana před přírodními vlivy apod. [5]. Zajištění bezpečnosti takto komplexního systému není jednoduché, a proto je k němu potřeba přistupovat systematicky. V této části práce se dále budu zabývat úvodem do problematiky bezpečnosti informací ve zdravotnictví a souvisejícími právními předpisy a normami.

2.1 Legislativa a normy

Tato část se zabývá právními předpisy a normami, které upravují zacházení s osobními údaji, zdravotnickou dokumentaci a řízení bezpečnosti informací. Výčet se omezí pouze na základní předpisy upravující danou problematiku, neboť systém právních předpisů upravujících oblast bezpečnosti informací ve zdravotnictví je velmi komplexní a jeho vyčerpávající přehled by překročil hranice této práce.

2.1.1 ČSN EN ISO/IEC 27xxx

Jedná se o soubor českých překladů norem rodiny ISO/IEC 27xxx. Tato série obsahuje normy pokrývající celou škálu zajištění bezpečnosti informací. Pro řízení bezpečnosti informací v malém zdravotnickém zařízení jsou významné zejména následující:

- ČSN EN ISO/IEC 27000 – Přehled a slovník
- ČSN EN ISO/IEC 27001 – Systémy řízení bezpečnosti informací – Požadavky
- ČSN EN ISO/IEC 27002 – Soubor postupů pro opatření bezpečnosti informací
- ČSN EN ISO/IEC 27003 – Systémy řízení bezpečnosti informací – Pokyny
- ČSN EN ISO/IEC 27004 – Systémy řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení
- ČSN EN ISO/IEC 27005 – Řízení rizik bezpečnosti informací
- ČSN EN ISO/IEC 27799 – Systémy řízení bezpečnosti informací ve zdravotnictví

2.1.2 GDPR

General Data Protection Regulation neboli Obecné nařízení o ochraně osobních údajů představuje právní rámec ochrany osobních údajů v evropském prostoru s cílem hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich daty včetně osobních údajů. Je to přímo aplikovatelná norma na všechny subjekty, není nutná implementace do národních právních řádů. Stanovuje výjimky, které státům umožňují, nebo v některých případech ukládají povinnost upravit zacházení s osobními údaji v rámci těchto výjimek. Jednou z výjimek je i generální výjimka pro zdravotnictví.

GDPR bylo koncipováno jako performativní norma. Performativní norma (nebo také performance-based regulace) je způsob regulace, kde předpis stanoví cíle a podmínky regulace a ponechá na regulovaném subjektu stanovení vlastního způsobu provedení. Tím je umožněno pružněji reagovat na případný technický vývoj a individualizace příslušného způsobu plnění normy vlastním subjektem. Specifikou tohoto řešení je diverzita pravidel a postupů v rámci různých subjektů. Na úrovni EU vznikla pracovní skupina Working Party 29, která vydává výkladová stanoviska k jednotlivým článkům GDPR.

Osobní údaj

Základním pojmem pro GDPR je „osobní údaj“. Osobním údajem jsou jakékoli informace, které se týkají identifikované nebo identifikovatelné žijící osoby.

Norma GDPR vyčleňuje osobní údaj zvláštní kategorie. Jedná se o zvlášť citlivá data, jež lze zpracovávat pouze na výjimkou (ve zdravotnictví se jedná o generalizovanou výjimku pro zdravotnictví).

> *“Zvláštní kategorie osobních údajů jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby.” [6]*

Subjekt údajů

V kontextu GDPR je subjekt údajů fyzická žijící osoba. GDPR přiznává subjektu údajů celou řadu práv. V závislosti na právním důvodu zpracování může dojít k omezení práv subjektů, pro oblast zdravotnictví se jedná o práva na informování a zejména právo na výmaz.

Správce údajů

"Správcem je subjekt, nerozhoduje, jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (např. zákonem stanovené povinnosti, ze smluv), ale může je zpracovávat i pro vlastní určené účely např. pro své oprávněné zájmy, pokud tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob." [7]

Povinnosti správců je provádět záměrnou a standardní ochranu osobních údajů. Tím se rozumí, že správce musí:

- Provádět zpracování v souladu s GDPR
- Povinnost zajistit dostatečnou ochranu dat proti zničení, ztrátě, úniku a neoprávněné modifikaci
- Zavést vhodná technická, personální a organizační opatření k ochraně osobních údajů
- Být schopen doložit tato opatření
- Posuzovat vliv na ochranu osobních údajů při změnách v organizaci a aktualizovat opatření v případě potřeby.

Vzhledem ke komplexnosti povinností správce se jeví použití uceleného systému na ochranu osobních údajů jako nutnost.

Zpracovatel

Zpracovatelem je subjekt (nejčastěji fyzická nebo právnická osoba), který zpracovává pro správce zpracovatelské operace. Zpracovatel může tyto operace provádět pouze na základě pověření od správce osobních údajů.

Právní titul

Zpracování osobních údajů je obecně zakázáno. Z tohoto zákazu lze pomocí právních nařízení stanovit různé výjimky. Tyto výjimky, na jejichž základě lze osobní údaje zpracovávat, se nazývají právní ruly zpracování (právní důvody zpracování). Právní tituly zpracování jsou uvedeny v článku 6. odstavci 1. GDPR. [8]

„1. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo za účelem přijetí opatření na žádost subjektu údajů před uzavřením smlouvy;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě." [9]

Na základě právního titulu pro zpracování lze rozdělit soubory osobních údajů (zdroje údajů) do kolekcí. Právní titul určuje, která práva subjektu údajů mohou být omezena. Tabulka 2.1 zobrazuje vazbu právního titulu zpracování na práva subjektu údajů. Vedení zdravotnické dokumentace je dané zákonem (§53 odst. 1 zák. č. 372/2011 Sb.), proto spadá do kategorie plnění právní povinnosti. Pro vedení zdravotnické dokumentace je důležité zejména omezení práva subjektu údajů na výmaz.

Tabulka 2.1: Vazba práv subjektu údajů na právní titul zpracování údajů zdroj: [23]

Právní důvod	Informování, jsou-li údaje získány od subjektu údajů	Informování, jsou-li údaje získány z jiného zdroje	Právo na přístup	Právo na opravu (řetězení)	Právo na výmaz (řetězení)	Právo na omezení zpracování (řetězení)	Právo na přenositelnost (smlouva, souhlas a automatizované zpracování)	Právo vznést námitku	Právo nebýt podroben automatizo-vanému rozhodování
	13	14	15	16	17	18	20	21	22
Právní povinnost uložená správci	Ano	Ne, je-li výslovně stanoveno předpisem spolu se zárukami	Ano	Ano	Ne (do skartační lhůty)	Ano	Ne	Ne	Ne, pokud není povoleno právním předpisem stanovícím záruky
Životně důležitý zájem subjektu údajů	Ne	Ne, je-li výslovně stanoveno předpisem spolu se zárukami	Ano	Ano	Ne (ne do skartační lhůty)	Ano	Ne	Ne	Ne, pokud není povoleno právním předpisem stanovícím záruky
Souhlas udělený subjektem údajů	Ano, upozornit na možnost odvolání souhlasu	Ano	Ano	Ano	Ano	Ano	Ano	Ne (ale může odvolat souhlas)	Ne, pokud je souhlas výslovný
Plnění smlouvy, smluvní stranou je subjekt údajů	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ano
Úkol ve veřejném zájmu nebo výkon pravomoci	Ano	Jako právní povinnost. Ne, pokud by popřelo smysl zpracování	Ano	Ano	Ne (do skartační lhůty, pokud je)	Ano	Ne	Ano	Ne, pokud není povoleno právním předpisem stanovícím záruky
Oprávněný zájem mimo oblast úkolů správce	Ano	Ano. Ne, pokud by popřelo smysl zpracování	Ano	Ano	Ano. Ne, pokud jde o ochranu právních nároků	Ano	Ne	Ano	Ano

Zde je potřeba zmínit katalog osobních údajů a operací zpracování (případně souhrnně „záznamy o činnostech zpracování"). Jedná se o inventuru zpracovávaných osobních údajů nejčastěji v podobě tabulky. Pomáhá v orientaci, pod kterou kategorii osobní údaje spadají a tím určují, jakým způsobem je lze uchovávat a zpracovávat.

Procesy zpracování dat se liší se dle jednotlivých kategorií – jsou určeny právním titulem a jsou zaznamenány v katalogu operací zpracování.

2.1.3 Vyhláška č. 98/2012 Sb., O zdravotnické dokumentaci

Základní právní předpis stanovující obsah zdravotnické dokumentace, formální náležitosti vedení zdravotnické dokumentace. Vyhláška obsahuje 3 přílohy.

Příloha č.1 – Obsah samostatných částí (žádanky, výpisy…)

Příloha č.2 – Zásady pro uchování, vyřazování a zničení

Příloha č.3 – Doby uchování zdravotnické dokumentace

2.1.4 Zákon č. 372/2011 Sb., O zdravotních službách a podmínkách pro jejich poskytování

Zdravotnickou dokumentací se zabývá část šestá zákona. V §53 odstavci 2 zákon řeší obsah zdravotnické dokumentace. V §54 a §54 jsou vyjmenovány možné způsoby vedení zdravotnické dokumentace a podmínky za kterých je možné, zdravotnickou dokumentaci určeným způsobem vést.

2.2 Zdravotnická dokumentace

Zdravotnická dokumentace je základní a nejdůležitější informací ve zdravotnickém zařízení. Vzhledem k výjimečnému postavení zdravotnické dokumentace z pohledu právních předpisů a vysoké citlivosti údajů v ní obsažených se jedná o soubor informací se specifickým životním cyklem.

2.2.1 Vznik zdravotnické dokumentace

Sběr osobních údajů pro založení a aktualizování zdravotnické dokumentace je řízen právním titulem zpracování. Právní titul pro sběr a zpracování osobních údajů je dán splněním právní povinnosti správce danou §53 zákona č. 372/2011Sb. Osobní údaje, které je možné zpracovávat, jsou vyjmenované ve vyhlášce č 98/2012 Sb.

2.2.2 Uchovávání zdravotnické dokumentace

Po dobu uchovávání zdravotnické dokumentace je nutné ochránit informace v ní obsažené před únikem (zachování důvěrnosti), neoprávněnou modifikací (zachování integrity) a zničením. Dále nutné zachování dostupnosti zdravotnické dokumentace nejen pro provozování zdravotních služeb, ale i pro případ kontroly orgánem veřejné moci.

Dle §54 odstavce 1 zákona č. 372/2011Sb. je přípustná forma vedení zdravotnické dokumentace trojí: elektronická, listinná a kombinovaná forma.

Požadavky na uchovávání zdravotnické dokumentace.

- Dokumentace v listinné podobě – Zde je důraz kladený na fyzické zabezpečení zdravotnické dokumentace. Dokumentace musí být uchovávána v uzamčené místnosti nebo uzamčené kartotéce mimo dobu, kdy s ní manipuluje odpovědný personál. Musí být zajištěná ochrana proti zničení.
- Dokumentace v kombinované podobě – nutno splňovat standardy u jednotlivých položek odpovídající jejich formě.
- Dokumentace v elektronické podobě – Je nutné zajistit jak fyzickou bezpečnost (zařízení, na kterých se mohou vyskytovat osobní údaje, musí být zajištěna proti neoprávněnému přístupu jak z pohledu zničení – a tím ztráty dat – tak z pohledu možného úniku dat), tak kybernetickou – řízení přístupu, vytváření záloh, nastavení bezpečnostních opatření v podobě firewallu, antiviru atd.

2.2.3 Zálohování zdravotnické dokumentace

Zálohováním se rozumí vytvoření kopie souboru dat na jiném datovém nosiči a ideálně uchovávaném na jiném místě. Zálohování je nutné zejména ze dvou důvodů. Za účelem ochrany dat a zajištění provozu. Je nutno zálohovat 2 kategorie informací: nastavení systému a programů a data.

Dle místa uložení záložních kopií dělíme zálohy do 2 kategorií. V případě onsite zálohy jsou záložní média uložena ve stejné lokaci jako informační systém. V případě offsite zálohy jsou záložní média mimo lokaci zálohovaného informačního systému.

Zabezpečení záložních kopií musí splňovat stejné standardy bezpečnosti jako původní data. Zajištění všech aspektů informační bezpečnosti je obvykle u záložních kopií komplikovanější, zejména z důvodu uložení části záloh mimo budovu, ve které se nachází zálohovaný informační systém.

Pro vedení zdravotnické dokumentace v elektronické nebo kombinované formě je nutné splnit několik povinností. Podmínky pro vedení zdravotnické dokumentace elektronicky stanovuje § 55 zákona č. 372/2011 Sb., O zdravotních službách. Ze zákona vyplývají tyto povinnosti:

- Záznam nesmí být možné modifikovat (podle § 55 písm. a) zákona č. 372/2011 Sb.)
- Zálohy nejméně 1x za den (podle § 55 písm. c) zákona č. 372/2011 Sb.)
- Uložení kopií pro dlouhodobé uchování nejméně 1x za rok (podle § 55 písm. e) zákona č. 372/2011 Sb.)
- Musí být zajištěna čitelnost kopií po dobu uchování zdravotnické dokumentace (podle § 55 písm. f) zákona č. 372/2011 Sb.)

2.2.4 Likvidace zdravotnické dokumentace

Skartace zdravotnické dokumentace je upravena vyhláškou č. 98/2012 Sb., O zdravotnické dokumentaci, a to zejména přílohami č. 2 a 3. Příloha č. 2 upravuje zásady pro uchování, vyřazování a zničení. Příloha č. 3 určuje dobu, po kterou musí být zdravotnická dokumentace uchovávána.

Skartace začíná uplynutím doby uchování (určené přílohou č. 3 vyhlášky) a započetím skartačního řízení. V rámci skartačního řízení musí proběhnout posouzení potřebnosti dokumentace, a na jeho základě je dokumentace označena k prodloužení doby uchování nebo k vyřazení. Zdravotnická dokumentace určená k vyřazení poté musí být zničena, a to nevratně tak, aby byla znemožněna rekonstrukce a identifikace obsahu. Tím je dána povinnost smazat zdravotnickou dokumentaci i ze záloh. Závěrem skartačního řízení je vystavení skartačního protokolu.

2.3 Řízení bezpečnosti informací

Každá organizace do určité míry pracuje s informacemi. Tyto informace je třeba chránit proti narušení při všech operacích s informací. K zajištění bezpečnosti informací je nutné zajistit tři aspekty: důvěrnost, integritu a dostupnost informací. [10]. K zajištění bezpečnosti informací v organizace je nutné zavést takový soubor opatření, aby bylo možno předpokládat zajištění všech tří aspektů bezpečnosti informace. Tento proces se nazývá řízení informační bezpečnosti a soubor těchto opatření se nazývá systém řízení bezpečnosti informací (Information Security Management System = ISMS). Úplný ISMS, který by vedl k eliminování veškerých rizik, neexistuje. Navíc, skutečné podmínky provozovatelů informačních systémů bývají vzdálené ideálním podmínkám, což často znemožňuje realizaci optimálního systematického řešení informační bezpečnosti [11]. Proto by mělo být cílem organizace zavést takový ISMS, který umožní řízení rizik v takovém rozsahu, aby bylo dosaženo bezpečnostních cílů organizace za přiměřeného využití zdrojů organizace.

Proces řízení bezpečnosti informací má své standardy a normy. Nejrozšířenějším používaným standardem je rodina norem ISO/IEC 27xxx.

2.3.1 Vymezení pojmů

Aktivum

Aktivum je statek, který má hodnotu pro organizaci. Aktivum může být hmotné i nehmotné. Základní charakteristikou aktiva je jeho hodnota založená na objektivním nebo subjektivním ocenění jeho důležitosti pro organizaci [12]. Aktiva je nutné rozlišit na dvě podskupiny.

- Primární aktiva – jsou definována jako klíčové procesy a informace o předmětu činnosti organizace [13]. Při degradaci těchto procesů a informací dochází k překážce na straně organizace při plnění svých poslání.
- Podpůrná aktiva – jsou statky, jejichž poškozením může dojít k poškození aktiv primárních. Jejich hodnota se odvíjí od hodnot aktiv primárních.

Hrozba

Hrozba je potencionální příčina nechtěného incidentu, jehož výsledkem může být poškození organizace [10]. Pro účely zkoumání bezpečnosti informačního systému je nutné hrozby ohodnotit. Hodnocení je subjektivní, relativní a bere v úvahu četnost výskytu události u náhodných hrozeb a míru složitosti a motivace u úmyslných útoků [14]. Hrozby působí na aktiva skrze zranitelnosti.

Zranitelnost

Zranitelnost je slabé místo informačního systému, jenž může být využito hrozbou. Přítomnost zranitelnosti nezpůsobuje škodu sama o sobě. Ke zneužití zranitelnosti je potřebná přítomnost hrozby [13].

Riziko

Riziko je existence možnosti poškození hodnoty aktiva hrozbou. Riziko vzniká působením hrozby na aktivum. Proto v kontextu analýzy rizik nemusíme brát v úvahu aktiva, na která nepůsobí žádná hrozba, a hrozby, které nepůsobí na žádné aktivum [12].

Útok

Požár definuje útok jako:

> *„Pokus o zničení, vystavení hrozbě, změnu, vyřazení z činnosti, zcizení aktiva nebo získání neoprávněného přístupu k aktivu nebo uskutečnění neoprávněného použití aktiva.“ [15]*

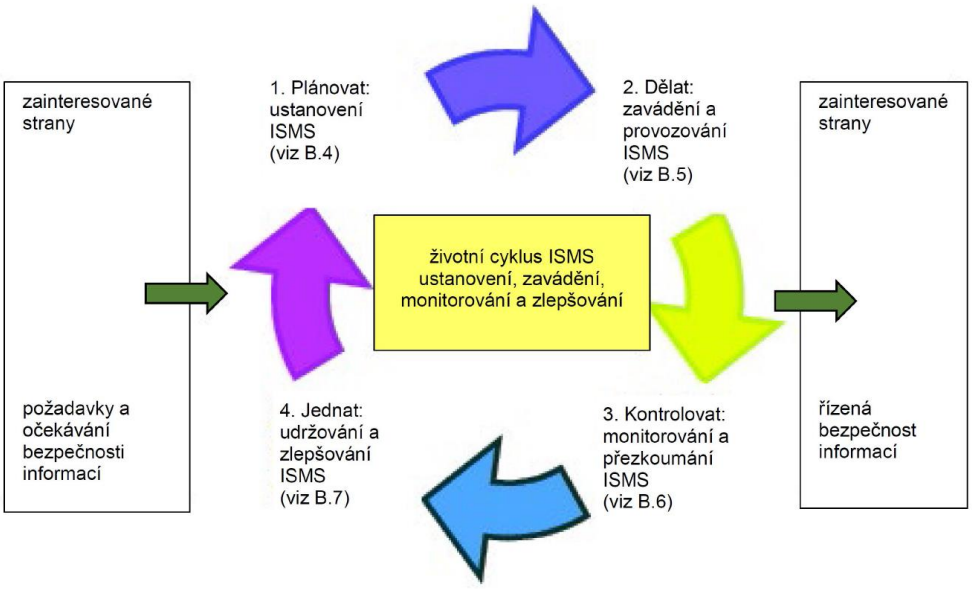
Útokem je akce, která může způsobit škodu na aktivech. Útoky využívají zranitelností. Pro útoku lze použít i označení bezpečnostní incident.

2.3.2 Systém řízení informační bezpečnosti (ISMS)

ISMS je systém sestávající se z politik, postupů, směrnic, zdrojů, činností, které organizace užívá k zajištění ochrany informace [10]. ISMS může nabývat různých podob dle potřeb organizace. Může se jednat o „ad hoc“ systém pro malou organizaci až po

rozsáhlé, komplexní systémy řízení rizik v nadnárodních organizacích. Pro oblast zdravotnictví je vhodné spravovat ISMS systematicky a standardizovaným způsobem.

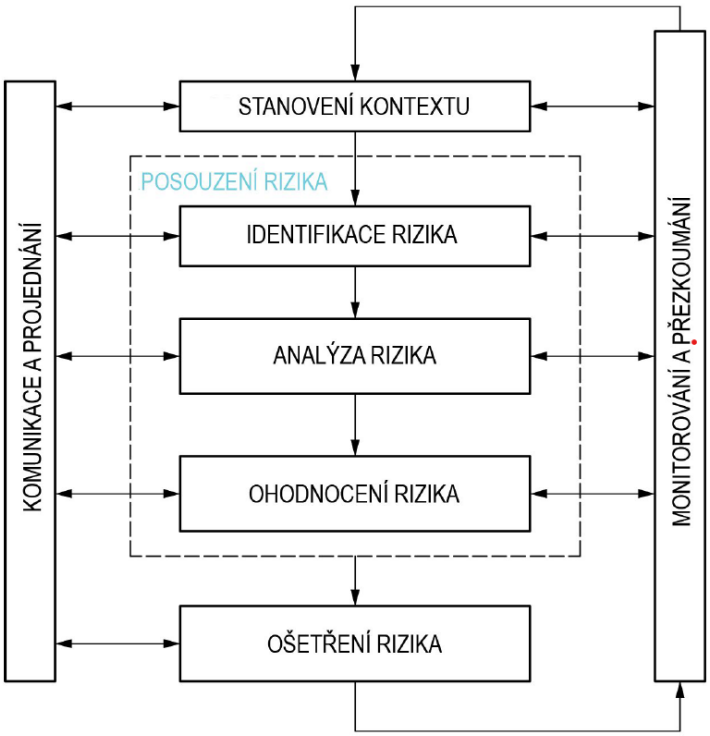
Sytém řízení bezpečnosti informací je založen na modelu PDCA (Plan – Do – Check – Act) [16]. PDCA metoda je obecná metoda řízení procesů v organizaci. Jedná se o iterativní proces skládající se ze 4 kroků: Plánuj – Dělej – Kontroluj – Jednej. Opakováním tohoto cyklu dochází k postupnému zlepšování řízení organizace. Aplikace PDCA metody řízení na životní cyklus ISMS je znázorněna na obrázku, viz Obrázek 2.1.



Obrázek 2.1: Přehled procesu ISMS zdroj: [17]

Ustanovení ISMS

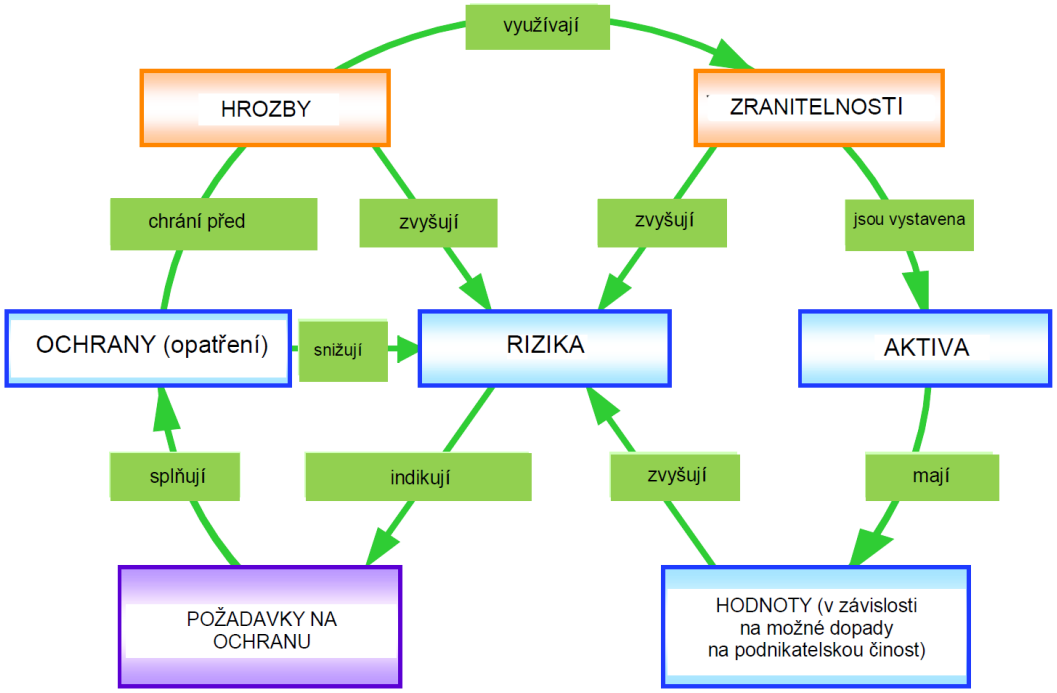
Ustanovení ISMS je první a velmi důležitou etapou procesu řízení bezpečnosti informací. Poklady vytvořené v tomto kroku vytváří základ, kterým se řídí celý proces zavádění, provozu, monitorování i zlepšování ISMS. Obrázek 2.2 ilustruje vztahy jednotlivých kroků při ustanovení ISMS.



Obrázek 2.2: Proces řízení rizik zdroj: [13]

Stanovení kontextu ISMS

Při vzniku každého systému řízení musí být nejprve vymezeny hranice řízeného systému, které reflektují požadavky organizace na rozsah a určení ISMS. V této fázi by měl být nastaven interní a externí rámec pro řízení rizik bezpečnosti informací [13]. V návaznosti na vymezení ISMS následuje vyhotovení a odsouhlasení Prohlášení a o politice ISMS. Jedná se o základní dokument ISMS, ve kterém je specifikován předmět bezpečnostní politiky, obsahuje cíle bezpečnostní politiky a ve kterém je ustanoven systém řízení informační bezpečnosti.



Obrázek 2.3: Vztahy mezi riziky a zdroji rizik na zjednodušeném modelu zdroj: [17]

Identifikace rizika

Identifikaci rizik musí předcházet identifikace aktiv. Identifikace aktiv vychází ze stanoveného rámce ISMS. Úroveň podrobností použitých při identifikace aktiv by měla být zvolena tak, aby poskytovala dostatečné informace pro posouzení rizika [13]. Neúměrně vysoká úroveň podrobností zvyšuje komplexnost a rozsah posouzení rizika. Pro každé aktivum by měl být určený vlastník. Hodnota aktiva je odvozena od závažnosti následků v případě úspěšného útoku na aktivum.

Dalším krokem při identifikaci rizika je identifikace hrozeb a zhodnocení jejich pravděpodobnosti. Hrozby jsou zaznamenány do katalogu hrozeb.

Zranitelnost vzniká interakcí hrozby a aktiva. Schéma vztahů jednotlivých atributů analýzy rizika lze znázornit grafem, viz Obrázek 2.3. Zranitelnosti musí být identifikovány, aby bylo možné vyhodnotit, nakolik jsou účinná existující bezpečnostní opatření. Existující bezpečnostní opatření je nutné nejprve identifikovat a poté zhodnotit jejich vliv na zranitelnosti. Výsledný stupeň zranitelnosti je zaznamenán.

Analýza rizika

Existují dvě hlavní metody pro vyhotovení analýzy rizik. Jedná se o metodu kvantitativní a kvalitativní. Dle požadavků na výstup analýzy rizik a dostupných vstupních datech lze použít obě metody i jejich kombinaci.

Kvantitativní metoda

Kvantitativní metoda je založena na matematickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu [12]. Pro využití této metody je nutné stanovit kvantifikované měřítko, například dopad může být ohodnocen vyčíslenou finanční ztrátou, proto měřítko bude „ztráta v Kč“.

Nevýhodou kvantitativní metody je poměrně velká náročnost na vstupní data. Při nedostatečné kvalitě vstupních dat může dojít k vzniku nepřesností při posouzení rizika. Kvantitativní metody bývají obvykle velmi náročné na zpracování.

Kvalitativní metoda

Kvalitativní analýza rizik používá popisná měřítka, kterými ohodnocuje jednotlivé položky analýzy rizika (např. pravděpodobnost vzniku události). Výhodou kvalitativní metody je srozumitelnost a obvykle menší náročnost vyhotovení. Nevýhodou je závislost na subjektivní volbě měřítka [13].

Ohodnocení rizika

Posledním krokem v procesu posouzení rizika by mělo být jeho ohodnocení. Ohodnocení rizika vychází z výstupů analýzy rizik a z kritérií hodnocení rizik definovaných při stanovení kontextu. Kritéria hodnocení rizik lze v této fázi přezkoumat a je možné na základě nových poznatků revidovat rozhodnutí učiněná při stanovení kontextu [13].

2.3.3 Zavádění a provoz ISMS

V této etapě cyklu ISMS dochází k prosazení a zavádění bezpečnostních opatření. Je důležité připravit dílčí plány, termíny, zodpovědné osoby apod. Tato bezpečnostní opatření by měla být zadokumentována v Příručce bezpečnosti informací [16].

2.3.4 Monitorování ISMS

Proces řízení bezpečnosti je iterativní proces, proto je nutné zajistit dostatečnou zpětnou vazbu z provozování ISMS. Zpětná vazba tvoří znalostní bázi pro zlepšování provozu ISMS a další iterace celého ISMS. Tyto informace lze získat auditní činností (externí i interní) nebo monitorováním účinnosti bezpečnostních opatření.

2.3.5 Udržování a zlepšování ISMS

Proces udržování a zlepšování ISMS je poslední fází v cyklu. Vstupními daty pro tento proces je datová báze vytvořená monitorováním a podněty zainteresovaných subjektů ke zlepšení ISMS. Na základě těchto informací by mělo docházet zavádění opatření k odstranění zjištěných nedostatků.

3 Cíle práce

Bezpečnost informací ve zdravotnickém zařízení je závažné téma. Jak vyplývá z přehledu legislativy, je potřeba vzít v úvahu jak specifické postavení zdravotnické dokumentace jako zdroje informací, tak specifika prostředí a provozu zdravotnického zařízení. Hlavním cílem této práce je systematizovat řízení informační bezpečnost v konkrétním malém zdravotnickém zařízení. Hlavní cíl je vhodné rozdělit na jednotlivé dílčí cíle.

Prvním dílčím cílem je navrhnout metodiku, podle které bude postupováno v dalších částech. Při volbě metodik bude nutné zohlednit potřeby a omezení malého zdravotnického zařízení. Je nutné stanovit metody pro sběr dat, jejich zpracování i pro zhodnocení výsledků.

Druhým dílčím cílem je zhodnocení současného stavu informační bezpečnosti v konkrétním zdravotnickém zařízení. Ke splnění tohoto cíle je potřeba postupovat po jednotlivých krocích. Prvním krokem je získání vstupních dat pro analýzu rizik. Následuje provedení vlastní identifikace a zhodnocení rizik. Postupy pro kroky se řídí zpracovanou metodikou.

Třetím dílčím cílem je navržení bezpečnostních opatření ke snížení identifikovaných rizik. K takto navrženým bezpečnostním opatřením budou zpracovány podklady, aby bylo možné navržená opatření uvést do praxe. Výstup bude mít podobu metodiky.

4 Metodika analýzy rizik

Postup pro analýzu rizik vychází z normy ČSN ISO/IEC 27005:2018. Rozsah jednotlivých částí je přizpůsoben velikosti organizace. Měřítko atributů bylo zvolené kvalitativní a pro provedení analýzy rizik byla zvolena kvalitativní metoda. Důvodem pro toto rozhodnutí je malá velikost organizace a nedostatek kvantifikovaných dat k vytvoření spolehlivého měřítka pro zhotovení kvantitativní analýzy. Zodpovědnost za procesy potřebné pro udržení aktuálnosti ISMS bude na provozovateli zdravotnického zařízení, z tohoto důvodu jsem zvolil kvalitativní metodu analýzy rizik pro její nižší náročnost oproti metodě kvantitativní. Data budou získána místním šetření, přístupem do provozní dokumentace, nestrukturovanými rozhovory s pracovníky zdravotnického zařízení a zkušenostmi z provozu tohoto konkrétního zdravotnického zařízení. Metody použité k získání vstupních dat budou uvedeny u jednotlivých podkapitol.

4.1 Stanovení kontextu ISMS

Při návrhu rozsahu ISMS je nutné vzít v úvahu požadavky směrnice GDPR a požadavky na zajištění bezpečnosti informací v ordinaci. Celkový ISMS by byl příliš komplexní a jeho údržba by byla velmi složitá, ne-li nemožná. Proto velmi důležitým požadavkem je zvolit hranice ISMS takovým způsobem, aby byl přehledný, ale aby nedošlo ke ztrátě informací významných pro zhodnocení rizik. Z tohoto důvodu budou provedena dvě opatření. V rámci prvních opatření bude provedena dekompozice systému podle specifických požadavků. Bude vyčleněn zvlášť subsystém ISMS pro zhodnocení a řízení správy osobních údajů podle směrnice GDPR. Pro zpracování tohoto ISMS bude použit standardizovaný formulář publikovaný Českou stomatologickou komorou. Tyto formuláře a související metodika jsou neveřejné, proto je zveřejněna pouze výsledná analýza rizik na přiloženém CD. Vyčleněním zpracování specifických požadavků požadovaných normou GDPR lze zjednodušit ISMS na úroveň komplexnosti, která umožní správu vzniklého systému a zároveň nedojde ke ztrátě vypovídající hodnoty o úrovni rizik. Druhým opatřením bude snaha o minimalizaci počtu aktiv, hrozeb, zranitelností a opatření začleněných do ISMS. O zařazení atributů do analýzy rizik bude rozhodovat aktuální význam pro informační bezpečnost. Tím bude udržena vypovídající hodnota analýzy a kompaktnost ISMS.

4.2 Identifikace aktiv

Identifikace primárních aktiv bude provedena na základě detailní znalosti provozu ordinace (autor je provozovatelem a lékařem ve zdravotnickém zařízení), místním šetřením, studiem provozní dokumentace a dále nestrukturovaným rozhovorem s nositeli výkonů. Následně bude provedena dekompozice identifikovaných primárních aktiv do několika kategorií souhrnných primárních aktiv na základě společných vlastností. V části ISMS pro GDPR bude použit kompletní seznam identifikovaných aktiv a pro analýzu rizik v hlavní části ISMS bude použit seznam souhrnných primárních aktiv. U každého takto identifikovaného souhrnného primárního aktiva bude zaznamenán jeho vlastník/garant. Dále bude provedeno zhodnocení následků v případě narušení důvěrnosti, integrity a dostupnosti primárního aktiva. Na základě možných následků budou jednotlivá souhrnná primární aktiva ohodnocena podle upravených stupnic uveřejněných v příloze číslo 1. vyhlášky č. 82/2018 Sb., viz Tabulka 4.1, Tabulka 4.2, Tabulka 4.3.

Tabulka 4.1: Stupnice pro hodnocení důvěrnosti aktiv zdroj: volně podle [18]

Úroveň	Hodnota	Popis
Nízká	1	Aktiva jsou veřejně přístupná. Narušení důvěrnosti neohrožuje zájmy povinné osoby.
Střední	2	Aktiva nejsou veřejně přístupná. Jejich ochrana není vyžadována právním předpisem nebo smluvním ujednáním
Vysoká	3	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy nebo smluvními ujednáními.
Kritická	4	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany.

Tabulka 4.2: Stupnice pro hodnocení integrity aktiv zdroj: převzato z [18] a upraveno

Úroveň	Hodnota	Popis
Nízká	1	Aktivum nevyžaduje ochranu z hlediska integrity.
Střední	2	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby.
Vysoká	3	Aktiva vyžaduje ochranu z hlediska integrity. Narušení integrity vede k poškození oprávněných zájmů povinné osoby.
Kritická	4	Aktiva vyžaduje ochranu z hlediska integrity. Narušení integrity vede k závažnému poškození oprávněných zájmů povinné osoby.

Tabulka 4.3: Stupnice pro hodnocení dostupnosti aktiv zdroj: vlastní

Úroveň	Hodnota	Popis
Nízká	1	Narušení dostupnosti aktiva i po delší dobu (déle než 1 týden) neomezí provoz ZZ.
Střední	2	Krátkodobé narušení dostupnosti aktiva neomezí provoz ZZ. (do 1 dne)
Vysoká	3	Narušení dostupnosti aktiva omezí poskytování neakutní zdravotní péče ve ZZ.
Kritická	4	Narušení dostupnosti aktiva omezí poskytování akutní zdravotní péče ve ZZ.

Identifikace podpůrných aktiv bude provedena místním šetřením. V průběhu místního šetření bude proveden soupis elektronické informační infrastruktury a infrastruktury používané pro udržování a zpracování informací v listinné formě. U každého takto identifikovaného podpůrného aktiva bude zhodnocen a zaznamenán vztah k souhrnným primárním aktivům a zaznamenán správce aktiva. Hodnota podpůrného aktiva je odvozena od hodnot odpovídajícího primárního aktiva. Hodnocení podpůrného aktiva bude provedeno pomocí stupnic pro hodnocení aktiv uvedených v tabulkách (viz Tabulka 4.1, Tabulka 4.2, Tabulka 4.3). Celková hodnota podpůrného aktiva bude stanovena jako nejvyšší dosažený stupeň mezi hodnotami pro důvěrnost, integritu a dostupnost. K dalším výpočtům bude využita celková hodnota aktiva.

4.3 Identifikace a hodnocení hrozeb

Identifikace hrozeb bude provedena na podkladě informací získaných místním šetřením, zhodnocením přístrojových deníků a nestrukturovaným rozhovorem se všemi pracovníky ordinace. V případě chybějících dat pro hrozby, které nebyly realizovány v tomto konkrétním zdravotnickém zařízení, bude provedený odhad pravděpodobnosti výskytu hrozby na základě dostupné literatury. Pro kybernetické hrozby se jednalo zejména o zdroje [19] a [20], pro hrozbu „nezákonné zpracování dat“ byla analyzována výroční zpráva Úřadu pro ochranu osobních údajů [21]. Tyto zdroje neuvádí úplná data, takže výsledné ohodnocení hrozby je subjektivní.

Na základě těchto údajů bude vypracován katalog hrozeb vycházející z přílohy C normy ČSN ISE/IEC 270005:2019. Jednotlivé záznamy budou ohodnoceny na základě pravděpodobnosti realizace hrozby dle stupnice pro hodnocení pravděpodobnosti hrozeb, viz Tabulka 4.4. Stupnice byla vytvořena úpravou stupnice zveřejněné v příloze č. 1 vyhlášky č. 82/2018 Sb. Hodnocení bude zaznamenáno do katalogu hrozeb. Hrozby, které nepůsobí na žádné aktivum, nebudou do katalogu hrozeb zařazeny.

Tabulka 4.4: Stupnice pro hodnocení hrozeb zdroj: převzato z [18]

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

4.4 Identifikace a zhodnocení zranitelností

Ve chvíli, kdy je k dispozici katalog aktiv a katalog hrozeb, lze přistoupit ke identifikaci zranitelností. Identifikace bude provedena na základě seznamu aktiv a katalogu hrozeb. Takto identifikované zranitelnosti budou zaznamenány do seznamu zranitelností.

V dalším kroku bude následovat identifikace bezpečnostních opatření. V rámci tohoto kroku budou zadokumentována v současnosti realizovaná bezpečnostní opatření zavedená ke zmírnění dopadů hrozeb na aktiva. Identifikace bezpečnostních opatření bude provedena na základě informací zjištěných při místním šetření, studiem dokumentace (pracovní smlouvy včetně dodatků, vnitřní směrnice) a nestrukturovaného rozhovoru s pracovníky. Zjištěná bezpečnostní opatření budou zaznamenána do seznamu zranitelností.

Ohodnocení zranitelnosti se provede ve vztahu k podpůrnému aktivu. Při hodnocení zranitelnosti bude brána v úvahu schopnost detekce útoku a účinnost přijatých bezpečnostních opatření. K hodnocení bude použito stupnice pro hodnocení zranitelností dle přílohy č. 1 vyhlášky č. 82/2018 Sb., viz Tabulka 4.5 Seznam zranitelností bude obsahovat název zranitelnosti, působící hrozbu, ovlivněné aktivum a ohodnocení stupně zranitelnosti.

Tabulka 4.5: Stupnice pro hodnocení zranitelností zdroj: převzato z [18]

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

4.5 Zhodnocení rizika

Zhodnocení rizika bude realizováno výpočtem dle vzorce pro výpočet míry rizika, viz Rovnice 4.1 Výsledná míra rizika (R) je kombinací hodnoty aktiva (A), pravděpodobnosti hrozby (T) a úrovně zranitelnosti (V). Výpočet proběhne podle vzorce:

$$R = A * T * V$$

Rovnice 4.1: Vzorec pro výpočet míry rizika

Míra rizika tak může nabývat hodnot <1-64>. Na základě míry rizika lze zařadit rizika do jednotlivých úrovní, které jsou uvedeny v tabulce, viz Tabulka 4.6.

Tabulka 4.6: Stupnice pro ohodnocení rizika zdroj: vlastní

Úroveň	Míra rizika	Popis
Nízká	<1-15>	Přijatelné riziko
Střední	<16-31>	Střední riziko
Vysoká	<32-47>	Vysoké riziko
Kritická	<48-64>	Nepřípustné riziko

Nízká úroveň rizika – Jedná se o přijatelné riziko. Není nutné zavádět nová bezpečnostní opatření nebo upravovat stávající.

Střední úroveň rizika – Jedná se o úroveň rizika, kterou lze v krátkodobém časovém horizontu tolerovat, ale měla by být navržena bezpečnostní opatření ke snížení rizika. V případě vysoké náročnosti navržených opatření, nebo různých omezení na straně organizace lze střední úroveň rizika akceptovat i dlouhodobě.

Vysoká úroveň rizika – Riziko je v dlouhodobém časovém horizontu nepřípustné a je nutné navrhnout a provést bezpečnostní opatření k jeho snížení.

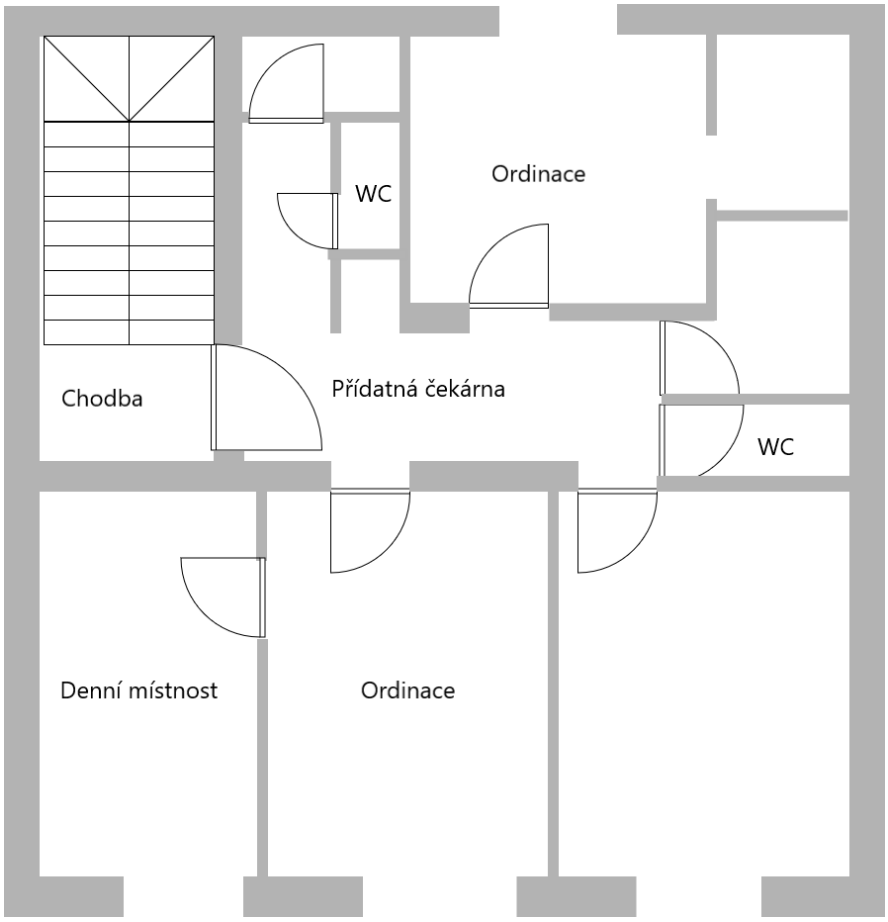
Kritická úroveň rizika – Riziko kritické úrovně není přípustné ani z krátkodobého pohledu a je nutné neprodleně zavést bezpečnostní opatření ke snížení rizika.

Rizika úrovně střední, vysoká nebo kritická budou uvedena v katalogu rizik s navrženým bezpečnostním opatřením ke zvládnutí rizika. Mezní hranice míry rizika 16 byla zvolena jako referenční hodnota, které dosáhne velmi hodnotné aktivum (A=4) ovlivněné velmi pravděpodobnou hrozbou (T=4) při velmi dobrých bezpečnostních opatřeních a tím pádem minimální úrovní zranitelnosti (V=1).

5 Analýza rizik

5.1 Kontext organizace

Ordinace MDDr. Vojtěch Boček je malé zdravotnické zařízení zabývající se poskytováním zdravotních služeb. Ordinace se nachází v třípatrovém objektu, ve kterém sídlí i další poskytovatelé zdravotních služeb. Provoz zdravotnických zařízení je koordinován, aby byla sjednocena provozní doba. Mimo provozní dobu je celý komplex uzamčený a nepřístupný veřejnosti. Zdravotnická zařízení sdílí i část provozních prostor: hlavní čekárnu, recepci, šatny a hygienická zařízení. Provozní prostory ordinace se nachází v prvním a druhém poschodí budovy, viz Obrázek 5.1. Prostory jsou členěné na tři zóny: veřejnou, provozní a soukromou zónu. Jednotlivé zóny jsou od sebe stavebně odděleny a průchod je možný přes uzamykatelné dveře. Veřejnou zónu tvoří chodby, hygienická zařízení a přídatné čekárny. Veřejné zóny jsou volně přístupné během provozní doby ordinace, mimo pracovní dobu jsou uzamčené.



Obrázek 5.1: Plán druhého podlaží ordinace zdroj: vlastní

Provozní zónu tvoří jednotlivé ordinace a hlavní čekárna. Do prostoru ordinací je přístup umožněn pouze pracovníkům ordinace a veřejnosti pouze v doprovodu pověřeného pracovníka. Do hlavní čekárny je povolen přístup pouze, pokud je přítomný pověřený pracovník.

Soukromá zóna je tvořena denní místností, do které nemá veřejnost přístup. V denní místnosti je umístěn i server a spisová skříň na dokumenty. Do soukromé zóny mají přístup pouze pověření pracovníci.

Ordinace je tvořena 4 pracovníky. Lékařem, zubní asistentkou, dentální hygienistkou a recepční. Úklid je zajištěn externě na úrovni objektu. Povinnosti pracovníka provádějícího úklid jsou ošetřeny zvlášť smlouvou mezi ordinací a pracovníkem provádějícím úklid.

Zdravotnická dokumentace je vedena v kombinované formě. Zdravotní textový záznam vzniká v elektronické podobě v ordinačním programu Hobosoft Stomatolog a po ukončení zápisu je vytištěn a uložen do karty pacienta. Software Stomatolog splňuje podmínky pro čistě elektronické vedení zdravotnické dokumentace, tak je elektronická forma zdravotního záznamu uchovávána pro případ zničení listinné formy zdravotnické

dokumentace. Obrazová část zdravotního záznamu (tvořená převážně rentgenovými snímky) vzniká a je uchovávána čistě v elektronické formě. Ke správě obrazové části zdravotnické dokumentace je využit program ezDent-i od firmy Vatech a program DBSWIN od firmy Dürr. U všech třech programů používaných pro vedení zdravotnické dokumentace jsou nastaveny přístupové účty s přístupovými právy odpovídajícími pracovní funkci chráněné heslem. Politika hesel je pouze verbálně doporučena, není dána metodikou a kontrola je ponechána na uživateli.

Infrastruktura informačního systému je tvořena centrálním serverem, modemem, switchem a pracovními stanicemi. Pracovní stanice v ordinaci lékaře plní funkce serveru pro ordinační software. Rozvody místní sítě jsou vedeny pod podlahou, ve zdech nebo v podhledu. Zálohovaní je prováděno minimálně 1x za den, záložní disky se uchovávají v blízkosti zálohovaných serverů a pracovních stanic. Offsite záloha je prováděna 1x za týden. Zálohovací disky používané pro offsite zálohu jsou umístěné mimo budovu zdravotnického a do ordinace jsou přesouvány pouze pro účel provedení zálohy. Archivní kopie jsou vytvářené 1x za rok a jsou uložené ve spisové skříní v denní místnosti. Inventarizace záložních médií není prováděna.

Zdravotní karty (listinná forma zdravotnické dokumentace) se nacházejí v uzamykatelné kartotéce, která je umístěna v soukromé části velké čekárny. Zdravotní karty jsou uchovávány v zamčené kartotéce. V případě, že je potřeba práce se zdravotní kartou, je zdravotní karta pacienta vyndána z kartotéky a předána lékaři. Obvykle na konci směny jsou karty přeneseny z ordinací zpět do kartotéky. Tento doporučený postup je předáván verbálně, metodika na zacházení s kartou pacienta není zpracována. Provozní dokumentace vztahující se k běžnému provozu ordinace (provozní listy přístrojů, kniha závad a servisních zásahů apod.) je umístěna v jednotlivých ordinacích. Provozní dokumentace týkající se celé ordinace je umístěna ve spisové skříni v denní místnosti. Záložní kopie se nacházejí mimo prostory ordinace.

5.2 Aktiva

Po identifikaci primárních aktiv byla primární aktiva seskupena do třech souhrnných primárních aktiv podle svých podobných vlastností. Úplný seznam identifikovaných primárních aktiv byl využit pro zhodnocení rizik v rámci části ISMS vztahující se k GDPR. V hlavní částí analýzy rizik byl využitý seznam souhrnných primárních aktiv. Dekompozice identifikovaných primárních aktiv na souhrnná primární aktiva je uvedena v tabulce, viz Tabulka 5.1

Tabulka 5.1: Dekompozice primárních aktiv zdroj: vlastní vypracování

Identifikované primární aktivum	Souhrnné primární aktivum
Zdravotnická dokumentace	Zdravotní záznam
Výkazy poskytnutých hrazených služeb	Mzdové a účetní záznamy
Finanční doklady	
Mzdová agenda	
Evidence a hlášení nežádoucích účinků	
Osobní spisy zaměstnanců	
Veřejná provozní dokumentace	Provozní dokumentace
Přístrojové deníky, karta přístroje	
Záznamy o provedených školeních	
Evidence případů porušení zabezpečení osobních údajů	

Souhrnná primární aktiva byla ohodnocena dle stupnic uvedených v metodice, viz kapitola 4.2, byl zaznamenán garant aktiva a výsledky byly zaznamenány do tabulky, viz Tabulka 5.2

Tabulka 5.2: Hodnocení souhrnných primárních aktiv zdroj: vlastní vypracování

Název	Garant	Hodnota	Důvěrnost	Integrita	Dostupnost
Zdravotní záznam	Nositel výkonů	4	4	4	3
Mzdové a účetní záznamy	Provozovatel	4	4	4	2
Provozní dokumentace	Provozovatel	3	2	3	2

Podpůrná aktiva byla ohodnocena pomocí stejných pravidel dle metodiky, bylo zaznamenáno odpovídající primární aktivum a výsledky zaznamenány do tabulky, viz Tabulka 5.3. Aktiva mohou nabývat hodnot od 1 (nízká hodnota aktiva) do 4 (kritická hodnota aktiva).

Tabulka 5.3: Hodnocení podpůrných aktiv zdroj: vlastní vypracování

Název podpůrného aktiva	Primární aktivum	Hodnota	Důvěrnost	Integrita	Dostupnost
Zdravotní záznam – elektronická verze	Zdravotní záznam	4	4	4	3
Zdravotní záznam – fyzická verze	Provozovatel	4	4	4	3
Mzdové a účetní záznamy	Mzdové a účetní záznamy	4	4	4	2
Provozní dokumentace	Provozní dokumentace	3	2	3	2
Záložní kopie	Zdravotní záznam	4	4	4	3
	Mzdové a účetní záznamy		4	4	2
	Provozní dokumentace		2	3	2
Server HP	Zdravotní záznam	4	4	3	2
Pracovní stanice – server	Zdravotní záznam	4	4	3	3
Pracovní stanice – klient	Zdravotní záznam	3	3	3	2
Modem ASUS	Zdravotní záznam	2	2	2	2
Switch NETGEAR	Zdravotní záznam	2	1	1	2
Kartotéka	Zdravotní záznam	4	4	4	3
Zálohovací média	Zdravotní záznam	4	4	4	3
	Mzdové a účetní záznamy		4	4	2
Windows server 2012	Zdravotní záznam	3	3	3	3
Windows 10	Zdravotní záznam	4	4	3	3
Software Stomatolog	Zdravotní záznam	4	4	4	2
Software Vatech	Zdravotní záznam	3	3	3	2
Software Dürr	Zdravotní záznam	3	3	3	2

5.3 Hrozby

Tabulka hrozeb zobrazuje identifikované hrozby a jejich odhadnutou pravděpodobnost realizace, viz. Tabulka 5.4. Nebyla identifikována žádná hrozba kritické úrovně. Hrozby s vysokou pravděpodobností realizace byly identifikovány tři:

- Ztráta dodávky energie – Pravděpodobnost realizace hrozby byla odvozena z historických dat. V provozním deníku bylo zaznamenáno 5 incidentů ztráty dodávek elektrické energie za 8 let, ale do provozních deníků nejsou zaznamenány události, které proběhly mimo ordinační dobu. Z logů serveru lze dohledat další incidenty, proto byla pravděpodobnost realizace hrozby odhadnuta častější než 1x za rok.
- Nezákonné zpracování dat – Za celou dobu provozu ordinace nebyl v evidenci případů porušení zabezpečení údajů zaznamenán žádný bezpečnostní incident. Absenci manifestovaného bezpečnostního incidentu lze vysvětlit obtížnou detekcí porušení pravidel pro ochranu osobních údajů

malého rozsahu. Z tohoto důvodu byla pravděpodobnost realizace hrozby stanovena odhadem.

- Zneužití přístupových práv – Podobně jako u předchozí hrozby nikdy nebyl zaznamenán bezpečnostní incident zneužití přístupových práv. Shodná s předchozí hrozbou je i obtížnost detekce bezpečnostních incidentů malého rozsahu. Z tohoto důvodu byla pravděpodobnost realizace hrozby stanovená odhadem.

Tabulka 5.4: Hodnocení hrozeb zdroj: vlastní vypracování

Název	Pravděpodobnost výskytu
Poškození ohněm	1
Poškození vodou	1
Zničení zařízení nebo médií	2
Ztráta dodávky energie	3
Přerušení přístupu k internetu	2
Neoprávněný přístup – fyzický	1
Neoprávněný přístup – dálkový	1
Odposlech	1
Nedostupnost dat	2
Technické selhání	2
Zneužití přístupových práv	3
Neúmyslné poškození dat	2
Nezákonné zpracování dat	3

5.4 Zranitelnosti a současná opatření

Z možných interakcí hrozeb a aktiv byla sestavena matice zranitelností, viz Tabulka 5.6, a jednotlivé zranitelnosti byly zaznamenány do katalogu zranitelností. Poté byl k jednotlivým zranitelnostem doplněn záznam o současných bezpečnostních opatření. Na základě metodiky, viz Kapitola 4.4, byly jednotlivé zranitelnosti ohodnoceny. Příklad záznamu je uvedený v tabulce, viz Tabulka 5.5. Úplný katalog zranitelností a bezpečnostních opatření lze dohledat na přiloženém CD.

Tabulka 5.5: Příklad záznamu v katalogu zranitelností zdroj: vlastní vypracování

Hrozba	Aktivum	Název zranitelnosti	Stupeň zranitelnosti	Současná opatření
Poškození ohněm	Zdravotní záznam – fyzický	Náchylnost papírové dokumentace k poškození přírodními živly	2	Prostory vybavené odpovídajícími hasícími přístroji. Pravidelné revizní prohlídky.
	Účetní a mzdové doklady		1	
	Provozní dokumentace		1	
	Záložní kopie		1	
	Kartotéka		1	

Matice zranitelností zobrazuje vztah aktiv a hrozeb na ně působící, viz Tabulka 5.6. Hodnoty zaznamenané v matici jsou stupně zranitelnosti přiřazené jednotlivým zranitelnostem.

Tabulka 5.6: Matice zranitelností zdroj: vlastní vypracování

Míra zranitelnosti [V]	Aktivum	Zdravotní záznam - elektronický	Zdravotní záznam - fyzický	Účetní a mzdové doklady	Provozní dokumentace	Záložní kopie	Server HP	Pracovní stanice server	Pracovní stanice - klient	Modem Asus	Switch Netgear	Kartotéka	Zálohovací média	Windows Server	Windows 10	Software Stomatolog	Software Vatech	Software Dürr
	A	4	4	4	3	4	4	4	3	2	2	4	4	3	4	4	3	3
Hrozba	T																	
Poškození ohněm	1		2	1	1	1	2	2	2	3	2	1	2					
Poškození vodou	1		2	1	1	1	1	2	2	3	1	1	1					
Zničení zařízení/médií	2						2	2	2	3	1		3					
Ztráta dodávky energie	3						1	3	3		3							
Přerušení přístupu k internetu	2									2								
Neoprávněný přístup - fyzický	1		3	1	1	1	1	2	2	3	1	2	2					
Neoprávněný přístup dálkový	1									2				1	1	1		
Odposlech	1		3	1						2				1	1			
Nedostupnost dat	2						2	2										
Technické selhání	2						3	3	2	2	1		3					
Zneužití přístupových práv	3													1	1	1	2	2
Neúmyslné poškození dat	2		1	1	1	1								1	3	1	1	2
Nezákonné zpracování dat	3	3	2	1	1	1										3	2	2

5.5 Matice rizik

Pro vypočtení míry rizika byl použit vzorec uvedený v metodice, viz Rovnice 4.1. Míra rizika je zaznamenána do matice rizik.

Tabulka 5.7: Matice rizik zdroj: vlastní vypracování

Míra rizika [R]	Aktivum	Zdravotní záznam - elektronický	Zdravotní záznam - fyzický	Účetní a mzdové doklady	Provozní dokumentace	Záložní kopie	Server HP	Pracovní stanice server	Pracovní stanice - klient	Modem Asus	Switch Netgear	Kartotéka	Zálohovací média	Windows Server	Windows 10	Software Stomatolog	Software Vatech	Software Dürr
	A	4	4	4	3	4	4	4	3	2	2	4	4	3	4	4	3	3
Hrozba	T																	
Poškození ohněm	1		8	4	3	4	8	8	6	6	4	4	8					
Poškození vodou	1		8	4	3	4	4	8	6	6	2	4	4					
Zničení zařízení/médií	2						16	16	12	12	4		24					
Ztráta dodávky energie	3						12	36	27		18							
Přerušení přístupu k internetu	2									8								
Neoprávněný přístup - fyzický	1		12	4	3	4	4	8	6	6	2	8	8					
Neoprávněný přístup dálkový	1									4				3	4	4		
Odposlech	1		12	4						4				3	4			
Nedostupnost dat	2						16	16										
Technické selhání	2						24	24	12	8	4		24					
Zneužití přístupových práv	3													9	12	12	18	18
Neúmyslné poškození dat	2		8	8	6	8								6	24	8	6	12
Nezákonné zpracování dat	3	36	24	12	9	12										36	18	18

5.6 Výsledek analýzy rizik

Analýza rizik neodhalila žádné riziko, které by bylo zařazeno do kategorie kritických rizik. Vysoké riziko bylo odhaleno v oblasti působení hrozby „Nezákonné zpracování dat“ a „Ztráta dodávky energie“. Každé riziko, u kterého vyšla míra rizika větší než 15, bylo zařazeno do katalogu rizik a bylo navrženo opatření na jeho snížení.

5.7 Navržená opatření

5.7.1 Metodika pro zacházení s osobními údaji

Hrozby: nezákonné zpracování dat

Zranitelnosti: nedostatečné poučení pracovníků

Cíl: snížit riziko porušení právních předpisů na ochranu osobních údajů

Opatření: vypracovat metodiku pro zacházení s osobními údaji, provést školení pracovníků a absolvované školení řádně zadokumentovat

Zdůvodnění: V současnosti jsou pravidla pro zacházení s osobními údaji v ordinaci předávána verbálně a toto vzdělávání nemá pevně daný rámec. Současnou úpravu nelze brát jako uspokojující ze dvou důvodů. Prvním důvodem je, že při nesystémovém „ad hoc“ vzdělávání pracovníků nelze kontrolovat úplnost poučení v pravidlech a procesech zajišťujících zpracování osobních údajů v souladu s právními předpisy. Druhým důvodem je, že při případném bezpečnostním incidentu by provozovatel musel prokázat, že pracovník byl řádně proškolen a poučen. Toto dokazování je při proškolování čistě verbální formou značně ztížené. Z těchto důvodů je vhodné vypracovat metodiku obsahující popis procesů a pravidel pro nakládání s osobními údaji a seznámení pracovníka s touto metodikou zaznamenat písemně.

5.7.2 Metodika zálohování, plánu obnovy a inventury záloh

Hrozby: zničení zařízení/médií, neúmyslné poškození dat, nedostupnost dat, technické selhání

Zranitelnosti: nedostatečná kontrola stavu elektronických zařízení, nedostatečné řízení přístupových práv, nedostatečné zajištění alternativního zdroje dat, nedostatečná kontrola stavu součástí informačního systému

Cíl: zajistit dostupnost dat během bezpečnostních incidentů

Opatření: vypracovat metodiku zálohování, vypracovat plán obnovy a provést inventuru záloh

Zdůvodnění: Toto opatření má za cíl snížení dopadů celé řady hrozeb. Opatření necílí na jednotlivé zranitelnosti, ty by bylo možné ošetřit adresněji, ale narážíme zde na personální omezení ordinace. Například pravidelná kontrola stavu jednotlivých elektronických zařízení a provádění pravidelného testování by jistě lépe ošetřilo zranitelnost „nedostatečná kontrolo stavu elektronických zařízení“ nebo „nedostatečná kontrola stavu součástí informačního systému“, ale provádění kontrol v dostatečné četnosti a rozsahu pro identifikaci selhávajících zařízení by neúměrně zatížilo správce zařízení. Z tohoto důvodu se jeví robustní systém záloh a připravený plán obnovy jako vhodnější řešení pro toto zdravotnické zařízení. Metodika pro zálohování a plán obnovy by měly mít písemnou formu, aby i v případě nepřítomnosti pracovníka zodpovědného za zálohování nebo obnovu dat bylo možné potřebné činnosti provést jiným pracovníkem.

5.7.3 Zajištění alternativního zdroje napájení

Hrozby: ztráta dodávky elektrické energie

Zranitelnosti: nedostatečné zajištění elektronických zařízení při výpadku elektrické sítě

Cíl: zajistit integritu zpracovávaných dat v době přerušení dodávky elektrické energie

Opatření: vybavit prvky informační infrastruktury zdrojem elektrické energie dostatečným pro bezpečné vypnutí v případě přerušení dodávky elektrické energie

Zdůvodnění: V případě ztráty napájení během zpracování elektronických dat může dojít k poškození ukládaného datového souboru. Proto je nutné vybavit prvky infrastruktury zařízením UPS (uninterruptible power supply – zdroj nepřerušovaného napětí). Kapacita UPS musí být dostatečná na bezpečné vypnutí.

5.7.4 Politika hesel

Hrozby: zneužití přístupových práv

Zranitelnost: nedostatečná autentizace

Cíl: stanovit jasná pravidla pro tvorbu a užívání hesel a prokazatelně s ní seznámit pracovníky

Opatření: vypracovat politiku hesel, provést školení zaměstnanců a zadokumentovat absolvování školení

Zdůvodnění: Pokud to používaný software umožňuje, měla by být pravidla pro tvorbu a výměnu hesel stanovena centrálně a hlídána automaticky. Bohužel ne každý software používaný v ordinaci toto umožňuje. Z tohoto důvodu je vhodné stanovit metodiku upravující tvorbu, výměnu a používání hesel ve zdravotnickém zařízení. Tato metodika by měla vycházet z doporučení NÚKIB [22], čímž lze dosáhnout dosažení standardní úrovně bezpečnosti hesel. Zpracování metodiky pro správu hesel, provádění pravidelných školení a dokumentace seznámení pracovníků s pravidly pro tvorbu hesel se jeví v současné době jako vhodné řešení pro danou ordinaci. Ideálním řešením by bylo přejít na jiný způsob autentizace, a to buď biometricky, nebo pomocí certifikátu. Zavedení alternativních způsobů autentizace v současnosti naráží na technická omezení, zejména se jedná o nemožnost integrování těchto systémů do programového vybavení ordinace.

6 Diskuse

Z provedeného šetření lze odvodit, že zkoumané zdravotnické zařízení splňuje minimální zákonné požadavky na zabezpečení zdravotnické dokumentace. Splnění zákonných požadavků však nelze považovat za důkaz optimalizace rizik. Provedená analýza rizik odhalila několik oblastí, ve kterých lze provést bezpečnostní opatření, a tak zlepšit úroveň zabezpečení dat. Hlavní část zjištěných rizik vycházela ze způsobu poučení pracovníků ohledně procesů k zajištění bezpečnosti informací. Tato poučení byla vydávána převážně verbálně, nesystematicky a bez zadokumentování o provedení těchto školení. Tento nesystematický „ad hoc“ přístup k zajištění bezpečnosti informací je poměrně rozšířenou praxí v malých zdravotnických zařízeních. Malá zdravotnická zařízení obvykle naráží na výrazná personální omezení při zajišťování bezpečnosti informací. V malých zdravotnických zařízení je obvykle správcem ISMS sám provozovatel a pouze dílčí specializované úkony (např. instalace ordinačního softwaru) jsou zajištěny externě. Vzhledem k podobnému charakteru malých zdravotnických zařízení lze vypracovanou metodiku pouze s drobnými úpravami použít pro jiné podobné zdravotnické zařízení.

Při zpracování práce jsem narazil na několik problémů. Obtížným problémem bylo stanovení hranic ISMS. Bylo nutné navrhnout hranice ISMS tak, aby systém pokryl všechna důležitá rizika, a zároveň tak, aby byl ISMS v praxi použitelný a udržovatelný. Řešením bylo vyčlenit subsystém pro zpracování analýzy rizik zvlášť pro potřeby splnění požadavků normy GDPR. Tímto krokem došlo k vyčlenění části systému, která má velmi podobný charakter s jinými stomatologickými ordinacemi, a proto pro její zpracování šlo využít standardního postupu doporučeným Českou stomatologickou komorou. Tento výstup je na přiloženém CD. Vyčleněním subsystému pro splnění specifických požadavků stanovených normou GDPR vznikl kompaktní ISMS pro hlavní část práce.

Při zpracování metodiky pro analýzu rizik jsem vycházel z norem rodiny ČSN/ISO 27xxx a přílohy č. 1 vyhlášky č. 82/2018 Sb. Volba těchto dvou zdrojů umožnila vytvoření rámce analýzy rizik, který lze snadno modifikovat a využít pro další iterace cyklu řízení informační bezpečnosti.

Analýza rizik odhalila některá střední a vysoká rizika, viz Kapitola 5.6. Na každé takto identifikované riziko jsem návrh bezpečnostního opatření. Posledním úkolem práce bylo vypracovat podklady k navrženým bezpečnostním opatřením. Podklady pro bezpečnostní opatření mají formu bezpečnostní směrnice. Při vypracování směrnice byl kladen důraz na srozumitelnost a jednoduchou formou. Bezpečnostní směrnice je rozčleněna na dvě části: směrnice pro zacházení s osobními údaji a směrnice pro zálohování a obnovu dat. Bezpečnostní směrnice má tři přílohy: analýza rizik – GDPR, politika hesel a katalog dat k zálohování. Bezpečnostní směrnice je na přiloženém CD.

Dalším podstatným zjištěním bylo, že charakter malých zdravotnických zařízení je v mnoha aspektech velmi podobný. Toho lze využít při zajišťování bezpečnosti ve zdravotnictví. Připravením standardizovaných postupů nebo formulářů, jako tomu je u materiálů pro splnění povinností vyplývajících z normy GDPR poskytnutých Českou stomatologickou komorou, lze výrazně usnadnit řízení informační bezpečnosti v jednotlivých malých zdravotnických zařízeních. Proto byla vypracovaná bezpečnostní směrnice koncipována tak, aby jí bylo možné snadno modifikovat pro jiná zdravotnická zařízení.

7 Závěr

Hlavním tématem této bakalářské práce byla bezpečnost informací v malém zdravotnickém zařízení.

V teoretické části této bakalářské práce byl proveden nejprve přehled legislativy, která upravuje sběr, zpracování, uchovávání a vyřazování osobních údajů. A poté byl zpracován úvod do problematiky vedení zdravotnické dokumentace a řízení rizik informační bezpečnosti.

V praktické části jsem vycházel z teoretického základu z první části práce. Hlavním úkolem praktické části bylo provedení analýzy rizik v oblasti informační bezpečnosti. Předmětem analýzy rizik byla konkrétní stomatologická ordinace. Vlastní analýze předcházel sběr dat místním šetřením, studiem dokumentace a sérií rozhovorů s pracovníky ordinace. Na základě získaných vstupních dat byla provedena identifikace a zhodnocení aktiv, hrozeb a zranitelností. Následovala kalkulace míry rizika a zadokumentování rizik, které dosáhly střední, vysoké nebo kritické úrovně.

V poslední části práce jsem pro identifikovaná rizika navrhnul bezpečnostní opatření ke snížení rizika. Nakonec jsem pro navržená bezpečnostní opatření zpracoval podklady k jejich zavedení.

Z výsledků provedené analýzy lze konstatovat, že zkoumané zdravotnické zařízení splňuje zákonné požadavky na zajištění bezpečnosti informací. Byla však identifikována rizika, jejichž eliminací by se úroveň bezpečnosti dala zlepšit. Na identifikovaná rizika byla navržena protiopatření. Tato bezpečností opatření byla směřována zejména k větší systemizaci informační bezpečnosti v ordinaci a k řádné dokumentaci a kodifikaci bezpečnostních procesů.

Praktická část práce byla zpracována pro případ reálné stomatologické ordinace. Tato ordinace je typickým zástupcem malého zdravotnického zařízení. Vzhledem k podobnému charakteru malých zdravotnických zařízení v segmentu ambulantní péče, lze předpokládat, že zvolené postupy pro zajištění informační bezpečnosti lze aplikovat i na jiná zdravotnická zařízení podobného charakteru.

Citovaná literatura

[1] Uniklá SMS pro Babiše: specialista vyloučil, že Zeman potřebuje transplantaci jater, napsal poslanec Špičák. In: *IROZHLAS* [online]. Praha [cit. 2022-05-10]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/milos-zeman-sms-transplantace-vojenska-nemocnice-hospitalizace-andrej-babis_2110161910_zpo

[2] Celkový přehled zdravotnických zařízení. In: *Ústav zdravotnických informací a statistiky České republiky: Regionální zpravodajství Národního zdravotnického informačního systému* [online]. Praha: ÚZIS ČR, 2016 [cit. 2022-05-05]. Dostupné z: https://reporting.uzis.cz/cr/index.php?pg=statisticke-vystupy--infrastruktura-zdravotni-pece--prehled-zdravotnickych-zarizeni--celkovy-prehled-zdravotnickych-zarizeni

[3] *Důvodová zpráva k zákonu č. 326/2021 Sb., změna některých zákonů v souvislosti s přijetím zákona o elektronizaci zdravotnictví*. In: . Praha, 2021, ročník 2021. Dostupné také z: https://www.psp.cz/sqw/text/orig2.sqw?idd=184747

[4] ZACHA, Ondřej. Náměstek NÚKIB Kintr: Vakcína proti Covidu je pro útočníky horké zboží. Bezpečnost nemocnic jsme podcenili. *Voxpot* [online]. [cit. 2022-05-06]. Dostupné z: https://www.voxpot.cz/namestek-nukib-kintr-kybernetickou-bezpecnost-nemocnic-jsme-podcenili/

[5] ZVÁROVÁ, Jana, Lenka LHOTSKÁ, Vladimír PŘIBÍK et al. *Biomedicínská informatika IV.: Data a znalosti v biomedicíně a zdravotnictví*. 1. vyd. Praha: Karolinum, 2010. Biomedicínská informatika. ISBN 978-80-246-1805-0.

[6] Zvláštní kategorie osobních údajů. In: *Ministerstvo vnitra České republiky* [online]. Ministerstvo vnitra České republiky [cit. 2022-05-10]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zvlastni-kategorie-osobnich-udaju.aspx

[7] Základní pojmy v GDPR. In: *Ministerstvo vnitra České republiky* [online]. Ministerstvo vnitra České republiky [cit. 2022-05-10]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

[8] POLČÁK, Radim, Leoš ŠEVČÍK, Michal KOŠČÍK, Jakub KLODWIG a Petr HOLUB. *Metodika: GDPR a výzkumná data v prostředí vysokých škol v*

ČR [online]. První. [cit. 2022-05-10]. Dostupné z: doi:10.5281/zenodo.2532860

[9] *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. Praha: Verlag Dashöfer, 2018. ISBN 978-80-87963-54-8.

[10] *ČSN EN ISO/IEC 27000 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Páté vydání. [Praha]: Česká agentura pro standardizaci, 2020.

[11] POŽÁR, Josef. *Informační bezpečnost*. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

[12] 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.

[13] *ČSN ISO/IEC 27005 (36 9790) Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Třetí vydání. [Praha]: Česká agentura pro standardizaci, 2019.

[14] POŽÁR, Josef, ed. Vybrané hrozby informační bezpečnosti organizace. In: KNÝ, Milan. *Kybernetická bezpečnost: sborník příspěvků z bezpečnostního semináře Policejní akademie a evropského vedení AFCEA konaného dne 12. dubna 2011 na Policejní akademii České republiky v Praze [CD-ROM]*. Vyd. 1. Praha: Policejní akademie České republiky, 2011. ISBN 978-80-7251-347-5.

[15] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[16] POŽÁR, Josef, Luděk NOVÁK, ed. Systém řízení informační bezpečnosti. In: KNÝ, Milan. *ISMS (ISO 2700x): Sborník příspěvků z bezpečnostního semináře Policejní akademie a evropského vedení AFCEA konaného 22. září 2011 na Policejní akademii České republiky v Praze*. Vyd. 1. Praha: Policejní akademie České republiky, 2011. ISBN 978-80-7251-356-7.

[17] *ČSN EN ISO 27799:2019: Zdravotnická informatika - Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002*. Druhé vydání. Česká agentura pro standardizaci, 2019.

[18] *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)*. In: . Praha: Ministerstvo vnitra ČR, 2018, ročník 2018, číslo 82.

[19] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2022-05-10]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

[20] MAMRILLA, Filip a Šimon TOMAN. Kybernetická bezpečnost ve zdravotnictví. In: *Epravo.cz* [online]. 2021 [cit. 2022-05-10]. Dostupné z: https://www.epravo.cz/top/clanky/kyberneticka-bezpecnost-ve-zdravotnictvi-112849.html

[21] PATÁK, Tomáš, ed. *Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2021* [online]. Praha: Úřad pro ochranu osobních údaj, 2022 [cit. 2022-05-10]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=55760

[22] NÚKIB, , NAKIT a MINISTERSTVO VNITRA ČR. *Minimální bezpečnostní standard* [online]. Verze 1.0. Národní úřad pro kybernetickou a informační bezpečnost, 2020 [cit. 2022-05-06]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf

[23] TĚŠITELOVÁ, Vladimíra, Radek POLICAR, Milan BLAHA, Daniel KLIMEŠ a Ladislav DUŠEK. *Jak implementovat nařízení evropského parlamentu a rady (EU) 2016/679*. Vydání první. Praha: Ministerstvo zdravotnictví ČR, 2018. ISBN 978-80-85047-55-4.

Příloha A: Bezpečnostní směrnice

Směrnice k zajištění informační bezpečnosti

Obsah

1 Úvodní ustanovení

Tento dokument stanovuje pravidla a pracovní postupy pro zajištění informační bezpečnosti ve zdravotnickém zařízení.

1.1 Oblast platnosti

Pracovní postupy jsou závazné pro všechny osoby vykonávající činnosti pro poskytovatele na základě smluvního vztahu s poskytovatelem.

2 Směrnice pro nakládání s osobními údaji

2.1 Účel

Tato nařízení upravují postup pracovníků při zpracování osobních údajů. Účelem je zajistit ochranu osobních údajů při jejich zpracování.

2.2 Definice pojmů

Informační aktivum – statek s hodnotou pro organizaci

Osobní údaj – neveřejná informace týkající se identifikovatelné žijící osoby

Zdravotnická dokumentace – soubor osobních údajů potřebný k poskytování zdravotních služeb

Karta pacienta – část zdravotnické dokumentace uchovávaná v listinné formě

Elektronický zdravotní záznam – část zdravotnické dokumentace uchovávaná v elektronické formě

Riziko – Existence možnosti výskytu nežádoucí události

2.3 Povinnosti pracovníků

2.3.1 Základní zásady práce s osobními údaji

1) Pracovník povinen seznámit se se „záznamy o činnostech zpracování“ a zpracovávat osobní údaje pouze v souladu s tímto dokumentem.
2) Při pochybnostech o zařazení informačního aktiva je pracovník povinen kontaktovat správce a dotázat se na kategorii a způsob zacházení s aktivem.
3) Přístup ke zdravotnické dokumentaci mají pouze osoby ustanovené zákonem č. 372/2011 Sb. – dále jen „pověřené osoby“
4) Nakládat se zdravotnickou dokumentací lze pouze podle příslušných právních předpisů

5) Pracovník má povinnost hlásit každé narušení bezpečnosti nebo podezření na narušení bezpečnosti provozovateli.

2.3.2 Povinnosti pracovníků – listinná forma zdravotnické dokumentace

1) Karta pacienta je uchovávána v zamčené kartotéce
2) Přístup ke kartě pacienta mají pouze pověřené osoby
3) Po vyjmutí karty z kartotéky musí být karta vždy pod dohledem pověřené osoby.
4) Po ukončení práce s kartou pacienta je nutné vrátit zpět do kartotéky nebo předat jiné pověřené osobě.

2.3.3 Povinnosti pracovníků – elektronický zdravotní záznam

1) K přístupu k elektronickému zdravotnímu záznamu využívá pracovník jen zařízení výslovně k tomu určená poskytovatelem
2) Pracovník se do zařízení a programů hlásí pouze svým uživatelským účtem
3) Přístup k zařízení musí být chráněn heslem. Stejně tak i přístup do jednotlivých programů (Stomatolog, ezDent-i, Dürr). Pracovník je povinen řídit se politikou hesel uvedenou v příloze č. 2.
4) Po ukončení práce s elektronickým zdravotním záznamem nebo při opuštění pracoviště je pracovník povinen provést odhlášení.

2.3.4 Povinnosti – osobní údaje nespadající do zdravotnické dokumentace

1) Přístup k osobním údajům mají pouze pracovníci pověření provozovatelem, a to pouze v rozsahu nezbytně potřebnému pro plnění pracovních povinností.
2) Dokumenty a média jsou uchovávány odděleně od zdravotnické dokumentace v místech k tomu určeným provozovatelem.
3) Osobní údaje jsou zpracovávány v souladu s katalogem zpracování v příloze č.1.
4) Osobní údaje jsou uchovávány pouze po nezbytně nutnou dobu.

3 Směrnice pro zálohování a obnovu dat

3.1 Účel

Toto nařízení upravuje procesy zálohování a obnovy dat ve zdravotnickém zařízení. Účelem je zajistit ochranu dat v případě bezpečnostního incidentu v informačním systému.

3.2 Definice pojmů

Garant – osoba určená provozovatelem zodpovědná za správu informačního aktiva

Zálohování – vytvoření kopie na jiném nosiči

3.2.1 Povinnosti – Zálohování

1) Za zálohování informačního aktiva je zodpovědný garant uvedený v katalogu dat k zálohování
2) Zálohování je prováděno dle plánu v katalogu dat k zálohování způsobem uvedeným tamtéž
3) Garant informačního aktiva vede evidenci archivačních médií. Média musí být jednoznačně identifikovatelná
4) V případě uplynutí doby uchovávání informačního aktiva nebo záloh je jeho garant odpovědný za provedení skartačního řízení včetně zhotovení záznamu do skartační knihy.)
5) V případě ztráty nebo zničení záložního média je garant povinen tuto událost zaznamenat a nahlásit správci osobních údajů.

3.2.2 Povinnosti – Obnovení

1) Za provedení obnovení dat ze záloh je zodpovědný garant informačního aktiva
2) Pro obnovení je použit záložní soubor určený v katalogu dat k zálohování
3) V případě selhání infrastruktury počítačové sítě spolupracuje garant informačního aktiva s garantem hardwarového aktiva na stanovení postupu obnovení

4 Seznam příloh

1) Příloha č. 1: Analýza rizik – GDPR
2) Příloha č. 2: Politika hesel
3) Příloha č. 2: Katalogu dat k zálohování

Příloha B: Politika hesel

1 Příloha – Politika hesel

1.1 Povinnosti pracovníků

1) Pracovník je povinen vytvářet a obměňovat hesla dle pravidel pro tvorbu hesla
2) Pracovník je povinen zachovávat důvěrnost hesla. Je zakázáno sdělovat hesla třetím osobám nebo je zaznamenávat.
3) Při podezření na prolomení hesla je pracovník povinen neprodleně změnit heslo a bez prodlení o tom informovat správce informačního systému.

1.2 Povinnosti správce informačního systému

1) Správce informačního systému (dále jen „správce IS") je povinen stanovit centrální politiku hesel, kde to programové vybavení umožňuje.
2) Správce IS je povinen přijímat hlášení od pracovníků o prolomení hesla.
3) Správce IS je při podezření na zneužití uživatelského účtu povinen účet zablokovat a nastavit nové jednorázové heslo.

1.3 Pravidla pro tvorbu hesla

- **Privilegované účty**
  - Minimální délka hesla 17 znaků
  - Heslo musí obsahovat minimálně 3 znaky z následujících skupin (velká písmena, malá písmena, číslovky, speciální znaky)
  - Maximální doba platnosti 18 měsíců
  - Zákaz opakovaného používání stejných hesel (posledních 12 hesel)
  - Zamčení účtu po 5 neplatných pokusech v řadě
  - Jednorázové prvotní heslo – nutné změnit při prvním přihlášení nebo zneplatněno po 24 hodinách

- **Uživatelské účty**
  - Minimální délka hesla 10 znaků
  - Maximální doba platnosti 18 měsíců
  - Zákaz opakovaného používání stejných hesel (posledních 12 hesel)
  - Zamčení účtu po 10 neplatných pokusech v řadě
  - Jednorázové prvotní heslo – nutné změnit při prvním přihlášení nebo zneplatněno po 24 hodinách

Příloha C: Obsah přiloženého CD

Key_Words.pdf	Klíčová slova
Abstrakt_CZ.pdf	Abstrakt v českém jazyce
Abstract_ENG.pdf	Abstrakt v anglickém jazyce
Zadani_BP.pdf	Zadání bakalářské práce
BP_Bocek.pdf	Text bakalářská práce
Analyza_Rizik_GDPR.xlsx	Analýza rizik pro část GDPR
Analyza_Rizik_Hlavni.xlsx	Analýza rizik pro hlavní část
Bezpecnostni_Smernice.pdf	Text bezpečnostní směrnice
Katalog_Dat_K_Zalohovani.xlsx	Katalog dat k zálohování
Politika_Hesel.pdf	Politika hesel