VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ V SOULADU S ISMS PRO ZDRAVOTNICKÉ ZAŘÍZENÍ

DESIGN OF SECURITY MEASURES IMPLEMENTATION IN ACCORDANCE WITH ISMS FOR HEALTHCARE INSTITUTION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Martina Valášková**
AUTHOR

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

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Martina Valášková**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2019/20

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

Návrh bezpečnostních opatření v souladu s ISMS pro zdravotnické zařízení

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Cílem této diplomové práce je navrhnout opatření v souladu se systémem řízení informační bezpečnosti za účelem zvýšení její aktuální úrovně. Jednotlivá opatření budou navržena na základě analýzy současného stavu sítě a určitých oblastí nemocnice a následné analýzy rizik. Vzhledem k tomu, že se jedná o zdravotnické zařízení, je cílem také soulad s platnými normami pro prvek kritické infrastruktury.

Základní literární prameny:

ČSN ISO/IEC 27000. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Přehled a slovník. Praha: Český normalizační institut, 2017.

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.

ČSN EN ISO 27799. Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002. Praha: Český normalizačný institut, 2019.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-87.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

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

Abstrakt

Diplomová práca sa zaoberá návrhom bezpečnostných opatrení, ktoré sú v súlade so systémom riadenia informačnej bezpečnosti a keďže sa jedná o zdravotnícke zariadenie, rovnako aj s normami platnými pre prvok kritickej infraštruktúry. Jej obsah tvoria teoretické východiská danej problematiky, analýza súčasného stavu siete a určitých oblastí nemocnice. Praktická časť je venovaná analýze rizík a z nej vyplývajúceho návrhu konkrétnych opatrení, ktorých výsledkom je zvýšenie úrovne informačnej bezpečnosti. Súčasťou práce je taktiež ekonomické zhodnotenie implementácie návrhov.

Kľúčové slová

ISMS, ISO/IEC 27000, ISO/IEC 27799, informačná bezpečnosť, zdravotnícke zariadenie, analýza rizík, bezpečnostné opatrenia

Abstract

The Master Thesis deals with the design of security measures in accordance with the information security management system and as well as the standards applicable to the critical infrastructure element since it is a healthcare institution. It consists of theoretical background, analysis of the current state of the network and certain areas of the hospital. The practical part is devoted to the risk analysis and the design of concrete measures that result in an increase in the information security level. This part also includes an economic evaluation of the design implementation.

Key words

ISMS, ISO/IEC 27000, ISO/IEC 27799, information security, healthcare institution, risk analysis, security measures

Bibliografická citácia

VALÁŠKOVÁ, Martina. *Návrh bezpečnostních opatření v souladu s ISMS pro zdravotnické zařízení.* Brno, 2020. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/127737. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prehlásenie

Prehlasujem, že predložená diplomová práca je pôvodná a spracovala som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušila autorské práva (v zmysle zákona č.121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brne dňa 15. mája 2020

.....

podpis autora

Poďakovanie

Moje poďakovanie má predovšetkým vedúci práce, Ing. Petr Sedlák, za jeho cenné rady a ľudský prístup počas konzultácií a vedenia celej práce. Tiež by som rada poďakovala pracovníkom IT oddelenia Nemocnice s poliklinikou Považská Bystrica, za ochotu a spoluprácu pri poskytovaní informácií pre vypracovanie analytickej časti práce.

OBSAH

ÚVOD

Súčasným trendom je digitalizácia dát a informácií, ktorá uľahčuje procesy vykonávané v spoločnosti. Digitalizáciou však vzniká potreba tieto dáta aj patrične zabezpečiť proti ich zneužitiu. Kompromitácia citlivých údajov má v oblasti zdravotníctva obzvlášť závažné dôsledky. Napriek tomu stále nie je venovaná dostatočná pozornosť ochrane týchto dát a zvyšovaniu bezpečnostného povedomia v prípade personálu, ktorý s nimi pracuje. Takisto je nutná ochrana osobných údajov pacientov, zamestnancov a dodávateľov, ktorá je povinná zo zákona. Problematika bezpečnosti informácií je veľmi rozsiahla a jej komplexné zabezpečenie nie je jednoduché. Pri tvorbe vhodného systému na riadenie bezpečnosti informácii je potrebné sa riadiť odporúčaniami obsiahnutými v normách rady 27000. Práve o tieto normy sa budem v mojej práci opierať.

Diplomová práca sa bude zaoberať návrhom bezpečnostných opatrení v súlade s normami ISO 27000. Rozhodla som sa pre zdravotnícke zariadenie, a to konkrétne Nemocnicu s poliklinikou Považská Bystrica.

V prvej časti práce si stanovím jej ciele a metodiku vypracovania. Vzhľadom na to, že ide o prvok kritickej infraštruktúry, je potrebné klásť väčší dôraz na súlad s platnými normami.

Nasledujúca kapitola bude slúžiť ako teoretický úvod k problematike riešenej v zvyšných častiach práce.

V úvode analytickej časti popíšem zvolenú spoločnosť, jej sieťovú infraštruktúru a súčasnú situáciu ohľadom systému riadenia informačnej bezpečnosti. Na základe vykonanej analýzy následne zhodnotím aktuálnu situáciu.

Posledná kapitola bude venovaná vlastnému návrhu, ktorý bude vychádzať z vykonanej analýzy. Súčasťou tejto kapitoly bude identifikácia a ohodnotenie aktív spoločnosti, ich zraniteľností a hrozieb, ktoré na ne vplývajú. Podstatnou súčasťou kapitoly bude aj analýza rizík, ktorej výsledkom bude nájdenie problematických oblastí a teda oblastí, v ktorých je nutné zavedenie ISMS. Následne budú navrhnuté konkrétne opatrenia smerujúce k náprave zistených nedostatkov. Súčasťou tejto kapitoly bude aj ekonomické zhodnotenie zvoleného návrhu zavedenia ISMS.

VYMEDZENIE PROBLÉMU A CIELE PRÁCE

Práca sa zaoberá problematikou bezpečnosti informácií, ktorá je v oblasti zdravotníctva obzvlášť dôležitá. Dostatočná úroveň ochrany informácií môže spoločnosti poskytnúť dôveru zo strany verejnosti, dobrú povesť a z nej vyplývajúcu konkurenčnú výhodu. V posledných rokoch sa bezpečnosť informácií stala tiež súčasťou legislatívy, čím vznikla mnohým subjektom povinnosť zariadiť súlad s platnými zákonmi v danej oblasti. V prípade ich nedodržania hrozia spoločnosti vysoké sankčné postihy.

Hlavným cieľom práce je preto navrhnúť pre nemocničné zariadenie bezpečnostné opatrenia v súlade s ISMS, ktorých výsledkom bude zvýšenie celkovej úrovne informačnej bezpečnosti spoločnosti. Predmetom práce nie je návrh zavedenia systému riadenia bezpečnosti informácií v plnom rozsahu ale len jeho vybraných častí. Ďalším cieľom je zabezpečenie súladu s legislatívou platnou pre prvok kritickej infraštruktúry. Navrhované opatrenia je nutné voliť s prihliadnutím na ich efektivitu z hľadiska ekonomického a tiež časového.

Konkrétne opatrenia budú zvolené na základe analýzy súčasného stavu sieťovej infraštruktúry spoločnosti a jednotlivých oblastí informačnej bezpečnosti nemocnice. Informácie potrebné na analýzu získam predovšetkým spoluprácou s pracovníkmi IT oddelenia. Výsledky analýzy budú použité v návrhovej časti pri identifikácií a analýze aktív, zraniteľností, pôsobiacich na identifikované aktíva a tiež v analýze rizík. Výstupom analýzy rizík budú kritické miesta informačnej bezpečnosti, pre ktoré bude nutné zavedenie bezpečnostných opatrení v záujme zníženia miery jednotlivých rizík na ich prijateľnú úroveň.

1 TEORETICKÉ VÝCHODISKÁ

Nasledujúca kapitola bude slúžiť ako teoretický úvod k problematike riešenej v zvyšných častiach práce.

1.1 Základné pojmy

Informácie – podľa normy ISO/IEC 2382:2015 sú informácie vedomosťami, ktoré znižujú alebo odstraňujú neistotu o výskyte konkrétnej udalosti z daného súboru možných udalostí (1). Pre účely tejto práce majú informácie význam aktív spoločnosti, dôležitých pre podnikanie, preto je nutné aby boli dôkladne ochránené. Môžu mať formu:

- materiálnu – napr. na papieri, CD alebo USB nosiči,
- digitálnu – elektronický dokument uložený na disku,
- znalosť zamestnancov (2).

Dáta – opakovane interpretovateľné vyjadrenie informácií formalizovaným spôsobom, vhodným na komunikáciu, interpretáciu alebo spracovanie (1). Sú teda akýmsi „plnením" informácie, ktorú vytvárajú (2).

Informačný systém (IS) – systém spracovania informácií, ktorý v spojení s organizačnými zdrojmi (ľudské, technické a finančné zdroje), uchováva, poskytuje a distribuuje informácie (1).

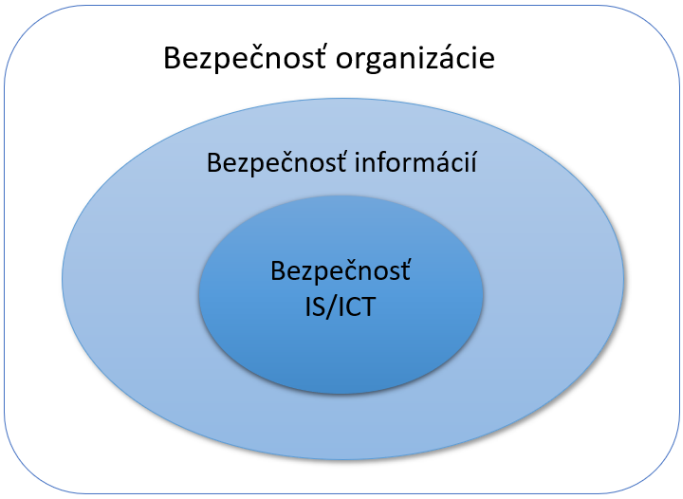
Sieťová infraštruktúra – súbor všetkých sieťových prvkov a zariadení použitých na realizáciu ICT prostredia. Taktiež môže zahŕňať aktíva v oblasti ICT, ktoré slúžia k vytváraniu a podpore informačného systému (2).

Počítačová sieť – súčasť sieťovej infraštruktúry, vytvárajúca komunikačné prostredie medzi jednotlivými užívateľmi siete (2).

IMS (Integrated Management System) – integrovaný systém riadenia je filozofia komplexného riadenia spoločnosti (2).

Bezpečnosť informácií – predmetom informačnej bezpečnosti je ochrana informácií a takisto ich dostupnosť. Existuje vzájomné prepojenie s bezpečnosťou organizácie a bezpečnosťou IS/ICT. Najvyššie je postavená bezpečnosť organizácie, ktorá zahŕňa zaistenie bezpečnosti objektu a zároveň majetku organizácie. Jej podmnožinou je aj

bezpečnosť informácií, ktorá má okrem bezpečnosti IS/ICT, ktorá chráni len aktíva informačného systému podporované informačnými a komunikačnými technológiami, za úlohu ochrániť aj prácu s nedigitálnymi informáciami (2). Nasledujúci obrázok graficky znázorňuje vzťah medzi týmito pojmami.



Obrázok č. 1: Vzťah úrovní bezpečnosti
(Zdroj: Vlastné spracovanie podľa: 2, s. 14)

Základné bezpečnostné atribúty – základné bezpečnostné požiadavky na ochranu údajov:

- **dôvernosť** (confidentiality) – k informácii, ktorú údaje obsahujú nemajú prístup nepovolané osoby,
- **integrita** (integrity) – údaje nemôžu byť modifikované bez toho, aby si to oprávnená osoba všimla,
- **dostupnosť** (availability) – oprávnená osoba má údaje k dispozícii kedykoľvek, keď o to požiada (3).

Aktívum – čokoľvek, čo pre vlastníka (subjekt) predstavuje nejakú hodnotu a vplyvom hrozby môže byť poškodené alebo zničené. Rozdeľujú sa na dva typy:

- hmotné – napr. hnuteľné, nehnuteľné, finančné prostriedky, cenné papiere,
- nehmotné – napr. software, informácie, patenty, znalosti, kvalifikácia (4).

Jeho základnými charakteristikami sú hodnota aktíva (vyjadrená cenou prípadne dôležitosťou pre vlastníka) a zraniteľnosť (2).

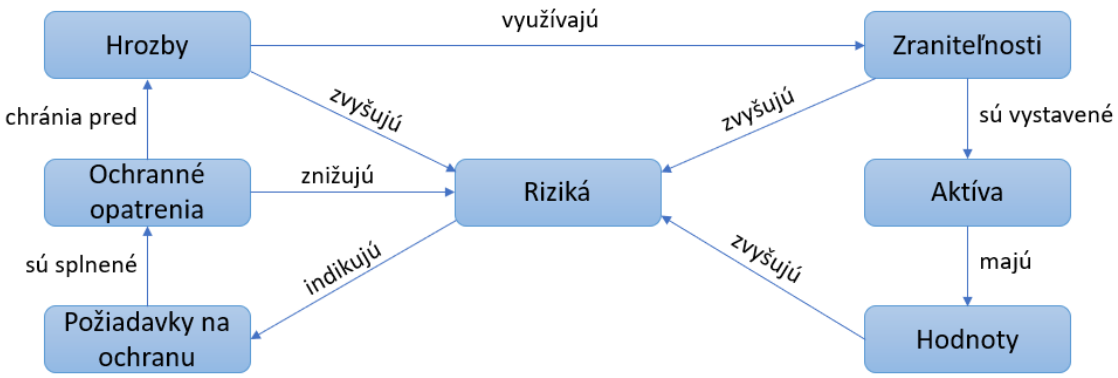
Zraniteľnosť – slabina, nedostatok alebo chyba aktíva. Vyjadruje citlivosť aktíva na pôsobenie danej hrozby. Citlivosť predstavuje náchylnosť aktíva na poškodenie danou hrozbou (4).

Hrozba – udalosť, aktivita alebo subjekt, ktorý potenciálne môže mať za následok nežiadúci incident, škodu alebo nežiaduco ovplyvniť vývoj udalostí. Jej následky sú označované ako dopad hrozby. Základnou charakteristikou hrozby je jej úroveň, ktorá sa hodnotí podľa nasledujúcich faktorov:

- nebezpečnosť – schopnosť spôsobiť škodu,
- prístup – možnosť pôsobiť na aktívum,
- motivácia – záujem o naplnenie hrozby (4).

Opatrenie – čokoľvek (postup, proces, služba, fyzický prostriedok) čo bolo navrhnuté a aplikované za účelom zmiernenia dopadu hrozby alebo jej úplnú elimináciu. Výsledkom zavedenia opatrenia je teda zníženie rizika. Rozsah opatrenia je klasifikovaný ako úroveň opatrenia. Podľa typu ich môžeme rozdeliť na preventívne, podporné, detekčné, atď. Účinnosť opatrenia vyjadruje splnenie účelu v reálnom procese (4).

Vzťah medzi vyššie spomínanými pojmami znázorňuje nasledujúci obrázok č. 2.



Obrázok č. 2: Vzťah medzi základnými pojmami
(Zdroj: Vlastné spracovanie podľa 3)

1.1.1 Zdravotnícke prostredie

Zdravotnícka informatika (Health informatics) – vedecká disciplína, zaoberajúca sa poznávacími, informačne-spracovateľskými a komunikačnými úlohami nie len v rámci

zdravotníckej praxe ale tak isto aj vzdelania a výskumu vrátane informačnej vedy a technológií podporujúcich tieto úlohy (2).

Zdravotnícky informačný systém (Health informatic system) – úložisko informácií ohľadne zdravotného stavu subjektu starostlivosti v počítačovo spracovateľnej podobe. Tieto informácie sú ukladané a prenášané bezpečne a sú prístupné viacerým autorizovaným užívateľom (2).

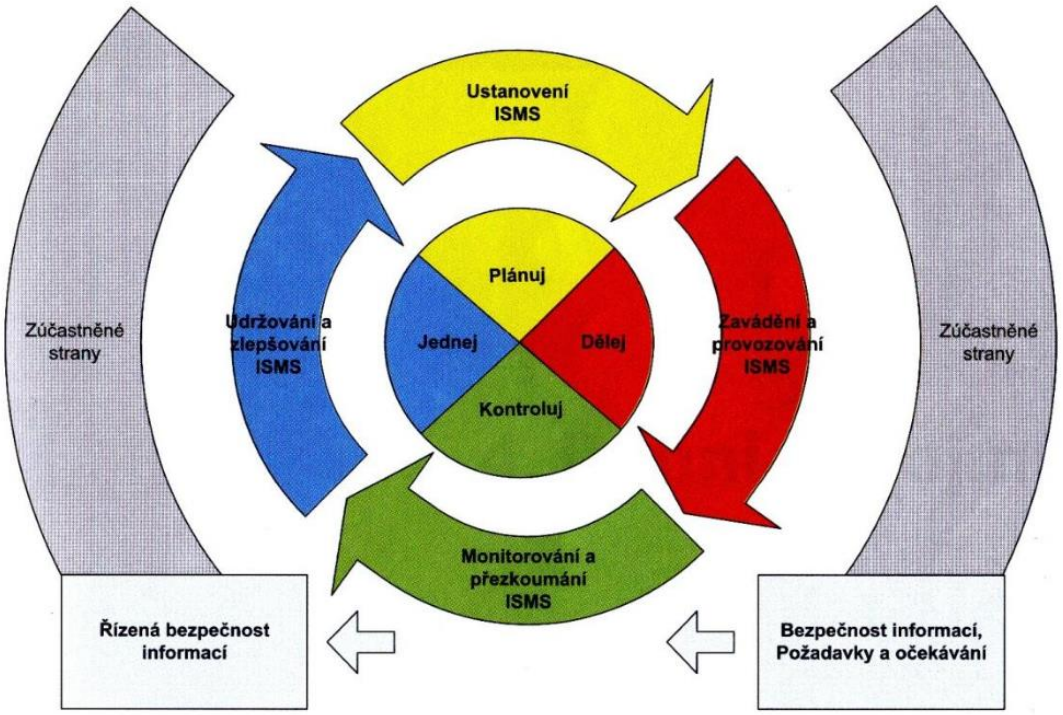
Osobné zdravotné informácie (Personal health information) – informácie o identifikovateľnej osobe, popisujúce jej fyzické alebo psychické zdravie, prípadne poskytovanie zdravotníckych služieb. Môžu zahŕňať:

- informácie o registrácií na poskytovanie zdravotnej služby,
- informácie o platbách alebo nároku na zdravotnú starostlivosť,
- jednoznačný identifikátor jednotlivca (napríklad vo forme čísla alebo symbolu),
- všetky informácie o jednotlivcovi, zozbierané počas poskytovania zdravotníckych služieb,
- informácie z testovania či vyšetrenia časti tela alebo telesnej látky,
- identifikačné údaje osoby, poskytujúcej zdravotnú starostlivosť (2).

1.2 ISMS

Definícia pojmu ISMS vyplýva už z jej názvu Information Security Management System. Ide o systém, ktorý je časťou celkového systému riadenia organizácie, zaoberajúci sa riadením bezpečnosti informácií. ISMS je podľa normy ISO/IEC 27001 postavený na modeli PDCA (Demingovom model), z čoho vyplývajú aj jeho 4 etapy:

- PLAN – zriadenie ISMS – určenie rozsahu a zodpovednosti,
- DO – zavedenie a prevádzka ISMS – aplikovanie bezpečnostných opatrení,
- CHECK – monitorovanie a preskúmanie ISMS – spätná väzba a hodnotenie,
- ACT – údržba a zlepšovanie – eliminácia slabých miest systému riadenia a neustále zlepšovanie (2).



Obrázok č. 3: Životný cyklus ISMS
(Zdroj: 2, s.25)

1.2.1 Zriadenie ISMS

Fáza stanovenia ISMS je procesom špecifikácie a návrhu ISMS od vzniku až po vypracovanie implementačných plánov. V tejto fáze sa vstupy, ako je napríklad vízia zainteresovaných strán, transformujú na výstupy, akými je schválenie vedenia pre rozsah ISMS či rozsah ISMS (5). Je základom budovania systému riadenia informačnej bezpečnosti. Okrem stanovenia rozsahu ISMS zahŕňa taktiež definovanie bezpečnostnej politiky, návrh riadenia rizík vrátane ich vyhodnotenia a voľbu opatrení na zníženie rizík (6). Výsledkom tejto fázy v zdokumentovanej podobe by mali byť:

- **Súhlas vedenia so zavádzaním ISMS** – jeho získanie je prvým krokom pri zavádzaní ISMS. Dokument nemusí byť rozsiahly, musí však jasne vyjadrovať ochotu a vôľu spoločnosti podriadiť sa systému ISMS (2).
- **Definovanie rozsahu a hraníc ISMS** – Nie je pravidlom, že rozsah a hranice musia pokývať celú organizáciu. ISMS môže byť zamerané len na zvolenú časť organizácie (pobočka, informačný systém) (7).
- **Prehlásenie o politike ISMS** – definovanie politiky ISMS na základe špecifických potrieb organizácie. Politika by mala definovať ciele ISMS, vytvoriť

väzby potrebné na vybudovanie a údržbu ISMS a tiež stanoviť kritériá popisu a hodnotenia rizík. Po dokončení by mala byť schválená vedením (7).

- **Analýza rizík –** dôležitý dokument vypracovaný pomocou zvolenej metodiky na základe identifikácie primárnych (nehmotných) a sekundárnych (hmotných) aktív a ich následnom ohodnotení z hľadiska dostupnosti, dôvernosti a integrity (2).
- **Návrh opatrení** – obsahom tohto dokumentu sú bezpečnostné opatrenia odvíjajúce sa od nájdených kritických miest, zvolených bezpečnostných potrieb a určených priorít. Účelom týchto opatrení je efektívna eliminácia zistených rizík. V prípade nízkej mieri rizika alebo potreby veľmi drahého opatrenia existuje tiež možnosť prípadné riziko akceptovať (2).
- **Prehlásenie o aplikovateľnosti** (Statement of Applicability) – tento dokument je podľa normy povinnou súčasťou dokumentácie ISMS. Popisuje relevantné a aplikovateľné bezpečnostné opatrenia v rámci ISMS organizácie, vrátane ich cieľov. Musí tiež obsahovať popis jednotlivých bezpečnostných opatrení a ich cieľov, ktoré sú:
    - zvolené, spolu s dôvodom ich výberu,
    - už implementované,
    - vyradené, spolu s dôvodom ich vyradenia (2).

1.2.2 Zavedenie a prevádzka ISMS

Druhá fáza zahŕňa zavedenie systému a využívanie bezpečnostných opatrení, procesov a postupov vrátane monitorovania ich účinnosti. Jej súčasťou je takisto:

- vytvorenie plánu kontinuity, postupov reakcie v prípade výskytu bezpečnostného incidentu (6),
- formulovanie programu budovania bezpečnostného povedomia a príprave a zaškoleniu pracovníkov z oddelenia informatiky a riadenia bezpečnosti,
- zadefinovanie spôsobov merania účinnosti bezpečnostných opatrení a sledovať stanovené ukazovatele. Samozrejmou činnosťou,
- riadenie záznamov, zdrojov a dokumentov ISMS (7).

1.2.3 Monitorovanie a preskúmanie ISMS

V tejto fáze je posudzovaná funkčnosť a efektivita procesov a opatrení. Sú vykonávané interné audity, prehodnotené riziká a preskúmaný systém riadenia bezpečnosti informácií (4). Zistené výsledky sú zaznamenané v správe o stave ISMS, podľa ktorej je prehodnotené ISMS na úrovni vedenia organizácie (7).

1.2.4 Údržba a zlepšovanie

V poslednej fáze cyklu sú na základe výsledkov z predchádzajúcej fázy identifikované možnosti zlepšenia a vykonávané nápravné a preventívne opatrenia za účelom odstránenia nedostatkov (6).

1.3 Riadenie rizík

Riadenie rizík je oblasťou riadenia zameranou na analýzu a následné zníženie rizika, pomocou rôznych metód a techník, ktoré dokážu eliminovať existujúce alebo odhaliť budúce faktory zvyšujúce riziko. Zahŕňa sústavné, opakujúce sa navzájom previazané aktivity, ktorých účelom je predísť problém či negatívnym javom a vyhnúť sa krízovému managementu. Skladá sa zo 4 prepojených fáz:

- identifikácia rizík,
- zhodnotenie rizík,
- zvládnutie rizík,
- monitoring rizík (8).

Identifikácia rizík

Pred samotnou identifikáciou aktív je vhodné stanoviť hranice revízie v záujme zamedzenia zbytočných činností. Samotná identifikácia rizík zahŕňa identifikovanie kľúčových aktív v rámci definovaných hraníc a ich následné ohodnotenie. Hodnota aktíva vychádza z jeho potenciálneho dopadu na dostupnosť, dôvernosť a integritu informácií (8).

Zhodnotenie rizík

V tejto fáze je potrebné identifikovať hrozby pôsobiace na jednotlivé aktíva a ich zraniteľnosť prípadnej hrozbe podľahnúť. Hodnotenie hrozieb a zraniteľností, spolu s ohodnotením aktív z prvej fázy, určuje mieru rizika systému. Miera rizika každého aktíva je stanovená funkciou hodnoty aktíva s hodnotením hrozby a zraniteľnosti. Na ich základe sú navrhnuté vhodné bezpečnostné opatrenia (8).

Zvládnutie rizík

Súčasťou riadenia rizík je aj ich zvládanie (resp. ich zmiernenie). V prípade existencie rizika s mierou neprijateľnou pre spoločnosť, je nutné zvoliť vhodný spôsob zvládnutia rizika. Spôsoby akými je možné riziká eliminovať alebo zmierniť sú retencia, redukcia, transfer, poistenie, zdieľanie a vyhnutie sa riziku. Výsledkom tejto fázy je rozhodnutie o použití konkrétnych bezpečnostných opatrení, ktorých účelom je zníženie miery rizika na prijateľnú úroveň. Pre akceptované riziká, na ktoré nie je možné aplikovať bezpečnostné opatrenia sa spracovávajú krízové plány (8).

Monitoring rizík

V záujme zachovania aktuálnosti plánu riadenia rizík, je nutné naďalej sledovať výskyt nových rizík ale takisto aj identifikované riziká, ktorých dopad a pravdepodobnosť výskytu sa môžu zmeniť vplyvom zmeny podmienok, prostredia, technológií a tak podobne. Zmeniť sa tiež môžu okolnosti, ktoré ovplyvňujú náklady alebo vhodnosť zavedených opatrení (8).

1.4 Metodiky a rámce

Existujú rôzne metodiky, podľa ktorých môžeme pri zavádzaní ISMS postupovať.

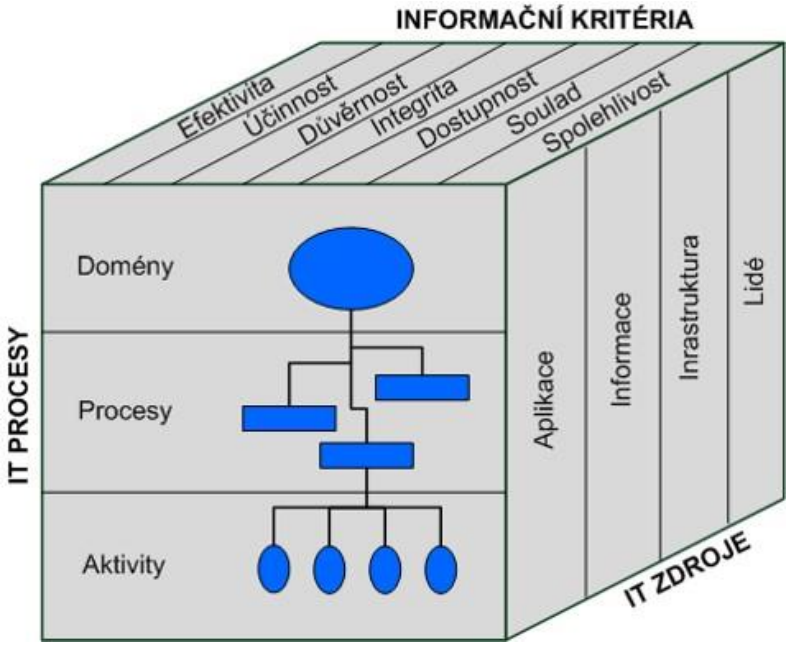
1.4.1 COBIT

COBIT (Control Objectives for Information and related Technology) je medzinárodne uznávaná metodika, ktorá vychádza z najlepších skúseností a širokého okruhu zdrojov - napríklad ISO/IEC 27000, ITIL, PMBOK (Project Management Body of Knowledge) a ďalšie. Jej cieľom je prepojenie princípov všeobecného riadenia organizácie s pravidlami uplatňovanými v oblasti IT a zariadiť, aby bol tento zložitý systém riadenia

IT zrozumiteľný pre riadiacich pracovníkov a užívateľov bez detailných znalostí IT. Úspešnosť či neúspešnosť jednotlivých oblastí riadenia je posudzovaná na základe požiadaviek na informácie (informačných kritérií), ktoré sú štruktúrované do nasledujúcich skupín:

- **efektivita** – včasné doručovanie relevantných informácií v správnom, použiteľnom a konzistentnom tvare,
- **účinnosť** – spracovanie informácií prostredníctvom optimálneho využitia zdrojov informatiky,
- **dôvernosť** – ochrana informácií proti neoprávnenému použitiu,
- **integrita** – presnosť a kompletnosť informácií,
- **dostupnosť** – dostupnosť informácií a ochrana potrebných zdrojov (napr. dátových),
- **súlad** – udržovanie súladu so zákonmi, reguláciami, smernicami a zmluvnými podmienkami,
- **spoľahlivosť** – prínos informácií pre manažérske rozhodovanie (2).

Vyššie spomínané informačné kritéria sú jednou osou COBIT kocky. Zvyšné dve tvoria zdroje IT (aplikácie, informácie, infraštruktúra, ľudia) a IT procesy (domény, procesy, aktivity). Kocka COBIT je zobrazená na nasledujúcom obrázku (2).



Obrázok č. 4: COBIT kocka
(Zdroj: 2, s. 31)

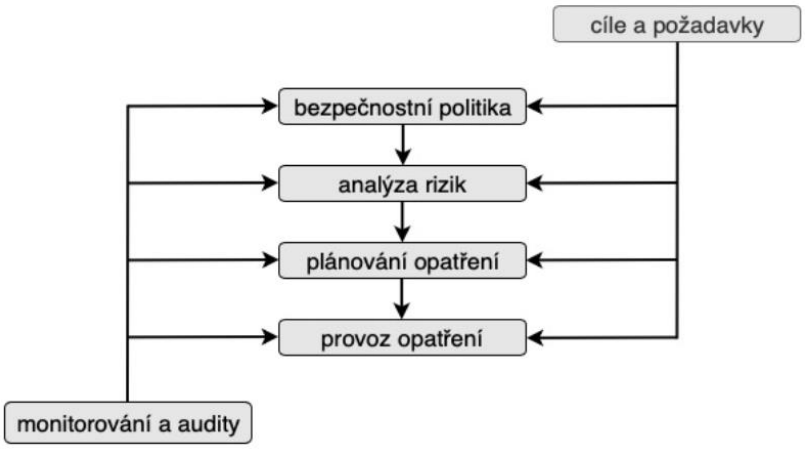
1.4.2 ITIL

(Information Technology Infrastructure Library) – rámec, knižnica (nie metodika) doporučení a osvedčených postupov (Best Practices) pre návrh procesov ITSM (IT Service Management) (2).

Vzhľadom na to, že ITIL je rámec a nie je závislý na platforme, umožňuje veľkú voľnosť pri implementácii procesov. Obsahom knižnice ITIL je:

- definovanie procesov potrebných pre zaistenie ITSM
  - stanovenie cieľov, vstupov, výstupov a aktivít každého procesu,
  - stanovenie rolí a ich zodpovednosti v danom procese,
  - spôsob merania kvality poskytovaných IT služieb a účinnosti ITSM procesov,
  - vzájomné väzby medzi jednotlivými procesmi,
  - postupy auditu a zásady reportingu pre každý proces,
- zásady pre implementáciu procesov ITSM
  - prínosy každého procesu,
  - Critical Success Factors, možné problémy a vhodné opatrenia,
  - náklady na implementáciu a následnú prevádzku,
  - zásady pre riadenie podpornej ICT infraštuktúry,
  - zásady bezpečnosti ICT infraštruktúry (2).

Na nasledujúcom obrázku.je znázornený proces riadenia bezpečnosti informácií podľa rámca ITIL.



Obrázok č. 5: Základné procesy riadenia bezpečnosti informácií podľa ITIL
(Zdroj: 2, s. 30)

1.4.3 CRAMM

CCTA Risk Analysis and Management Method je metodika a súbor softwarových nástrojov ktoré plne podporujú zavádzanie a podporu ISMS v súlade s normou ISO/IEC 27001:2005 (2).

CRAMM Express môže byť definovaná aj ako jednodňová analýza rizík, ktorá využíva opatrenia len prvej z troch kategórií z knižnice opatrení (2).

CRAMM Expert je detailnou analýzou rizík, ktorá disponuje plnohodnotnou knižnicou opatrení (2).

1.5 Normy

Ak by každá organizácia mala riešiť problémy informačnej bezpečnosti samostatne, pre väčšinu by to neriešiteľná úloha. Vzhľadom na to, že organizácie využívajú štandardné technické prostriedky so štandardným programovým vybavením, problémy informačnej bezpečnosti v organizáciách je možné riešiť štandardnými prostriedkami. Z tohto dôvodu vyvinuli v posledných troch dekádach štátne, súkromné, odborné a iné organizácie značné úsilie o štandardizáciu informačnej bezpečnosti. Jej výsledkom je množstvo noriem, technických správ (3).

1.5.1 Normalizačné inštitúcie

IEC

IEC (International Electrotechnical Commission), založená v roku 1906, je poprednou svetovou organizáciou, ktorá pripravuje a vydáva medzinárodné normy pre všetky elektrické, elektronické a súvisiace technológie. S cieľom zabezpečiť súlad a vzájomné dopĺňanie medzinárodných noriem IEC spolupracuje s organizáciami ISO (International Organization for Standardization) alebo ITU (International Telecommunication Union) (7).

ISO

V roku 1946 sa v Londýne stretlo 65 delegátov z 25 krajín, aby prediskutovali budúcnosť medzinárodnej normalizácie. O rok neskôr oficiálne vznikla organizácia ISO

(International Organization for Standardization) so 67 technickými komisiami zloženými z odborníkov na konkrétne oblasti. V súčasnosti je ISO nezávislá mimovládna organizácia, zložená zo 164 národných normalizačných orgánov. ISO združuje odborníkov, ktorí zdieľajú znalosti a rozvíjajú medzinárodné trhové štandardy, ktoré podporujú inovácie a poskytujú riešenia globálnych výziev (9).

NIST

Americká organizácia NIST (National Institute of Standards and Technology) zodpovedá za vývoj štandardov, techník a návodov na zaistenie informačnej bezpečnosti v amerických štátnych inštitúciách a agentúrach. Napriek tomu, že právne prostredie a organizácia amerických inštitúcií je iné ako na Slovensku, niekoľko štandardov a množstvo metodických materiálov je použiteľných aj v slovenských podmienkach (3).

ČSNI

Český normalizační institut bol zriadený ako štátna príspevková organizácia. V súčasnosti je podriadený Ministerstvu priemyslu a obchodu. ČSNI má štatút národnej normalizačnej organizácie, ktorá zastupuje národné záujmy v európskych a medzinárodných organizáciách. Inštitút je členom medzinárodných normalizačných organizácií ISO a IEC, európskych normalizačných organizácií CEN a CENELEC a európskom normalizačnom inštitúte pre telekomunikácie ETSI [2]. Od 1.1.2018 prešli všetky činnosti súvisiace s tvorbou, vydávaním a distribúciou technických noriem na ČAS (Česká agentura pro standardizaci) (10).

SÚTN

Organizácia Slovenský úrad technickej normalizácie bola založená v roku 2000. Jej úlohou bola tvorba, vydávanie, aktualizácia a preberanie národných, európskych a medzinárodných technických noriem. O 13 rokov neskôr bol SÚTN zrušený a jeho záväzky prevzal Úrad pre normalizáciu, metrológiu na skúšobníctvo Slovenskej republiky. Slovensko sa týmto stalo jedinou krajinou Európskej únie, v ktorej oblasť technickej normalizácie priamo riadi vládny úrad, čím nie sú zabezpečené základné princípy (politická a finančná nezávislosť od štátnej moci) vnútorných predpisov Európskych normalizačných organizácií CEN-CENELEC a nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012 o európskej technickej normalizácií (11).

1.5.2 Základné normy rady 27000

Rodina noriem ISMS slúži organizáciám všetkých typov a veľkostí na pomoc so zavádzaním a prevádzkou systému riadenia bezpečnosti informácií. Použitím týchto noriem môžu organizácie vyvinúť a implementovať rámec pre riadenie bezpečnosti svojich bezpečnostných aktív a pripraviť nezávislé ohodnotenie ochrany informácií (napr. finančných, informácií o zamestnancoch alebo informácií, ktoré im boli zverené zákazníkmi alebo tretími stranami) (2).

ČSN ISO/IEC 27000:2017 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník

Ako už vyplýva z názvu, táto medzinárodná norma poskytuje prehľad systémov riadenia bezpečnosti informácií, ktoré sú predmetom rodiny noriem ISMS a zároveň definuje súvisiace termíny (2).

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

Obsahom tejto normy sú odporučenia ako aplikovať vybrané opatrenia ISO/IEC 17799 (predchodca normy ISO/IEC 27002) v rámci procesu zavádzania, prevádzky, údržby a zlepšovania ISMS v organizácii. Norma odporúča prijatie procesného prístupu a zavádza PDCA model, ktorý môže byť aplikovaný na všetky procesy ISMS. Je prepojená a harmonizovaná s normami ISO/IEC 9001 a ISO/IEC 14001 za účelom podpory ich konzistentného a jednotného zavedenia a prevádzky (2).

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

Táto norma obsahuje viac ako 5000 priamych a odvodených bezpečnostných opatrení, rozdelených do viac ako 133 štruktúrovaných oblastí. Zodpovednosť za opatrenia je možné jednoducho priradiť k osobe so zodpovedajúcou funkciou. Vďaka tomu je možné rýchle určenie stavu bezpečnosti informačného systému organizácie a vytvorenie východiska pre jeho zlepšenie (2).

ČSN ISO/IEC 27005:2019 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

Norma je aplikovateľná na všetky typy organizácií, ktoré majú v úmysle riadiť riziká, ohrozujúce bezpečnosť informácií organizácie. Poskytuje odporúčania pre riadenie rizík bezpečnosti informácií, podporuje všeobecný koncept špecifikovaný v ISO/IEC 27001, neponúka však konkrétnu metodiku pre riadenie rizík bezpečnosti informácií. Je teda len na organizácií, aký prístup k riadeniu rizík zvolí, napríklad na základe rozsahu ISMS (2).

1.5.3 Zdravotnícke prostredie

ČSN ISO/IEC 27799:2019 **Zdravotnická informatika** – Systémy řížení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002.

Zavedenie tejto normy zabezpečuje nevyhnutnú minimálnu úroveň zabezpečenia, zodpovedajúcu pomerom v organizácií a zachovanie dôvernosti, integrity a dostupnosti osobných zdravotných informácií. Rieši bezpečnosť zdravotníckych informácií bez ohľadu na ich formu, na prostriedky k ich ukladaniu a na prostriedky využívané k ich prenosu, pretože všetky tieto údaje musia byť patrične ochránené (2).

1.6 Legislatíva

Návrh bezpečnostných politík musí byť tiež v súlade s platnou legislatívou v danom štáte. V nasledujúcich kapitolách sú predstavené základné zákony a vyhlášky týkajúce sa oblasti informačnej bezpečnosti.

1.6.1 Slovenská republika

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov je transpozičným zákonom smernice Európskeho parlamentu a Rady 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Tento zákon je účinný od 1.1.2019 a upravuje:

- organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
- národnú stratégiu kybernetickej bezpečnosti,
- jednotný informačný systém kybernetickej bezpečnosti,

- organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (CSIRT) a ich akreditáciu,
- postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby,
- bezpečnostné opatrenia,
- systém zabezpečenia kybernetickej bezpečnosti,
- kontrolu nad dodržiavaním tohto zákona a audit (12).

V súvislosti so zákonom o kybernetickej bezpečnosti nadobudli 15. júna 2018 účinnosť nasledujúce vyhlášky:

- **vyhláška** Národného bezpečnostného úradu **č. 166/2018 Z. z.** o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
- **vyhláška** Národného bezpečnostného úradu **č. 165/2018 Z. z.**, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
- **vyhláška** Národného bezpečnostného úradu **č. 164/2018 Z. z.**, ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) (13).

Základná služba – služba, ktorá je zaradená v zozname základných služieb a:

1) závisí od sietí a informačných systémov a je vykonávaná aspoň v jednom sektore alebo podsektore,
2) je informačným systémom verejnej správy, alebo
3) je prvkom kritickej infraštruktúry (14).

NBÚ zaradí základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb:

1) na základe oznámenia prevádzkovateľa služby,
2) na základe podnetu ústredného orgánu, ak došlo k prekročeniu identifikačných kritérií prevádzkovanej služby,
3) z vlastnej iniciatívny, ak sa dozvedel o prekročení identifikačných kritérií a nedošlo k postupu podľa predchádzajúcich bodov (14).

Dopadové identifikačné kritéria zahŕňajú najmä:

- počet používateľov využívajúcich základnú službu,
- závislosť ostatných sektorov základnej služby,
- vplyv, ktorý by mohli mať kybernetické bezpečnostné incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti a záujmy štátu alebo na bezpečnosť štátu,
- trhový podiel prevádzkovateľa služby,
- geografické rozšírenie z hľadiska oblasti, ktorú by kybernetický bezpečnostný incident mohol postihnúť,
- význam prevádzkovateľa základnej služby z hľadiska zachovania kontinuity poskytovania služby (14).

Zákon č. 45/2011 Z.z. o kritickej infraštruktúre, účinný od 1.1.2019, ustanovuje:

- organizáciu a pôsobnosť orgánov štátnej správy na úseku kritickej infraštruktúry,
- postup pri určovaní prvku kritickej infraštruktúry,
- povinnosti prevádzkovateľa pri ochrane prvku kritickej infraštruktúry a zodpovednosť za ich porušenie (15).

Kritická infraštruktúra (KI) - systém, ktorého narušenie alebo strata funkčnosti má závažný dopad na určitú množinu užívateľov (napr. jednotlivec, rodina, firma, mesto, štát ale aj celý svet). Subjektom KI je prevádzkovateľ prvku kritickej infraštruktúry. Pre určenie prvkov kritickej infraštruktúry vo všeobecnosti platia dva typy kritérií:

- prierezové – na základe výšky škôd,
- odvetvové – špecifikujú jednotlivé odvetvia patriace do KI štátu (4).

Vyhláška č. 362/2018 Z. z. o bezpečnostných opatreniach podľa zákona o kybernetickej bezpečnosti. Táto vyhláška, ktorá nadobudla platnosť 1. januára 2019 ustanovuje poskytovateľom základných služieb obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (13).

Podľa **zákona 275/2006 Z. z.** o informačných systémoch verejnej správy (IS VS) je inštitúcia verejnej správy povinná zabezpečovať, aby bol IS VS v súlade so štandardmi IS VS. Aktuálne znenie týchto štandardov je možné nájsť vo **výnose č. 55/2014 Z. z.**, kde sú uvedené bezpečnostné štandardy inšpirované štandardom ISO 27001 (16).

Dňa 30. januára 2018 bol v zbierke zákonov Slovenskej republiky publikovaný nový **zákon č. 18/2018 Z. z.** o ochrane osobných údajov. Nahradil predchádzajúci zákon č. 122/2013 o ochrane osobných údajov. Dôvodom prijatia nového zákona bola predovšetkým celoeurópska reforma právnej úpravy ochrany osobných údajov realizovaná Všeobecným nariadením o ochrane osobných údajov označovaným ako GDPR z anglického General Data Protection Regulation. Účinnosť nadobudol 25.mája 2018 (17).

1.6.2 Európska únia

Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácií kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (13).

Smernica Európskeho parlamentu a Rady (EÚ) č. 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii je prvým právnym aktom Európskej únie zaoberajúcim sa problematikou zaručenia bezpečnosti informácií. Jej cieľom je dosiahnuť vysoký štandard bezpečnosti sietí a informačných systémov vo všetkých členských štátoch EÚ (12).

2 ANALYTICKÁ ČASŤ

Predmetom tejto časti práce je predstavenie zvolenej spoločnosti, analýza sieťovej infraštruktúry spoločnosti a vybraných oblastí systému riadenia informačnej bezpečnosti. V závere kapitoly budú predstavené požiadavky na navrhované opatrenia.

2.1 Základné údaje o spoločnosti

Obrázok č. 6: Logo nemocnice
(Zdroj: 18)

Názov:	**Nemocnica s poliklinikou Považská Bystrica**
IČO:	00610 411
DIČ:	2020705038
Sídlo:	Nemocničná 986, 017 01 Považská Bystrica
Zriaďovateľ:	Trenčiansky samosprávny kraj (TSK)

2.2 Všeobecné predstavenie spoločnosti

Základný kameň bol položený 9. mája 1952. NsP Považská Bystrica bola oficiálne otvorená 9. mája 1957. V r. 1960 dochádza k územnej reorganizácii okresov. Zlúčením okresu: Ilava, Púchov, Považská Bystrica, vznikol nový okres Považská Bystrica s následnou reorganizáciou zdravotníckych služieb, preto dochádza k rozširovaniu ako lôžkovej, tak i ambulantnej starostlivosti (18).

2.3 Zameranie spoločnosti

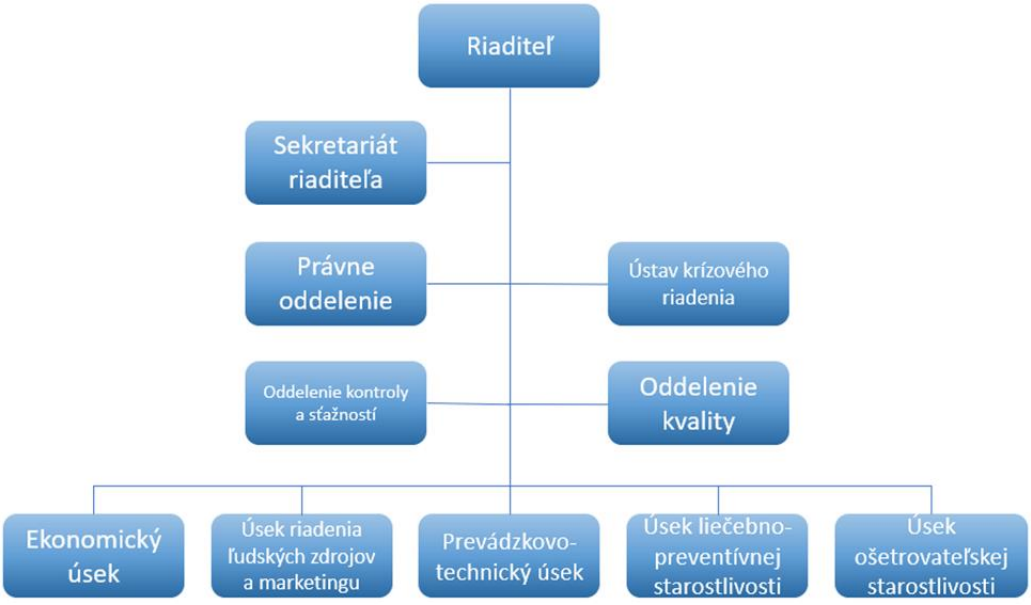
NsP poskytuje všeobecnú a špecializovanú zdravotnú starostlivosť v odboroch schválených MZ SR hlavne pacientom z regiónu Považská Bystrica, ako aj ďalším pacientom, ktorí potrebujú zdravotnú starostlivosť.

Náplň činností NsP:

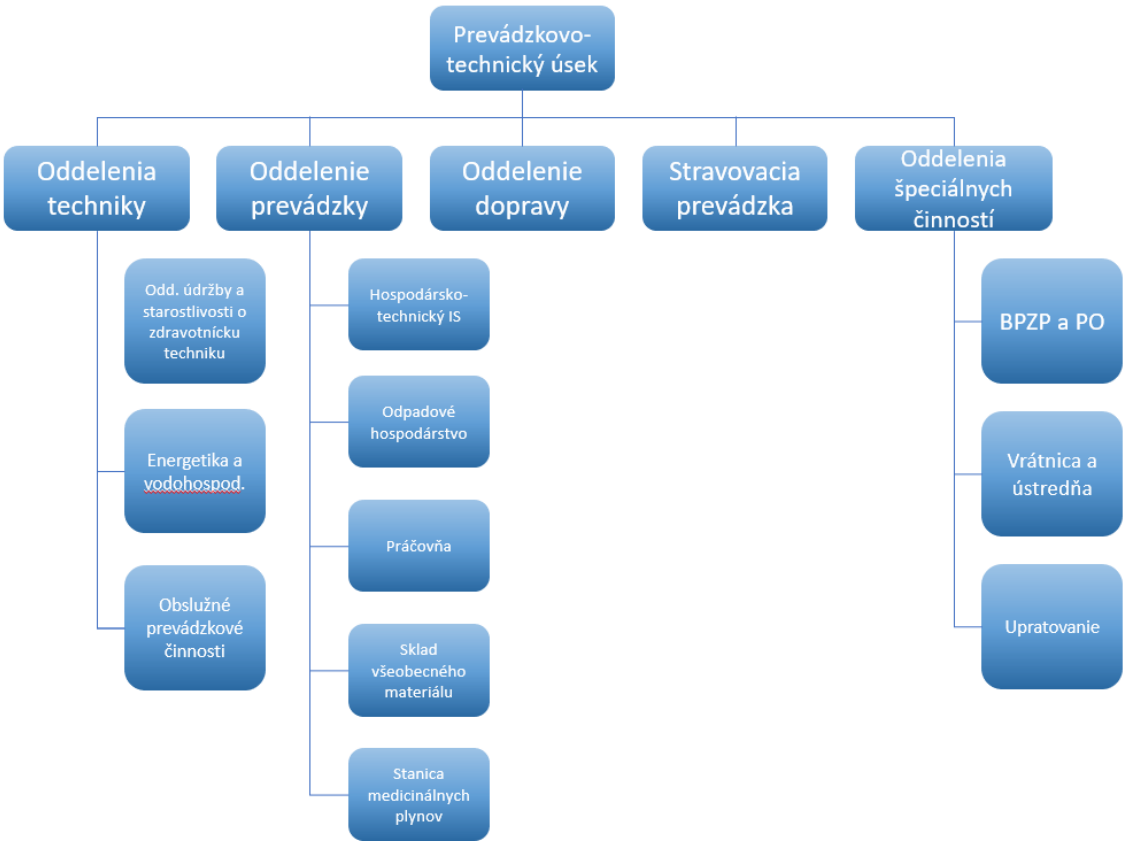
- 14 lôžkových oddelení,
- 7 zariadení spoločných vyšetrovacích a liečebných zložiek,
- špecializovaná ambulantná zdravotná starostlivosť v 42 špecializačných odboroch,
- ústavná zdravotná starostlivosť,
- lekárenská starostlivosť v nemocničnej lekárni,
- záchranná zdravotná služba,
- poskytovanie neodkladnej zdravotnej starostlivosti akémukoľvek pacientovi, ak by bez takejto pomoci bol ohrozený život alebo zdravie osoby,
- zabezpečovanie ďalšej odbornej zdravotnej starostlivosti (18).

2.4 Organizačná štruktúra spoločnosti

Na čele organizačnej štruktúry je riaditeľ nemocnice. Riaditeľovi nemocnice sa priamo zodpovedajú vedúci jednotlivých oddelení, primári a námestníci – vedúci jednotlivých úsekov. Pod oddelenie prevádzky prevádzkovo-technického úseku, konkrétne časť hospodársko-technický IS, spadajú IT oddelenie a oddelenie správy NIS, ktoré majú spoločného vedúceho oddelenia. Organizačná štruktúra Nemocnice s poliklinikou Považská Bystrica je znázornená na nasledujúcich obrázkoch.



Obrázok č. 7: Organizačná štruktúra NsP
(Zdroj: Vlastné spracovanie podľa 18)



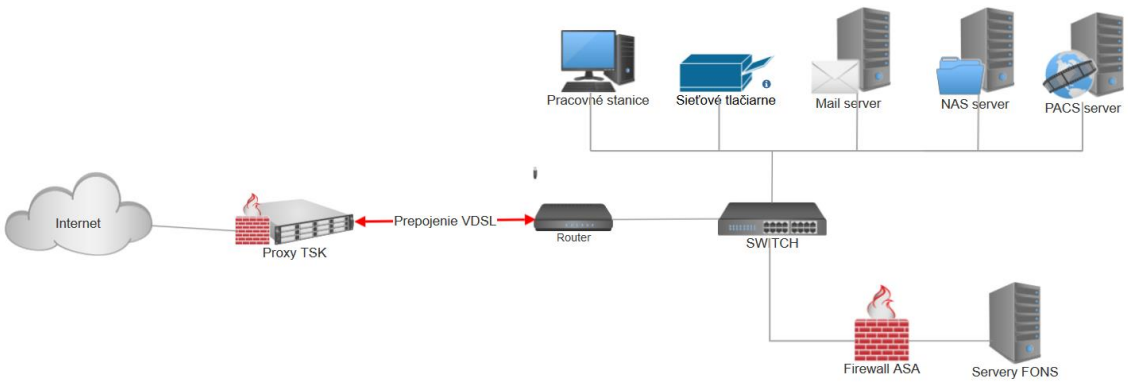
Obrázok č. 8: Organizačná štruktúra prevádzkovo-technického úseku
(Zdroj: Vlastné spracovanie podľa 18)

2.5 Analýza ICT spoločnosti

Táto podkapitola je venovaná analýze informačných a komunikačných technológií nemocnice s poliklinikou.

2.5.1 Infraštruktúra spoločnosti

Infraštruktúru spoločnosti znázorňuje zjednodušená topológia na obrázku č. 9. Prístup k internetu je zabezpečený proxy serverom a firewallom v správe zriaďovateľa. Vnútorná komunikácia so serverom FONS je zabezpečená pomocou firewallu ASA. Vo vnútornej sieti sa nachádzajú servery, tlačiarne a pracovné stanice.



Obrázok č. 9: Topológia infraštruktúry spoločnosti
(Zdroj: Vlastné spracovanie)

2.5.2 Hardwarové vybavenie

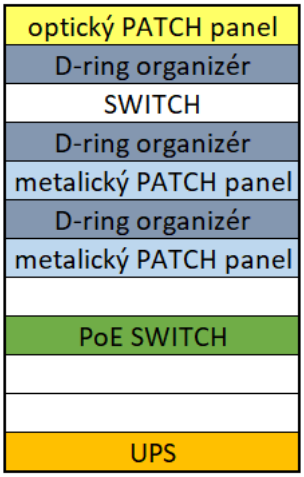
Technická miestnosť

Nemocnica má dve miestnosti slúžiace ako serverovne. Prvá, primárna, sa nachádza na treťom poschodí polikliniky. Nachádzajú sa v nej tri 42U 19´´ skriňové rozvádzače, vzduchotechnika zabezpečujúca ideálne podmienky a záložný zdroj serverovne. Usporiadanie prvkov v jednotlivých rozvádzačoch je znázornené na obrázku v Prílohách.

Druhá miestnosť sa nachádza na druhom poschodí polikliniky. Sú v nej dva 42U 19´´ skriňové rozvádzače, vzduchotechnika a takisto záložný zdroj. Jej funkcia nie je záložná, bola zriadená z kapacitných dôvodov, je v nej umiestnené najnovšie technologické vybavenie.

Obe miestnosti sú bez okien, zabezpečené certifikovanými bezpečnostnými požiarnymi dverami s päťbodovým zamykaním. V prípade výpadku distribúcie elektrickej energie je v každej miestnosti umiestnená veľká UPS značky EATON, z ktorej je napájaná celá miestnosť serverovne. Každý server má navyše svoju vlastnú UPS umiestnenú v RACK-u. Toto riešenie je schopné udržať systém v chode cca 90 minút bez distribúcie elektrickej energie. To však nie je potrebné, z dôvodu že nemocnica má vlastný naftový agregát, ktorý nabieha do 5 minút od výpadku prúdu.

Na oddeleniach sa nachádza 25 menších nástenných 12U 19 ´´ dátových rozvádzačov. Usporiadanie ich prvkov je uvedené na nasledujúcom obrázku.



Obrázok č. 10: Usporiadanie prvkov rozvádzačov na oddeleniach
(Zdroj: Vlastné spracovanie)

Pracovné stanice a notebooky

Nemocnica disponuje 300 pevnými pracovnými stanicami. Väčšina je značky HP 6200 a HP 6300. Ďalej tromi notebookmi značky Lenovo, modelová rada ThinkPad. Na všetkých pracovných staniciach je nainštalovaný operačný systém Windows 7 Pro. Momentálne prebieha postupný update všetkých pracovných staníc na Windows 10 Pro, z dôvodu ukončenia podpory Windows 7 Pro. Na všetkých počítačových zariadeniach je nainštalovaný antivírus ESET Endpoint Security.

Prenos dát

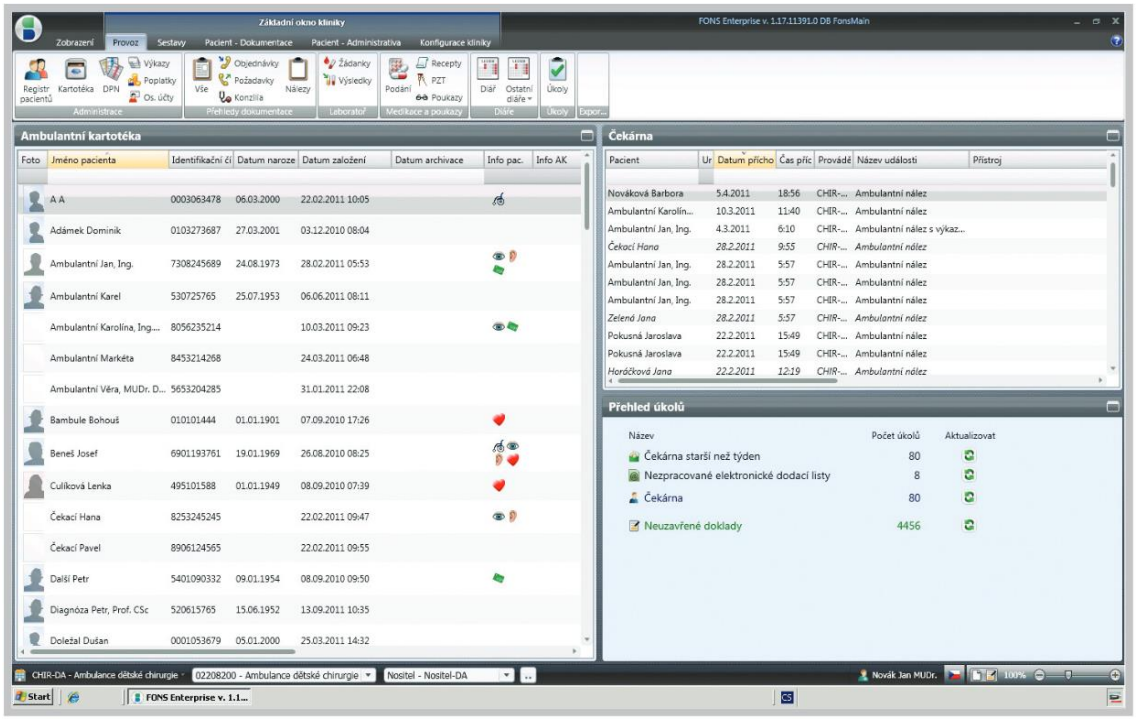
Nemocnica uskutočňuje prenos dát prostredníctvom vnútornej siete. Dáta pacientov sú ukladané priamo na dátový server spoločnosti Stapro. Zvyšné dáta sú ukladané na NAS server s RAID 5 od spoločnosti QNAP. Tieto dáta sú takisto ako dáta pacientov dostupné iba v rámci lokálnej siete nemocnice. Momentálne nemajú pracovníci umožnené pripájať sa do vnútornej siete nemocnice prostredníctvom VPN ani RDP.

Niektoré dáta z PACS systému sú pacientom nahrávané na CD nosiče. Flash disky sú využívané len v prípade údržby počítačov.

2.5.3 Softwarové vybavenie

Nemocničný IS – FONS Enterprise

FONS Enterprise je systém plne podporujúci bezpapierovú prevádzku a maximálne zdieľanie informácií v zdravotníctve. Vývoj a údržba systému je zodpovednosťou dodávateľskej spoločnosti Stapro, s.r.o. Na nasledujúcom obrázku je ukážka užívateľského rozhrania informačného systému.



Obrázok č. 11: Užívateľské rozhranie FONS Enterprise
(Zdroj: 19)

FONS Openlims

FONS Openlims je informačný systém určený pre všetky typy laboratórií. Podporuje špecifické pracovné procesy väčšiny odborností. Prístup k dátam je riešený s ohľadom na ich vysokú bezpečnosť. Systém umožňuje komunikáciu so všetkými typmi analyzátorov a rôznymi prístrojmi. Bezpečná distribúcia výsledkov v elektronickej podobe (formáty TXT, XML, rozhranie DS) podľa platnej legislatívy je zabezpečené systémom MISE, ktorý je postavené na prenose komprimovaných a zašifrovaných správ. Vývoj a údržba je opäť úlohou spoločnosti Stapro, s.r.o.

Dicompass

Dicompass je certifikovaný multiplatformový DICOM prehliadač spoločnosti MEDORO s.r.o. Software Dicompass slúži na digitalizáciu videa z endoskopie, ultrazvukov, mikroskopov ale aj ďalších zariadení, ktoré nemajú priamy DICOM výstup, prevod záznamov z digitálnych fotoaparátov, skenerov a kamier do formátu DICOM (DICOMizácia). Dicompass tiež ponúka funkcie pre rádiodiagnostiku a rádioterapiu.

2.6 Analýza určitých oblastí ISMS

Zhodnotenie miery zavedenia určitých oblastí ISMS vykonám na základe dokumentu NBÚ určeného na pomoc s auditom informačnej bezpečnosti. Na analýzu jednotlivých kritérií použijem nasledujúce hodnotenie:

Tabuľka č. 1: Hodnotiaca škála pre analýzu kritérií
(Zdroj: vlastné spracovanie podľa: 20)

Z	zavedené
ČZ	čiastočne zavedené
N	nezavedené
-	irelevantné

2.6.1 Systém riadenia bezpečnosti informácii

Je stanovený rozsah ISMS.	N
Je zavedený proces riadenia rizík.	N
Sú vytvorené, schválené a zavedené bezpečnostné politiky v oblasti ISMS, zavedené príslušné bezpečnostné opatrenia.	ČZ
Zavedený proces monitorovania bezpečnostných opatrení.	N
Zavedený proces vyhodnocovania vhodnosti a účinnosti bezpečnostnej politiky.	N
Audit kybernetickej bezpečnosti je vykonávaný najmenej 1-krát ročne.	N
Zaistené vyhodnotenie účinnosti ISMS, ktoré obsahuje hodnotenie stavu ISMS vrátane revízie hodnotenia rizík, posúdené výsledky vykonaných kontrol a auditov kybernetickej bezpečnosti a dopadov kybernetických bezpečnostných incidentov na systém riadenia bezpečnosti informácií, a to najmenej 1-krát ročne.	N
Je vykonávaná aktualizácia ISMS a súvisiaca dokumentácia na základe zistených auditov kybernetickej bezpečnosti, výsledkov hodnotenia účinnosti ISMS a v súvislosti s vykonávanými zmenami.	N

Riadená prevádzka a zdroje ISMS, zaznamenávaná činnosť spojená s ISMS a súvisiacim riadením rizík.	N

Nemocnica nemá zavedený systém riadenia informačnej bezpečnosti a takisto ani riadenie rizík. Má čiastočne zavedené bezpečnostné politiky, avšak oficiálna dokumentácia upravuje len legislatívne pravidlá pri nakladaní so zdravotnou dokumentáciou, ktorá ich zaväzuje k chráneniu citlivých dát pred ich zneužitím neoprávnenou osobou. Má zavedené riadenie aktív formou dokumentácie s názvom *Správa drobného hmotného majetku*. Kontrola prebieha raz ročne. Čo sa týka aktív z oblasti informačnej bezpečnosti, konkrétneho garanta majú určené len mobilné zariadenia. V prípade ostatných zariadení nie je garantom konkrétna osoba ale celé oddelenie, resp. jeho vedenie. Za bezpečnosť dát v IS je zodpovedné oddelenie Informačných technológií.

2.6.2 Riadenie rizík

Stanovené metodiky na identifikáciu a hodnotenie aktív a na identifikáciu a hodnotenie rizík vrátane stanovenia kritérií pre prijateľnosť rizík.	N
Vykonávaná identifikácia a hodnotenie dôležitosti aktív, a výstupy zapracuje do správy o hodnotení aktív a rizík.	N
Vykonávaná identifikácia rizík, pri ktorých sú zohľadňované hrozby a zraniteľnosti a posudzované možné dopady na aktíva. Sú určené a schválené prijateľné riziká a je spracovaná správa o hodnotení aktív a rizík.	N
Na základe bezpečnostných potrieb a výsledkov hodnotenia rizík je spracované prehlásenie o aplikovateľnosti, ktoré obsahuje prehľad vybraných a zavedených bezpečnostných opatrení.	N
Je spracovaný a zavedený plán zvládania rizík, ktorý obsahuje ciele a prínosy bezpečnostných opatrení pre zvládanie rizík, určenie osoby zodpovednej za presadzovanie bezpečnostných opatrení pre zvládanie rizík, potrebné finančné, technické, ľudské a informačné zdroje, termín ich zavedenia a popis väzieb medzi rizikami a príslušnými bezpečnostnými opatreniami.	N
Bez zbytočného odkladu sú zohľadňované reaktívne a ochranné opatrenia vydané NBÚ v hodnotení rizík a v prípade, že hodnotenie rizík aktualizované o nové zraniteľnosti spojené s realizáciou reaktívneho alebo ochranného opatrenia prekročí stanovené kritéria pre prijateľnosť rizík, sú doplnené plány zvládania rizík.	N
Riadenie rizík je zaistené inými spôsobmi a orgán a osoba doložil(a), že použité opatrenia zaisťujú rovnakú alebo vyššiu úroveň riadenia rizík.	N

Sú zvážené **hrozby** súvisiace s:	
porušením bezpečnostnej politiky, vykonaním neoprávnených činností, zneužitím oprávnenia zo strany užívateľov a administrátorov	N
poškodením alebo zlyhaním technického alebo programového vybavenia	N
zneužitie identity fyzickej osoby	N
používaním programového vybavenia v rozpore s licenčnými podmienkami	N
kybernetickým útokom z komunikačnej siete	N
škodlivým kódom (víry, spyware, trójske kone)	N
nedostatkami pri poskytovaní služieb IS a KS	N
narušením fyzickej bezpečnosti	N
prerušením poskytovania služieb elektronickej komunikácie alebo dodávky elektrickej energie	N
zneužitím alebo neoprávnenou modifikáciou údajov	N
trvale pôsobiacimi hrozbami	N
odcudzením alebo poškodením aktíva	N
porušením bezpečnostnej politiky, vykonaním neoprávnených činností, zneužitím oprávnení zo strany administrátorov KII	N
pochybením zo strany zamestnancov	N
zneužitím vnútorných prostriedkov, sabotážou	N
dlhodobým prerušením poskytovaných služieb elektronickej komunikácie, dodávky el. energie alebo iných dôležitých služieb	N
nedostatkom zamestnancov s potrebnou odbornou úrovňou	N
cieleným kybernetickým útokom pomocou sociálneho inžinierstva, použitím špionážnych techník	N
zneužitím vymeniteľných technických nosičov dát	N

Sú zvážené **zraniteľnosti**, súvisiace s:	
nedostatočnou ochranou vonkajšieho perimetru	N
nedostatočnou údržbou informačného systému KII, komunikačného systému KII alebo VIS	N
nevhodným nastavením prístupových oprávnení	N
nedostatočnými postupmi pri identifikovaní a odhalení negatívnych bezpečnostných javov, kybernetických bezpečnostných udalostí a kybernetických bezpečnostných incidentov	N

nedostatočným monitorovaním činností užívateľov a administrátorov a neschopnosťou odhaliť ich nevhodné alebo závadné spôsoby chovania	N
nedostatočným stanovením bezpečnostných pravidiel, nepresným alebo nejednoznačným vymedzením práv a povinností užívateľov, administrátorov a bezpečnostných rolí	N
nedostatočnou ochranou prostriedkov KII	N
nevhodnou bezpečnostnou architektúrou	N
nedostatočnou mierou nezávislej kontroly	N
neschopnosťou včasného odhalenia pochybenia zo strany zamestnancov	N

Riadenie rizík nie je zdokumentované. Bezpečnostné opatrenia vydávané NBÚ sú však zohľadňované a v prípade, že pracovníci IT vyhodnotia možné riziko ako neprijateľné, vykonajú potrebné opatrenia.

2.6.3 Bezpečnostná politika

Je stanovená bezpečnostná politika v oblastiach:	
systém riadenia bezpečnosti informácií	N
organizačná bezpečnosť	N
riadenie vzťahu s dodávateľmi	Z
riadenie dodávateľov	Z
klasifikácia aktív	N
bezpečnosť ľudských zdrojov	ČZ
riadenie prevádzky a komunikácií	ČZ
riadenie prístupu	ČZ
bezpečné chovanie užívateľov	N
zálohovanie a obnova	ČZ
bezpečné predávanie a výmena informácií	ČZ
riadenie technických zraniteľností	ČZ
bezpečné používanie mobilných zariadení	ČZ
poskytovanie a nadobúdanie licencií programového vybavenia a informácií	ČZ
dlhodobé ukladanie a archivácia informácií	Z
ochrana osobných údajov	Z
fyzická bezpečnosť	N
bezpečnosť komunikačnej siete	ČZ

ochrana pred škodlivým kódom	ČZ
nasadenie a používanie nástroja na detekciu kybernetických bezpečnostných udalostí	N
využitie a údržba nástroja na zber a vyhodnotenie kybernetických bezpečnostných udalostí	N
používanie kryptografickej ochrany	ČZ
Bezpečnostná politika je pravidelne aktualizovaná a jej účinnosť pravidelne hodnotená.	N

Dodávateľské vzťahy nemocnice sú upravované zákonom č. 343/2015 o verejnom obstarávaní. Bezpečnostné politiky ohľadom ochrany osobných údajov sú podmienené zákonu č. 18/2018 o ochrane osobných údajov a sú zahrnuté v dokumente *Legislatívne pravidlá pri nakladaní so zdravotnou dokumentáciou pacientov*. Tento dokument takisto obsahuje aj pravidlá archivácie zdravotnej dokumentácie.

Čiastočné zavedenie politiky znamená, že existujú pravidlá, ktoré zamestnanci dodržujú, avšak nemajú formu oficiálnej dokumentácie.

2.6.4 Organizačná bezpečnosť

Je zavedená organizácia riadenia bezpečnosti informácií, v rámci ktorej je určený výbor pre riadenie kybernetickej bezpečnosti a bezpečnostné role a ich práva a povinnosti súvisiace s informačným systémom a komunikačným systémom.	N
Je určená bezpečnostná rola: manažér kybernetickej bezpečnosti.	N
Je určená bezpečnostná rola: architekt kybernetickej bezpečnosti.	N
Je určená bezpečnostná rola: audítor kybernetickej bezpečnosti.	N
Je určená bezpečnostná rola: garant aktíva.	Z
Je určený výbor pre riadenie kybernetickej bezpečnosti.	N
Je zaistené odborné školenie osôb, ktoré zastávajú bezpečnostné role v súlade s plánom rozvoja bezpečnostného povedomia.	N

Jedinou určenou bezpečnostnou rolou sú garanti aktív. V prípade mobilných zariadení je to konkrétna osoba, oboznámená so zodpovednosťou plynúcou z prideleného aktíva. V ostatných prípadoch je garantom aktív vedenie oddelenia, ktorému bolo aktívum pridelené.

2.6.5 Stanovenie bezpečnostných požiadaviek pre dodávateľa

Sú stanovené pravidlá pre dodávateľa, ktoré zohľadňujú potreby riadenia bezpečnosti informácií a riadia svojich dodávateľov alebo iné externé subjekty, ktoré sa podieľajú na rozvoji, prevádzke alebo zaistení bezpečnosti IS alebo KS KII a VIS. Rozsah zapojenia dodávateľov na rozvoji, prevádzke alebo zaistení bezpečnosti IS alebo KS je zdokumentovaný písomnou zmluvou, ktorej súčasťou je ustanovenie o bezpečnosti informácií.	ČZ
U dodávateľov je pred uzatvorením zmluvy vykonané hodnotenie rizík, ktoré sú spojené s podstatnými dodávkami.	N
U dodávateľov sa uzatvára zmluva o úrovni služieb, ktorá stanoví spôsoby a úrovne realizácie bezpečnostných opatrení a určí vzťah vzájomnej zmluvnej zodpovednosti za zavedenie a kontrolu bezpečnostných opatrení.	ČZ
U dodávateľov sa vykonáva pravidelné hodnotenie rizík a pravidelná kontrola zavedených bezpečnostných opatrení u poskytovaných služieb a zistené nedostatky sú odstránené alebo po dohode s dodávateľom zaistí ich odstránenie.	N

V prípade dodávateľov služieb, ktorých dostupnosť závažne ovplyvňuje poskytovanie zdravotnej starostlivosti sú zmluvne určené podmienky ohľadom dostupnosti (čas na obnovu služby v prípade poruchy, sankcie v prípade nedodržania zmluvných podmienok). Takisto je zmluvne ošetrená dôvernosť a integrita údajov, ktoré sú poskytované dodávateľovi.

2.6.6 Riadenie aktív

Sú identifikované a evidované primárne aktíva.	Z
Sú určení jednotliví garanti aktív, ktorí sú zodpovední za primárne aktíva.	Z
Je hodnotená dôležitosť primárnych aktív z hľadiska dôvernosti, integrity a dostupnosti a tieto aktíva sú zaradené do jednotlivých úrovní minimálne v rozsahu podľa prílohy č. 1 k VKB	N

Pri hodnotení dôležitosti primárnych je posúdené predovšetkým:	
rozsah a dôležitosť osobných údajov alebo obchodného tajomstva	N
rozsah dotknutých právnych povinností alebo iných záväzkov	N
rozsah narušenia vnútorných riadiacich a kontrolných činností	N
poškodenie verejných, obchodných alebo ekonomických záujmov	N
možné finančné straty	N
rozsah narušenia bežných činností orgánu a osoby	N

dopady spojené s narušením dôvernosti, integrity a dostupnosti	N
dopady na zachovanie dobrého mena alebo ochranu dobrej povesti	N
Sú identifikované a evidované podporné aktíva.	N
Sú určení garanti aktív, ktorí sú zodpovední za podporné aktíva.	N
Sú určené väzby medzi primárnymi a podpornými aktívami a hodnotené dôsledky závislosti medzi primárnymi a podpornými aktívami.	N

Sú stanovené pravidlá ochrany, nutné pre zabezpečenie jednotlivých úrovní aktív tým, že:	
sú určené spôsoby rozlišovania jednotlivých úrovní aktív.	N
sú stanovené pravidlá pre manipuláciu a evidenciu s aktívami podľa úrovní aktív, vrátane pravidiel pre bezpečné elektronické zdieľanie a fyzický prenos aktív.	N
sú stanovené prípustné spôsoby používania aktív.	ČZ
sú zavedené pravidlá ochrany zodpovedajúce úrovni aktív.	ČZ
sú určené spôsoby pre spoľahlivé zmazanie alebo zničenie technických nosičov dát s ohľadom na úroveň aktív.	ČZ

Aktíva sú evidované, takisto aj ich garanti. Dôležitosť aktív však nie je hodnotená. Určité aktíva majú zvýšenú ochranu, ktorá však nie je podmienená analýze dôležitosti ale vykonáva sa intuitívne, podľa uváženie IT technikov.

2.6.7 Bezpečnosť ľudských zdrojov

Je stanovený plán rozvoja bezpečnostného povedomia, ktorý obsahuje formu, obsah a rozsah potrebných školení a sú určené osoby vykonávajúce jednotlivé činnosti, uvedené v pláne.	N
V súlade s plánom rozvoja bezpečnostného povedomia je zaistené poučenie užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role o ich povinnostiach a o bezpečnostnej politike formou vstupných a pravidelných školení.	N
Je zaistená kontrola dodržiavania bezpečnostnej politiky zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role.	ČZ
Je zaistené vrátenie zverených aktív a odobratie prístupových oprávnení pri ukončení zmluvného vzťahu s užívateľmi, administrátormi alebo osobami zastávajúcimi bezpečnostné role.	Z
O školení sú vedené prehľady, ktoré obsahujú predmet školenia a zoznam osôb, ktoré školenie absolvovali.	N

Sú stanovené pravidlá pre určenie osôb, ktoré budú zastávať bezpečnostné role, role administrátorov alebo užívateľov.	N
Je hodnotená účinnosť plánu rozvoja bezpečnostného povedomia, vykonaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia.	N
Sú určené pravidlá a postupy pre riešenie prípadov porušenia stanovených bezpečnostných pravidiel zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role.	N
Je zaistená zmena prístupových oprávnení pri zmene postavenia užívateľov, administrátorov alebo osôb zastávajúcich bezpečnostné role.	Z

Nemocnica nemá stanovený plán rozvoja bezpečnostného povedomia. Dodržiavanie bezpečnostných pravidiel je kontrolované náhodne, napríklad kontrola pridelenia prístupov pri servisnej údržbe. Pri zistení porušenia bezpečnostných pravidiel nie sú definované postupy pre ich riešenie. V prípade ukončenia zmluvného vzťahu dochádza k vráteniu pridelených aktív (v prípade mobilného zariadenia) a odobratiu prístupových oprávnení ku dňu ukončenia pracovného pomeru. Takisto je to aj v prípade zmeny postavenia užívateľov alebo administrátorov.

2.6.8 Riadenie prevádzky a komunikácií

Pomocou technických nástrojov sú detegované kybernetické bezpečnostné udalosti, pravidelne vyhodnocované získané informácie a na zistené nedostatky reagované.	ČZ

Kybernetické bezpečnostné udalosti sú detegované pomocou antivírusového/malwarového programu a firewallu.

Zaistená bezpečná prevádzka IS KII, KS KII a VIS. Za týmto účelom sú stanovené prevádzkové pravidlá a postupy.	N
Je realizované pravidelné zálohovanie a preverovanie použiteľnosti vykonaných záloh.	Z

V nemocnici sú zálohované 4 systémy. Prvým je systém FONS, ktorý je inštalovaný na samostatnom databázovom serveri. Dáta z tohto servera sú zálohované na sekundárny server. V prípade zlyhania hardwaru nedochádza k strate dát. PACS server so systémom Dicompass, je zálohovaný pomocou Mirror RAID. Ďalšie zariadenie, ktoré nemocnica používa na ukladanie dát je NAS server na ktorom je RAID 5. Zamestnanci nemocnice

majú na NAS serveri vytvorené priečinky, kde si môžu ukladať dôležité dáta. Jednotlivé priečinky majú „namapované“ na pracovných staniciach. Samostatnou jednotkou je CCTV systém, kde sa zálohuje každá IP kamera samostatne na vloženú microSD kartu. Pri momentálne používaných kartách s kapacitou 32GB, je umožnené nahratie cca 2 týždňového záznamu. Jednotlivé pracovné stanice zálohované nie sú.

Prevádzkové pravidlá a postupy orgánu a osoby obsahujú:	
práva a povinnosti osôb zastávajúcich bezpečnostné role, administrátorov a užívateľov.	ČZ
postupy pre spustenie a ukončenie chodu systému, pre reštart alebo obnovenie chodu systému po zlyhaní a pre ošetrenie chybových stavov alebo mimoriadnych javov.	N
postupy pre sledovanie kybernetických bezpečnostných udalostí a pre ochranu prístupu k záznamom o týchto činnostiach.	N
spojenie na kontaktné osoby, ktoré sú určené ako podpora pri riešené neočakávaných systémových alebo technických problémov.	ČZ
postupy riadenie a schvaľovania prevádzkových zmien.	ČZ
postupy pre sledovanie, plánovanie a riadenie kapacity ľudských a technických zdrojov.	N
Je zaistené oddelenie vývojového, testovacieho a produkčného prostredia.	Z

V súvislosti s prevádzkou IS a KS neexistuje dokument s pravidlami a postupmi. Písomnú podobu z tohto hľadiska majú len povinnosti IT oddelenia a oddelenia Prevádzkovanie nemocničného IS, ktoré sú zdokumentované v *Organizačnom poriadku NsP*. O kontaktných osobách, v prípade neočakávaných systémových alebo technických problémov, sú zamestnanci informovaní len verbálnou formou. Proces riadenia a schvaľovania prevádzkových zmien má zaužívané pravidlá a postupy avšak opäť chýba ich písomné zdokumentovanie. Nemocničný IS má oddelenú testovaciu prevádzku od ostrej prevádzky. V prípade zavádzania zmien je najskôr realizovaná niekoľkodňová testovacia prevádzka na „školskej“ verzii.

Sú riešené reaktívne opatrenia vydané NBÚ tým, že orgán a osoba:	
posudzuje očakávané dopady reaktívneho opatrenia na IS alebo KS a na zavedené bezpečnostné opatrenia, vyhodnocuje možné negatívne účinky a bez zbytočného odkladu ich oznamuje NBÚ.	ČZ
stanovuje spôsob rýchleho vykonania reaktívneho opatrenia, ktorý minimalizuje možné negatívne účinky a určuje časový plán jeho vykonania.	ČZ

Reaktívne opatrenia vydané NBÚ sú riešené a posudzované pracovníkmi IT oddelenia, ktorí stanovujú spôsoby ich vykonania v čo možno najkratšom čase. Spätná väzba o možných negatívnych účinkoch však nie je zavedená.

Je zaistená bezpečnosť a integrita komunikačných sietí a bezpečnosť komunikačných služieb.	Z
Sú určené pravidlá a postupy na ochranu informácií, ktoré sú prenášané komunikačnými sieťami.	N
Výmena a predávanie informácií je vykonávaná na základe pravidiel stanovených právnymi predpismi za súčasného zaistenia bezpečnosti informácií a tieto pravidlá sú dokumentované.	Z
S ohľadom na klasifikáciu aktív je vykonávaná výmena a predávanie informácií na základe písomných zmlúv, ktorých súčasťou je ustanovenie bezpečnosti informácií.	Z

Bezpečnosť a integrita komunikačných sietí je zaistená SSL protokolom, ktorý je aplikovaný na mailovom serveri ako aj na VoIP technológii. Pravidlá a postupy na ochranu informácií prenášaných komunikačnými sieťami neexistujú. V dokumente *Legislatívne pravidlá pri nakladaní so zdravotnou dokumentáciou pacientov* sú stanovené pravidlá pre predávanie informácií.

2.6.9 Riadenie prístupu a bezpečné chovanie užívateľov

Na základe prevádzkových a bezpečnostných potrieb je riadený prístup k IS a KS a každému užívateľovi je priradený jednoznačný identifikátor.	Z
Sú prijaté opatrenia, ktoré slúžia k zaisteniu ochrany údajov, ktoré sú používané pre prihlásenie užívateľov a administrátorov IS a KS a ktoré bránia v zneužití týchto údajov neoprávnenou osobou.	ČZ
Pristupujúcim aplikáciám je pridelený samostatný identifikátor.	Z
Je obmedzené prideľovanie administrátorských oprávnení.	Z
Prideľovanie a odoberanie prístupových oprávnení je realizované v súlade s politikou riadenia prístupu.	ČZ
Je vykonávané pravidelné preskúmanie nastavenia prístupových oprávnení vrátane rozdelenia jednotlivých užívateľov v prístupových skupinách alebo roliach.	N
Je využívaný nástroj pre overenie identity užívateľov.	Z

Sú zavedené bezpečnostné opatrenia potrebné pre bezpečné používanie mobilných zariadení, prípadne aj bezpečnostné opatrenia spojené s využitím technických zariadení, ktorými povinná osoba nedisponuje.	N

Prístup k IS a KS je riadený, prístupové údaje sú uložené v zaheslovanom dokumente. Administrátorské oprávnenia pre nemocničný IS prideľujú a odoberajú jeho správcovia (oddelenie Prevádzkovanie nemocničného IS), zvyšné oprávnenia má na starosti oddelenie IT. Administrátorské oprávnenia môžu byť udelené len pracovníkom IT oddelenia, resp. správcom nemocničného IS (v prípade IS). Kontrola pridelenia prístupov je náhodná, napríklad pri servisnej údržbe. Nemocnica nemá politiku upravujúcu riadenie prístupu, v prípade ukončenia zmluvného vzťahu dochádza k odobratiu prístupových oprávnení ku dňu ukončenia pracovného pomeru a takisto je to aj v prípade zmeny postavenia užívateľov alebo administrátorov.

2.6.10 Akvizícia, vývoj a údržba

Sú stanovené bezpečnostné požiadavky na zmeny IS a KS spojené s ich akvizíciou, vývojom a údržbou a sú zahrnuté do projektu akvizície, vývoja a údržby systému.	N
Sú identifikované, hodnotené a riadené riziká súvisiace s akvizíciou, vývojom a údržbou IS a KS.	ČZ
Je zaistená bezpečnosť vývojového prostredia a zároveň zaistená ochrana používateľských testovacích dát.	-
Je vykonávané bezpečnostné testovanie zmien IS alebo KS pred ich zavedením do prevádzky.	N

V prípade IS má na starosti vývoj a údržbu dodávajúca spoločnosť. Pri zavádzaní alebo zmenách sú v rámci projektu identifikované riziká a stanové opatrenia na ich elimináciu. Čo sa týka požiadaviek, sú definované len všeobecné požiadavky, nie bezpečnostné. Pri zavádzaní zmien do IS sa vykonáva testovacia prevádzka systému avšak tá je zameraná na správnosť chodu, nie na testovanie bezpečnosti. V prípade KS sú riziká riešené, avšak bez akejkoľvek dokumentácie.

2.6.11 Zvládanie kybernetických bezpečnostných udalostí a incidentov

Sú prijaté nevyhnutné opatrenia, ktoré zaistia oznamovanie kybernetických bezpečnostných udalostí u IS a KS zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role a o oznámeniach sú vedené záznamy.	N
Je pripravené prostredie pre vyhodnotenie oznámených kybernetických bezpečnostných udalostí a kybernetických bezpečnostných udalostí detegovaných technickými nástrojmi. Je vykonávané ich vyhodnotenie a sú identifikované kybernetické bezpečnostné incidenty.	N
Je vykonávaná klasifikácia kybernetických bezpečnostných incidentov, prijímané opatrenia pre odvrátenie a zmiernenie dopadu kybernetického bezpečnostného incidentu, vykonané hlásenie kybernetického bezpečnostného incidentu a zaistený zber vierohodných podkladov potrebných pre analýzu kybernetického bezpečnostného incidentu.	ČZ
Sú prešetrené a určené príčiny kybernetického bezpečnostného incidentu, vyhodnotená účinnosť riešenia kybernetického bezpečnostného incidentu a na základe vyhodnotenia sú stanovené nutné bezpečnostné opatrenia k zamedzeniu opakovania riešeného kybernetického bezpečnostného incidentu.	Z
Zvládanie kybernetických bezpečnostných incidentov je dokumentované.	N

Oznamovanie kybernetických bezpečnostných udalostí zo strany používateľov je vykonávané iba jednoduchým verbálnym oznámením pracovníkom oddelenia IT. V prípade, že by došlo k bezpečnostnému incidentu, bol by nahlásený NBÚ. Nemocnica incidenty neklasifikuje ani nedokumentuje, ale pracovníci IT sa snažia zmierňovať ich dopady a eliminovať ich prípadný opätovný výskyt.

2.6.12 Riadenie kontinuity činností

Sú stanovené práva a povinnosti garantov aktív, administrátorov a osôb zastávajúcich bezpečnostné role.	ČZ

Práva a povinnosti administrátorov sú zdokumentované v *Organizačnom poriadku NsP*, v prípadov garantov aktív v preberacom protokole k danému aktívu. Bezpečnostné role určené nie sú.

Sú stanovené ciele riadenia kontinuity činností formou určenia:	
minimálnej úrovne poskytovaných služieb, ktorá je prijateľná pre užívanie, prevádzku a správu IS alebo KS.	Z

doby obnovenia chodu, behom ktorej bude po kybernetickom bezpečnostnom incidente obnovená minimálna úroveň poskytovaných služieb IS alebo KS.	N
doby obnovenia dát ako termínu, ku ktorému budú obnovené dáta po kybernetickom bezpečnostnom incidente.	N

Nemocnica požaduje okamžitú obnovu (Hot Standby) IS a KS. Z tohto dôvodu je použité zrkadlenie a minimálna úroveň poskytovaných služieb je stanovená v SLA zmluvách s dodávateľmi IS, internetových a komunikačných služieb. Doba obnovy chodu a dát po kybernetickom bezpečnostnom incidente nie je uvažovaná.

Je stanovená stratégia riadenia kontinuity činností.	N
Sú vyhodnocované a dokumentované možné dopady kybernetických bezpečnostných incidentov a posúdené možné riziká súvisiace s ohrozením kontinuity činností.	N
Sú stanovené, aktualizované a pravidelne testované plány kontinuity činností IS a KS.	N
Sú realizované opatrenia na zvýšenie odolnosti IS a KS voči kybernetickému bezpečnostnému incidentu a je využívaný nástroj na zaisťovanie úrovne dostupnosti.	Z

Zvýšená odolnosť IS a KS je zabezpečená použitím firewallu a antivírusového softwaru. Dostupnosť je zaistená použitím redundancie hardwaru (v prípade výpadku el. energie viacnásobnej).

Sú stanovené a aktualizované postupy na zavedenie opatrení vydaných NBÚ, v ktorých je zohľadňované:	
výsledky hodnotenia rizík vykonania opatrení	ČZ
stav dotknutých bezpečnostných opatrení	ČZ
vyhodnotenie prípadných negatívnych dopadov na prevádzku a bezpečnosť IS alebo KS.	ČZ

Pracovníci IT vyššie spomínané záležitosti vyhodnocujú avšak opäť je to bez dokumentácie a v nej stanovených postupov.

2.6.13 Kontrola a audit kybernetickej bezpečnosti

Je posúdený súlad bezpečnostných opatrení s všeobecne záväznými právnymi predpismi, vnútornými predpismi, inými predpismi a zmluvnými záväzkami vzťahujúcimi sa k IS a KS a sú určené opatrenia na jeho presadenie.	Z
Sú vykonávané a dokumentované pravidelné kontroly dodržovania bezpečnostnej politiky a výsledky týchto kontrol sú zohľadnené v pláne rozvoja bezpečnostného povedomia a pláne zvládania rizík.	N
Je zaistené vykonanie auditu kybernetickej bezpečnosti osobou s odbornou kvalifikáciou , ktorá hodnotí správnosť a účinnosť zavedených bezpečnostných opatrení.	N
Pre IS alebo KS je vykonávaná kontrola zraniteľnosti technických prostriedkov pomocou automatizovaných nástrojov a ich odborné vyhodnocovanie a na zistené zraniteľnosti je reagované.	N

Každé opatrenie je posúdené z hľadiska súladu s predpismi či už právnymi, internými alebo zmluvnými záväzkami. Pravidelné kontroly dodržovania bezpečnostnej politiky, zraniteľnosti technických prostriedkov ani audit kybernetickej bezpečnosti sa nevykonáva.

2.6.14 Fyzická bezpečnosť

Sú prijaté nevyhnutné opatrenia k zamedzeniu neoprávneného vstupu do vymedzených priestorov, kde sú spracované informácie a umiestnené technické aktíva IS alebo KS.	ČZ
Sú prijaté nevyhnutné opatrenia k zamedzeniu poškodenia a zásahom do vymedzených priestorov, kde sú uchovávané informácie a umiestnené technické aktíva IS alebo KS.	Z
Predchádza sa poškodeniu, krádeži alebo kompromitácii aktív alebo prerušeniu poskytovania služieb IS alebo KS.	Z
Sú uplatnené prostriedky fyzickej bezpečnosti na zaistenie ochrany na úrovni objektov.	Z
Sú uplatnené prostriedky fyzickej bezpečnosti pre zaistenie ochrany v rámci objektov zaistením zvýšenej bezpečnosti vymedzených priestorov, v ktorých sú umiestnené technické aktíva IS a KS.	Z

Zamestnanci nemocnice majú pridelené kľúče len od miestností, ktoré nevyhnutne potrebujú na vykonávanie svojho povolania. Do serverovní majú prístup iba pracovníci IT oddelenia, tak isto aj do RACK skríň, ktoré sú umiestnené na jednotlivých

oddeleniach. Ďalej sú na niektorých oddeleniach nemocnice nainštalované kódové zámky na hlavných dverách. Tieto zámky umožňujú prístup len poverených osôb na jednotlivé oddelenia.

2.6.15 Nástroj na overovanie identity užívateľov

Sú používané nástroje na overovanie identity užívateľov a administrátorov IS a KS.	Z
Nástroj na overovanie identity užívateľov, ktorý používa autentizáciu len heslom, zaisťuje:	
minimálnu dĺžku hesla 12 znakov	N
minimálna zložitosť hesla tak, že heslo bude obsahovať aspoň tri z nasledujúcich 4 požiadaviek: najmenej jedno veľké písmeno najmenej jedno malé písmeno najmenej jednu číslicu najmenej jeden špeciálny znak, ktorý nie je uvedený v bodoch 1 až 3	ČZ
Maximálna doba pre povinnú výmenu hesla nepresahuje 100 dní. (Táto požiadavka nie je vyžadovaná pre samostatné identifikátory aplikácií.)	N
Je používaný nástroj na overovanie identity, ktorý:	
zamedzuje opätovnému používaniu predošlých používaných hesiel a neumožní viac zmien hesla jedného užívateľa behom stanoveného obdobia, ktoré musí byť najmenej 24 hodín.	N
vykonáva opätovné overenie identity po určitej doby nečinnosti.	ČZ
využíva nástroj na overenie identity administrátorov. V prípade, že tento nástroj využíva autentizáciu heslom, zaistí presadenie minimálnej dĺžke hesla 17 znakov.	N

Čo sa týka pracovných staníc, na jednej stanici pracuje aj niekoľko zamestnancov (v niektorých prípadoch aj 10), preto je na staniciach vytvorené len jedno používateľské konto, ktoré na počítačoch s operačným systémom Windows 7, nie je zabezpečené heslom. Na počítačoch, kde je operačný systém Windows 10, je na používateľskom konte vytvorené heslo. Tieto počítače sú inštalované s jednotným heslom, jednotliví zamestnanci sú upozorňovaní na potrebu zmeny hesla. Na konte administrátora je vytvorené heslo, ktoré poznajú výlučne pracovníci oddelenia IT. Do nemocničného informačného systému FONS, má každý zamestnanec vytvorené vlastné prihlasovacie meno a heslo. Pri vytváraní nového používateľského konta je heslo generované náhodne. Po prvom prihlásení je užívateľ vyzvaný na zmenu hesla, heslo musí obsahovať

minimálne 8 znakov, 1 veľké písmeno a číslicu alebo špeciálny znak. Do PACS systému majú prístup len používatelia, ktorí na výkon povolania potrebujú prístup k röntgenovým/sono snímkam(lekári ORT, rádiológovia). Používateľské kontá vytvárajú pracovníci oddelenia IT za prítomnosti daného lekára, preto si heslo určuje od počiatku daný zamestnanec. Heslo však musí obsahovať minimálne 8 znakov. Prístup do priečinkov na NAS serveri vytvárajú pracovníci IT. Heslá sú generované náhodne, obsahujú 8 znakov, malé a veľké písmená a číslice. Zamestnanci heslá nemôžu meniť.

2.6.16 Nástroj pre riadenie prístupových oprávnení

Je používaný nástroj na riadenie prístupových oprávnení, ktorým je zaistené riadenie oprávnení:	
na prístup k jednotlivým aplikáciám a dátam.	Z
na čítanie dát, na zápis dát a na zmenu oprávnení.	Z
Je používaný nástroj pre riadenie prístupových oprávnení, ktorý zaznamenáva použitie prístupových oprávnení v súlade s bezpečnostnými potrebami a výsledkami hodnotenia rizík.	N

Riadenie prístupu k jednotlivým aplikáciám je vykonávané obmedzením nutných inštalovaných aplikácii pre jednotlivých užívateľov. V praxi to znamená, že na každú pracovnú stanicu sú inštalované iba aplikácie, ktoré daný užívateľ potrebuje na výkon svojho povolania.

2.6.17 Nástroj pre ochranu pred škodlivým kódom

Pre riadenie rizík spojených s pôsobením škodlivého kódu je používaný nástroj pre ochranu IS a KS pred škodlivým kódom, ktorý zaistí overenie a stálu kontrolu:	
komunikácie medzi vnútornou a vonkajšou sieťou.	Z
serverov a zdieľaných dátových úložísk.	Z
pracovných staníc.	Z
Je vykonávaná pravidelná aktualizácia nástroja na ochranu pred škodlivým kódom, jeho definícií a signatúr.	Z

Nemocnica využíva na ochranu komunikácie medzi vnútornou a vonkajšou sieťou firewall od spoločnosti Fortigate. Na každý server a pracovnú stanicu je inštalovaný antivírusový program ESET Endpoint Security.

2.6.18 Nástroj na zaznamenávanie činnosti

Je používaný nástroj na zaznamenávanie činností IS a KS, ktorý zaisťuje:	
zber informácií o prevádzkových a bezpečnostných činnostiach, hlavne typ činnosti, dátum a čas, identifikáciu technického aktíva, ktoré činnosť zaznamenalo, identifikáciu pôvodcu a miesta činnosti a úspešnosť alebo neúspešnosť činnosti.	Z
ochranu získaných informácií pred neoprávneným čítaním alebo zmenou.	Z
Pomocou nástroja na zaznamenávanie činnosti IS a KS je zaznamenávané:	
prihlásenie a odhlásenie užívateľov a administrátorov.	Z
činnosť vykonaná administrátormi.	Z
činnosť vedúca ku zmene prístupových oprávnení.	Z
nevykonanie činnosti v dôsledku nedostatku prístupových oprávnení a ďalšie neúspešné činnosti užívateľov.	N
zahájenie a ukončenie činností technických aktív IS a KS.	N
automatické varovné alebo chybové hlásenie technických aktív.	N
prístupy k záznamom o činnostiach, pokusy o manipuláciu so záznamami o činnostiach a zmeny nastavenia nástroja na zaznamenávanie činnosti.	Z
použitie mechanizmov identifikácie a autentizácie vrátane zmeny údajov, ktoré slúžia na prihlásenie.	Z
Najmenej raz za 24 hodín je vykonávaná synchronizácia jednotného systémového času technických aktív patriacich do IS alebo KS.	Z
Záznamy činností sú uchovávané najmenej po dobu 3 mesiacov.	Z

Nemocničný IS zaznamenáva všetky udalosti ako napr. prihlásenie jednotlivých užívateľov, predpisovanie liekov, zmenu v medikácii do logov. K synchronizácií systémového času dochádza každých 8 hodín a záznamy činností sú uchovávané počas 3 mesiacov.

2.6.19 Nástroj na detekciu kybernetických bezpečnostných udalostí

Je používaný nástroj na detekciu kybernetických bezpečnostných udalostí, ktorý vychádza zo stanovených bezpečnostných potrieb a výsledkov hodnotenia rizík a ktorý zaistí overenie, kontrolu a prípadné zablokovanie komunikácie medzi vnútornou komunikačnou sieťou a vonkajšou sieťou.	Z
Je používaný nástroj na detekciu kybernetických bezpečnostných udalostí, ktorý zaistí overenie, kontrolu a prípadné zablokovanie komunikácie:	

v rámci vnútornej komunikačnej siete.	Z
serverov patriacich do IS a KS.	Z

Nemocnica využíva na ochranu komunikácie medzi vnútornou a vonkajšou sieťou proxy server a firewall, ktorý je u zriaďovateľa. Samotná nemocnica disponuje ďalším firewallom, ktorý slúži na ochranu komunikácie medzi FONS servermi a pracovnými stanicami. Na každý server a pracovnú stanicu je inštalovaný antivírusový program ESET Endpoint Security.

2.6.20 Nástroj na zber a vyhodnotenie kybernetických bezpečnostných udalostí

Je používaný nástroj na zber a priebežné vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý v súlade s bezpečnostnými potrebami a výsledkami hodnotenia rizík zaisťuje:	
integrovaný zber a vyhodnotenie kybernetických bezpečnostných udalostí z IS a KS.	N
poskytovanie informácií pre určené bezpečnostné role o detegovaných kybernetických bezpečnostných udalostiach v IS alebo KS.	N
nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí s cieľom identifikácie kybernetických bezpečnostných incidentov, vrátane včasného varovania určených bezpečnostných rolí.	N
Je zaistená pravidelná aktualizácia nastavení pravidiel pre vyhodnocovanie kybernetických udalostí a včasné varovanie, aby boli obmedzené prípady nesprávneho vyhodnotenia udalostí alebo prípady falošných varovaní.	N
Zaistené využívanie informácií, ktoré sú pripravené nástrojom na zber a vyhodnotenie kybernetických bezpečnostných udalostí, na optimálne nastavenie bezpečnostných opatrení IS a KS.	N

Nemocnica nevyužíva žiadny nástroj na zber a vyhodnocovanie kybernetických bezpečnostných udalostí.

2.6.21 Aplikačná bezpečnosť

Sú vykonávané bezpečnostné testy zraniteľnosti aplikácií, ktoré sú prístupné z vonkajšej siete a to pred ich uvedením do prevádzky a po každej zásadnej zmene bezpečnostných mechanizmov.	N

Je zaistená trvalá ochrana aplikácií a informácií dostupných z vonkajšej siete pred neoprávnenou činnosťou, popretím vykonaných činností, kompromitácií alebo neautorizovanou zmenou.	Z
Je zaistená trvalá ochrana transakcií pred ich nedokončením, nesprávnym smerovaním, neautorizovanou zmenou predávaného dátového obsahu, kompromitáciou, neautorizovaným duplikovaním alebo opakovaním.	N

Ochrana aplikácií a informácií je riešená prostredníctvom firewallu, spam filtru a obmedzením oprávnení a prístupu. Testy zraniteľnosti sa však nevykonávajú. Nie je zaistená ani trvalá ochrana transakcií.

2.6.22 Kryptografické prostriedky

Pre používanie kryptografickej ochrany je/sú stanovené:	
úroveň ochrany s ohľadom na typ a silu kryptografického algoritmu	N
pravidlá kryptografickej ochrany informácií pri prenose po komunikačných sieťach alebo pri uložení na mobilné zariadenie alebo vymeniteľné technické nosiče dát.	N
V súlade s bezpečnostnými potrebami a výsledkami hodnotenia rizík sú používané kryptografické prostriedky, ktoré zaistia ochranu dôvernosti a integrity predávaných alebo ukladaných dát a preukázanie zodpovednosti za vykonané činnosti.	N
Pre ochranu kryptografických prostriedkov je stanovený systém správy kľúčov, ktorý zaistí generovanie, distribúciu, ukladanie, archiváciu, zmeny, ničenie , kontrolu a audit kľúčov.	N
Sú používané odolné kryptografické algoritmy a kryptografické kľúče	Z

V rámci kryptografickej ochrany je používaný autentizačný certifikát SSL.

Nástroj na zaisťovanie úrovne dostupnosti

V súlade s bezpečnostnými potrebami a výsledkami hodnotenia rizík je používaný nástroj na zaisťovanie úrovne dostupnosti informácií.	ČZ
Je používaný nástroj na zaisťovanie úrovne dostupnosti informácií, ktorý zaisťuje:	
dostupnosť IS a KS pre splnenie cieľov riadenia kontinuity činností.	ČZ
odolnosť IS a KS voči kybernetickým bezpečnostným incidentom, ktoré by mohli znížiť dostupnosť.	Z
Zálohovanie dôležitých technických aktív IS a KS využitím redundancie v návrhu riešenia a zaistením náhradných technických aktív v určenom čase.	Z

Dostupnosť informácii je zabezpečená zálohovaním a redundanciou diskov ale nie na základe hodnotenia rizík. Dostupnosť IS je zaisťovaná pomocou redundanciou serverov a diskových polí. Voči kybernetickým bezpečnostným incidentom sa nemocnica chráni pomocou spam filtra, antivírusového programu a firewallu.

2.6.23 Zhrnutie analýzy

Nasledujúca tabuľka a graf zobrazujú súhrnné informácie z vykonanej analýzy požiadaviek.

Tabuľka č. 2: Zhrnutie analýzy
(Zdroj: Vlastné spracovanie)

Z	zavedené	49	24%
ČZ	čiastočne zavedené	37	18%
N	nezavedené	119	58%
-	irelevantné	1	0,005%

Obrázok č. 12: Zhrnutie analýzy
(Zdroj: Vlastné spracovanie)

Z uvedených údajov vyplýva, že aktuálna miera zavedenia ISMS v analyzovaných oblastiach je na úrovni približne 42%, z ktorých takmer polovica je zavedená len čiastočne. Nasledujúca tabuľka zobrazuje aktuálnu mieru zavedenia jednotlivých oblastí bezpečnostných opatrení a povinnosť resp. odporučenie ich zavedenia. Zo zistených údajov vyplýva, že najväčšie nedostatky má organizácia v oblasti administrácie riadenia informačnej bezpečnosti. Neexistuje takmer žiadna požadovaná ani odporúčaná dokumentácia a pracovné postupy sa vykonávajú intuitívne, na základe rozhodnutia jednotlivých zamestnancov.

Tabuľka č. 3: Aktuálna miera zavedenia bezpečnostných opatrení
(Zdroj: Vlastné spracovanie)

Oblasť bezpečnostných opatrení	Aktuálna miera zavedenia	Povinné/ odporúčané
Organizácia informačnej bezpečnosti	28%	odporúčané
Riadenie aktív, hrozieb a rizík	7%	povinné
Personálna bezpečnosť	25%	povinné
Riadenie dodávateľských služieb, akvizície, vývoja a údržby IS	22%	povinné
Technická zraniteľnosť systémov a zariadení	0%	povinné
Riadenie bezpečnosti sietí a IS	74%	povinné
Riadenie prevádzky	50%	povinné
Riadenie prístupov	50%	povinné
Kryptografické opatrenia	20%	odporúčané
Riešenia kybernetických bezpečnostných incidentov	30%	povinné
Monitorovanie, testovanie bezpečnosti a bezpečnostných auditov	34%	povinné
Fyzická bezpečnosť a bezpečnosť prostredia	90%	odporúčané
Riadenie kontinuity procesov	47%	povinné

2.7 Požiadavky

V roku 2018 vznikla nemocnici povinnosť nahlásiť sa NBÚ ako poskytovateľ základnej služby a záväzok splniť požiadavky na bezpečnostné opatrenia vyplývajúce z vyhlášky č. 362/2018 Z. z. Nemocnica preto požaduje zavedenie povinných, prípadne odporúčaných požiadaviek platných pre poskytovateľa základnej služby II. kategórie. Požadovaná je taktiež maximálna efektívnosť navrhovaných opatrení z hľadiska finančného aj časového.

3 NÁVRH VLASTNÉHO RIEŠENIA

Obsahom kapitoly venovanej návrhu vlastného riešenia je analýza rizík, na základe ktorej budú navrhnuté konkrétne opatrenia za účelom zníženia miery rizík na ich prijateľnú úroveň. Záver kapitoly je venovaný ekonomickému zhodnoteniu navrhovaných opatrení.

3.1 Analýza rizík

Pri analýze rizík budem vychádzať z doporučení normy ISO/IEC 27005. Podľa metodiky spomínanej normy sa analýza rizík skladá z identifikácie a hodnotenia aktív, identifikácie hrozieb a zraniteľností a následného vytvorenia matice zraniteľnosti a matice rizík.

3.1.1 Identifikácia a hodnotenie aktív

Pri hodnotení aktív je dôležitým faktorom najmä miera závažnosti možného dopadu spôsobeného porušením dostupnosti, dôvernosti či integrity daného aktíva. Na hodnotenie aktív som zvolila hodnotiacu škálu od 1 do 5, ktorá je bližšie popísaná v nasledujúcej tabuľke.

Tabuľka č. 4: Hodnotiaca škála pre aktíva
(Zdroj: Vlastné spracovanie podľa: 2, s. 267)

Hodnota aktíva	Hodnotenie dopadu
1 – Veľmi nízka	Žiadny dopad na spoločnosť
2 – Nízka	Zanedbateľný dopad na spoločnosť
3 – Stredná	Problémy alebo finančná strata
4 – Vysoká	Vážne problémy či podstatné finančné straty
5 – Veľmi vysoká	Existenčné problémy

V nasledujúcej tabuľke sú uvedené aktíva spoločnosti spolu s ich hodnotením. Tabuľka obsahuje len aktíva pre spoločnosť najdôležitejšie, ktoré sú rozdelené do rôznych kategórií.

Tabuľka č. 5: Hodnotenie aktív
(Zdroj: Vlastné spracovanie)

Kategória	Aktívum		C	I	A	H
Dáta	Osobné dáta pacientov		5	5	5	5
	Osobné dáta zamestnancov		5	4	3	4
	Interné dáta		3	3	3	3
	Zálohy dát	FONS	5	5	5	5
		PACS	4	5	4	4
	Kamerový systém		3	3	3	3
Hardware	Server	FONS	5	5	5	5
		PACS	4	5	4	4
		NAS	3	3	2	3
		MAIL	4	4	4	4
	Pracovné stanice		3	2	3	3
	Diagnostické prístroje		4	5	4	4
	Mobilné zariadenia		2	2	3	2
	Tlačiarne		3	3	4	3
	Kamerový systém		3	2	3	3
	IP telefónia		4	4	5	4
	Firewall		5	5	5	5
	Sieťové prvky	aktívne	5	5	5	5
		pasívne	5	5	5	5
	Záložné zdroje	UPS	1	2	4	2
		naftový generátor	1	2	5	3
Software	Nemocničný IS (FONS)		5	5	5	5
	PACS systém		4	5	4	4
	Operačný systém	servery	5	5	5	5
		pracovné stanice	3	3	3	3
	Antivírusový program		5	5	5	5
	Software kamerového systému		3	2	3	3
Služby	Internetové pripojenie		5	5	5	5
	Elektrická energia		5	5	5	5
	WWW		3	3	3	3
	Kamerový systém		3	2	3	3

3.1.2 Identifikácia hrozieb a zraniteľností

V ďalšom kroku identifikujem hrozby, ktoré môžu vplývať či už na jedno alebo na viaceré aktíva identifikované v predchádzajúcej podkapitole. Identifikované hrozby následne ohodnotím číslom od 1 do 5, pričom jednotlivé hodnoty vyjadrujú pravdepodobnosť výskytu týchto hrozieb. Vysvetlenie hodnotiacej škály je zobrazené v nasledujúcej tabuľke.

Tabuľka č. 6: Hodnotiaca škála pravdepodobnosti výskytu hrozieb
(Zdroj: Vlastné spracovanie, podľa: 2, s. 267)

Hodnota	Pravdepodobnosť výskytu hrozby
1	Veľmi nepravdepodobný
2	Málo pravdepodobný
3	Pravdepodobný
4	Veľmi pravdepodobný
5	Takmer istý

Nasledujúca tabuľka obsahuje identifikované hrozby, rozdelené do skupín podľa príbuznosti charakteru, spolu s určením ovplyvnených bezpečnostných atribútov a hodnotením pravdepodobnosti ich výskytu.

Tabuľka č. 7: Identifikované hrozby
(Zdroj: Vlastné spracovanie)

Hrozba	Vplyv na [C, I, A]	Pravdepodobnosť výskytu
Prírodné hrozby		
Požiar	I, A	3
Voda	I, A	4
Prírodné katastrofy	A	2
Technické zlyhania		
Zlyhanie zariadení alebo systémov	C, I, A	3
Nesprávne fungovanie zariadení alebo systémov	C, I, A	3
Strata služieb		
Zlyhanie alebo prerušenie poskytovaných služieb	C, I, A	2
Zlyhanie alebo prerušenie dodávky energie	I, A	3
Zlyhanie alebo prerušenie zdrojov energie	A	1

Nedostatok zdrojov	A	3
Ohrozenie informácií		
Odpočúvanie	C	3
Špionáž	C	3
Sociálne inžinierstvo	C, I	3
Strata údajov	A	3
Neoprávnené činnosti		
Neoprávnený vstup do priestorov	C, I, A	4
Krádež zariadení, pamäťových médií alebo dokumentov	C, A	3
Strata zariadení, pamäťových médií alebo dokumentov	C, A	2
Zničenie zariadení alebo pamäťových médií	A	2
Prezradenie citlivej informácie	C	3
Informácie z nespoľahlivého zdroja	C, I, A	3
Manipulácia s hardwarom a softwarom	C, I, A	2
Krádež informácie	I	4
Prinútenie, vydieranie, korupcia	C, I, A	3
Krádež identity	C, I, A	3
Zneužitie osobných údajov	C	3
Zneužitie oprávnení	C, I, A	2
Škodlivý software	C, I, A	2
Zlyhanie ľudského faktoru		
Nesprávne používanie alebo správa zariadení a systémov	C, I, A	3
Absencia personálu	A	3

Príklady zraniteľností jednotlivých identifikovaných hrozieb sú uvedené v nasledujúcej tabuľke.

Tabuľka č. 8: Príklady zraniteľností jednotlivých hrozieb
(Zdroj: Vlastné spracovanie)

Hrozba	**Príklad zraniteľnosti**
Požiar	Manipulácia s horľavinami
Voda	Manipulácia s vodou, prívalové dažde
Prírodné katastrofy	Záplava, silný vietor, zásah bleskom
Zlyhanie zariadení alebo systémov	Nedostatky v plánoch kontinuity

Nesprávne fungovanie zariadení alebo systémov	Nedostatočná údržba alebo doladenie zariadení alebo systémov
Zlyhanie alebo prerušenie poskytovaných služieb	Nedostatočná dohoda o úrovni poskytovaných služieb (SLA)
Zlyhanie alebo prerušenie dodávky energie	Nedostatočná dohoda o úrovni poskytovaných služieb (SLA)
Zlyhanie alebo prerušenie zdrojov energie	Citlivosť na zmeny napätia
Nedostatok zdrojov	Nedostatočná finančná rezerva
Odpočúvanie	Nechránené komunikačné linky
Špionáž	Nedostatočne bezpečná sieťová infraštruktúra
Sociálne inžinierstvo	Nedostatočné školenie / Nechránené pripojenie do verejnej siete
Strata údajov	Nedostatočné zálohovanie dát
Neoprávnený vstup do priestorov	Nedostatočná fyzická ochrana
Krádež zariadení, pamäťových médií alebo dokumentov	Nedostatočná fyzická ochrana
Strata zariadení, pamäťových médií alebo dokumentov	Chýba stanovenie zodpovednosti za IB v pracovnej náplni
Zničenie zariadení alebo pamäťových médií	Nedodržanie pravidelnej výmeny hardwaru
Prezradenie citlivej informácie	Nedostatočné školenie pracovníkov
Manipulácia s hardwarom a softwarom	Absencia pravidiel používania hardwaru a softwaru
Krádež informácie	Chýbajúca „politika čistého stola a čistej obrazovky“
Prinútenie, vydieranie, korupcia	Chýba stanovenie zodpovednosti za IB v pracovnej náplni
Krádež identity	Slabý management hesiel
Zneužitie osobných údajov	Chýbajúce procedúry upravujúce narábanie s informáciami, na ktoré sa vzťahuje ochrana osobných údajov
Zneužitie oprávnení	Neodhlásenie sa pri opúšťaní pracovnej stanice
Škodlivý software	Ukončenie licencie antivírusového programu
Nesprávne používanie alebo správa zariadení a systémov	Nedostatočná údržba, školenie, pridelenie prístupových práv
Absencia personálu	Neprimeraná alebo nedbalá kontrola fyzického prístupu do budovy, miestností, kancelárií

3.1.3 Matica zraniteľnosti

Ďalším krokom v hodnotení aktív je zostavenie matice zraniteľnosti. Zobrazuje úroveň zraniteľnosti medzi aktívom a hrozbou, pričom určitá hrozba nemusí ovplyvňovať všetky aktíva ale len niektoré a to v rôznom meradle. Interval pre hodnotenie zraniteľnosti je opäť v rozmedzí od 1 do 5, kde vyššie číslo značí vyššiu zraniteľnosť.

Tabuľka č. 9: Matica zraniteľnosti
(Zdroj: Vlastné spracovanie)

Zraniteľnosť [V]	**Popis aktíva**	DÁTA					
		Osobné dáta pacientov	Osobné dáta zamestnancov	Interné dáta	Zálohy		
					FONS	PACS	Kamerový systém
	A	5	4	3	5	4	3
Popis hrozby	**T**						
Požiar	3	2	2	2	2	2	2
Voda	4	3	3	3	3	3	1
Prírodné katastrofy	2	1	1	1	1	1	1
Zlyhanie zariadení alebo systémov	3	3	2	3	1	1	1
Nesprávne fungovanie zariadení alebo systémov	3						
Zlyhanie alebo prerušenie poskytovaných služieb	2						
Zlyhanie alebo prerušenie dodávky energie	3	1	1	1	1	1	1
Zlyhanie alebo prerušenie zdrojov energie	1						
Nedostatok zdrojov	3						
Odpočúvanie	3	3	3	3			
Špionáž	3	2	2	3	2	2	2
Sociálne inžinierstvo	3	4	4	4			
Strata údajov	3	3	3	2	3	2	2
Neoprávnený vstup do priestorov	4	2	2	2	1	1	1
Krádež zariadení, pamäťových médií alebo dokumentov	3	4	2	2	1	1	1
Strata zariadení, pamäťových médií alebo dokumentov	2	3	1	1			
Zničenie zariadení alebo pamäťových médií	2	2	3	3	2	2	2

Prezradenie citlivej informácie	3	3	3	3			
Manipulácia s hardwarom a softwarom	3						
Krádež informácie	4	4	3	3			
Prinútenie, vydieranie, korupcia	3	2	1	1			
Krádež identity	3	4	2	2			
Zneužitie osobných údajov	3	2	1	1			
Zneužitie oprávnení	2	3	3	3			
Škodlivý software	2	2	2	2	1	1	1
Nesprávne používanie alebo správa zariadení a systémov	3	2	2	2	1	1	1
Absencia personálu	3						

3.1.4 Matica rizík

Posledným krokom k vyhodnoteniu aktív je vytvorenie matice rizík. Hodnoty v matici sú výsledkom súčinu hodnoty hrozby, aktíva a zraniteľnosti. Výpočet znázorňuje aj nasledujúci vzťah:

$$\mathbf{R = T \times A \times V}$$

R = miera rizika

T = pravdepodobnosť vzniku hrozby

A = hodnota aktíva

V = zraniteľnosť

Miera rizika získaná spomínaným postupom sa následne vyhodnotí na základe nasledujúcej tabuľky podľa príslušnosti do konkrétneho intervalu hodnôt.

Tabuľka č. 10: Hodnotiaca škála rizík
(Zdroj: Vlastné spracovanie podľa:2, s. 268)

Hranice	Stupeň rizika
0 - 9	Bezvýznamné riziko
10 - 19	Akceptovateľné riziko
20 - 39	Mierne riziko
40 - 59	Nežiadúce riziko
viac ako 60	Neprijateľné riziko

Tabuľka č. 11: Matica rizík
(Zdroj: Vlastné spracovanie)

Úroveň rizika [R]	**Popis aktíva**	DÁTA					
		Osobné dáta pacientov	Osobné dáta zamestnancov	Interné dáta	Zálohy		
					FONS	PACS	Kamerový systém
	A	5	4	3	5	4	3
Popis hrozby	**T**						
Požiar	3	30	24	18	30	24	18
Voda	4	60	48	36	60	48	12
Prírodné katastrofy	2	10	8	6	10	8	6
Zlyhanie zariadení alebo systémov	3	45	24	27	15	12	9
Nesprávne fungovanie zariadení alebo systémov	3						
Zlyhanie alebo prerušenie poskytovaných služieb	2						
Zlyhanie alebo prerušenie dodávky energie	3	15	12	9	15	12	9
Zlyhanie alebo prerušenie zdrojov energie	1						
Nedostatok zdrojov	3						
Odpočúvanie	3	45	36	27			
Špionáž	3	30	24	27	30	24	18
Sociálne inžinierstvo	3	60	48	36			
Strata údajov	3	45	36	18	45	24	18
Neoprávnený vstup do priestorov	4	40	32	24	20	16	12
Krádež zariadení, pamäťových médií alebo dokumentov	3	60	24	18	15	12	9
Strata zariadení, pamäťových médií alebo dokumentov	2	30	8	6			
Zničenie zariadení alebo pamäťových médií	2	20	24	18	20	16	12
Prezradenie citlivej informácie	3	45	36	27			
Manipulácia s hardwarom a softwarom	3						
Krádež informácie	4	80	48	36			
Prinútenie, vydieranie, korupcia	3	30	12	9			
Krádež identity	3	60	24	18			
Zneužitie osobných údajov	3	30	12	9			
Zneužitie oprávnení	2	30	24	18			
Škodlivý software	2	20	16	12	10	8	6

Nesprávne používanie alebo správa zariadení a systémov	3	30	24	18	15	12	9
Absencia personálu	3						

3.1.5 Vyhodnotenie rizík

Zo zostavenej matice rizík som vytvorila tabuľku, obsahujúcu hrozby s neprijateľnou úrovňou miery rizika a aktíva, na ktoré vplývajú.

Tabuľka č. 12: Vyhodnotenie rizík
(Zdroj: Vlastné spracovanie)

Hrozba	**Úroveň miery rizika**	**Aktívum**
Voda	60	Osobné dáta pacientov
	60	Záloha dát - FONS
	60	Server - FONS
	60	Firewall
	60	Sieťové prvky - aktívne
Nedostatok zdrojov	75	Internetové pripojenie
	75	Elektrická energia
Sociálne inžinierstvo	60	Osobné dáta pacientov
Neoprávnený vstup do priestorov	60	Sieťové prvky - pasívne
Krádež zariadení, pamäťových médií alebo dokumentov	60	Osobné dáta pacientov
Krádež informácie	80	Osobné dáta pacientov
	80	Nemocničný IS (FONS)
Krádež identity	60	Osobné dáta pacientov

Hrozby, ktoré predstavujú pre nemocnicu najväčší zdroj rizika, sa týkajú osobných dát pacientov, čo vychádza zo samotnej podstaty organizácie. Zraniteľnosť pre ich krádež vzniká v dôsledku nepozornosti personálu a neodhlasovania sa pri odchode z pracovného miesta. Zamestnanci často krát ani neskrývajú dokumenty s osobnými dátami pacientov (napr. zdravotné záznamy) pred ostatnými pacientmi. S touto hrozbou súvisí aj fakt, že do priestorov, kde sa nachádzajú osobné dáta pacientov a pracovné stanice s nemocničným IS, má prístup aj verejnosť, v niektorých prípadoch bez dohľadu personálu. Táto skutočnosť je hrozbou aj pre pasívne sieťové prvky, keďže v niektorých častiach je kabeláž vedená voľne, bez ochrany vo forme lišty. Personál nemá dostatočné

bezpečnostné povedomie, čím vzniká priestor pre hrozby akými sú sociálne inžinierstvo či krádež identity. Ďalším rizikovým faktorom je aj umiestnenie hlavnej serverovne na najvyššom poschodí budovy. Stav strechy je neuspokojivý, čím vzniká riziko pre dôležité aktíva umiestnené v serverovni.

Chod nemocnice je závislý od dodávky elektrickej energie a internetového pripojenia, čo síce má ošetrené v dohode o úrovni poskytovaní služieb ale nemá vytvorené finančné rezervy na dodržanie zmluvných záväzkov čím sa vystavuje riziku následkov ich nedodržania.

3.1.6 Výber bezpečnostných opatrení

Na základe analýzy rizík a povinností vyplývajúcich zo zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., budú navrhnuté opatrenia pokrývať nasledujúce oblasti:

- riadenie aktív, hrozieb a rizík,
- personálna bezpečnosť,
- riadenie dodávateľských služieb, akvizície, vývoja a údržby IS,
- technická zraniteľnosť systémov a zariadení,
- riadenie bezpečnosti sietí a IS,
- riadenie prevádzky,
- riadenie prístupov,
- riešenia kybernetických bezpečnostných incidentov,
- riadenie kontinuity procesov,
- monitorovanie, testovanie bezpečnosti a bezpečnostných auditov.

Návrh bude zahŕňať aj opatrenia pre oblasti, ktoré sú pre danú kategóriu poskytovateľa základnej služby len odporúčané:

- organizácia informačnej bezpečnosti,
- kryptografické opatrenia,
- fyzická bezpečnosť a bezpečnosť prostredia.

3.2 Návrh bezpečnostných opatrení

A.5 Politika informačnej bezpečnosti

A.5 1 Usmernenie pre informačnú bezpečnosť

Cieľ: *Poskytnúť usmernenie pre riadenie a podporu informačnej bezpečnosti v súlade s požiadavkami organizácie a relevantnými zákonmi.*

A.5.1.1 Politiky informačnej bezpečnosti

Vytvorenie dokumentu Bezpečnostná politika NsP PB, ktorý bude vyjadrovať podporu vedenia nemocnice so zavádzaním bezpečnosti informácií. Zároveň bude jeho obsahom:

- definovanie rozsahu bezpečnosti informácií, jej ciele a princípy, ktorým budú podriadené všetky činnosti súvisiace s bezpečnosťou informácií,
- určenie bezpečnostných rolí a priradenie ich zodpovednosti,
- prehlásenie o potrebe bezpečnosti zdravotníckych informácií,
- ciele bezpečnosti zdravotníckych informácií,
- stanovenie spôsobu oznamovania bezpečnostných incidentov.

S obsahom bezpečnostnej politiky musia byť oboznámení všetci zamestnanci a takisto relevantné tretie strany.

Bezpečnostnú politiku bude dopĺňať už existujúci dokument *Legislatívne pravidlá pri nakladaní so zdravotnou dokumentáciou pacientov.*

A.5.1.2 Preskúmanie politiky informačnej bezpečnosti

Preskúmavanie politiky informačnej bezpečnosti v minimálne ročnom intervale, za účelom zaistenia neustálej vhodnosti, primeranosti a efektívnosti bezpečnostných politík. Revízia dokumentu je nutná aj v prípade vyskytnutia sa zmeny väčšieho rozsahu. Preskúmanie je zodpovednosťou manažéra informačnej bezpečnosti.

A.6 Organizácia informačnej bezpečnosti

A.6.1 Vnútorná organizácia

Cieľ: *Zaviesť rámec riadenia na zahájenie a riadenie implementácie a prevádzky informačnej bezpečnosti v organizácií.*

A.6.1.1 Roly a zodpovednosti

V záujme riadenia a koordinácie bezpečnosti informácií stanovenie nasledujúcich rolí a ich zodpovedností:

- **vedenie** – dohliadanie na realizáciu systému bezpečnosti informácií, definovanie politiky bezpečnosti informácií, určenie rolí a ich zodpovedností, podieľanie sa na hodnotení aktív a rizík.
- **manažéra informačnej bezpečnosti** – implementácia a rozvoj informačnej bezpečnosti, tvorba návrhov bezpečnostných smerníc a ich preskúmavanie, riadenie rizík, spracovanie bezpečnostných incidentov a ich ohlasovacia povinnosť. Z hľadiska organizačnej štruktúry zodpovedá priamo vedeniu nemocnice.
- **IT oddelenie** – vykonávanie bezpečnostných opatrení, konfigurácia hardwaru a softwaru v súlade s bezpečnostnými politikami, výber a implementácia technologických prostriedkov a posúdenie ich vplyvu na zavedené bezpečnostné opatrenia, školenie zamestnancov o správnom používaní zariadení a dodržiavaní bezpečnostných opatrení, prijímanie informácií o poruchách a bezpečnostných incidentoch a ich nahlásenie manažérovi informačnej bezpečnosti.
- **správca NIS** – zabezpečovanie správy, údržby, servisu a ďalších činností spojených s prevádzkovaním IS v NsP PB.
- **vlastníci aktív** – zodpovednosť za pridelené aktívum, hlásenie bezpečnostných incidentov pracovníkom IT oddelenia.

Jednotlivé role môžu delegovať úlohy s bezpečnostným zameraním na iné osoby, zodpovednosť však zostáva na nich. Zodpovednosť za bezpečnosť zdravotníckych informácií má v rámci organizácie každý, kto s týmito dátami pracuje.

Stanovenie smernice, ktorá bude definovať spôsob koordinácie bezpečnosti informácií. Vedenie nemocnice sa vďaka tejto smernici stane spoluzodpovedným za vzájomnú koordináciu pri riešení bezpečnostných incidentov. V prípade výskytu bezpečnostného incidentu sú zamestnanci povinní informovať o tom pracovníkov IT oddelenia, ktorý daný problém riešia podľa vopred daného postupu. Následne pracovníci IT oddelenia problém hlásia manažérovi informačnej bezpečnosti, ktorý ho ďalej spracováva. Každý

bezpečnostný incident alebo problém musí byť hlásený postupom stanoveným v Bezpečnostnej politike NsP PB a riadne zdokumentovaný.

A.6.1.2 Princíp oddelenia povinností

V rámci zamedzenia úmyselného či neúmyselného zneužitia prístupu k aktívam zo strany interných zamestnancov striktné pridelenie osobných prihlasovacích údajov do počítača každému zamestnancovi. Zavedenie centralizovaného systému správy užívateľov pre jednoduchú správu oprávnení zamestnancov.

A.6.1.3 Kontakt s autoritami

Zavedenie postupov, ktoré určujú kto a kedy môže kontaktovať autority a tiež spôsob včasného hlásenia identifikovaných bezpečnostných incidentov. Ohlasovaciu povinnosť dohliadajúcemu orgánu Slovenskej republiky má na starosť manažér informačnej bezpečnosti v prípade výskytu bezpečnostného incidentu, a to bez zbytočných odkladov, ideálne do 72 hodín od porušenia informačnej bezpečnosti.

A.6.1.4 Kontakt so zvláštnymi záujmovými skupinami

Udržiavanie kontaktu a priradenie zodpovednosti za kontakt s odbornými záujmovými skupinami, odbornými fórami a profesijnými združeniami v oblasti informačnej bezpečnosti manažérovi informačnej bezpečnosti v spolupráci s vedením. Vyjadrovať sa v mene organizácie, alebo jej súčasti do akýchkoľvek diskusných skupín, môžu len zamestnanci, ktorí sú riadne poverení komunikáciou s médiami. Ostatní používatelia Internetu a elektronickej pošty sa môžu zúčastňovať na diskusiách a fórach v priebehu pracovnej doby, ak sa to vzťahuje na ich odbornú činnosť, ale v tom prípade vystupujú ako jednotlivci vo vlastnom mene a sú povinní informovať ostatných zúčastnených, že nie sú oprávnení vystupovať v mene organizácie alebo jej súčasti. Pri účasti v diskusiách a fórach je nutné zdržať sa akýchkoľvek politických, náboženských, rasových prejavov, prejavov neznášanlivosti a prejavov urážajúcich ľudskú dôstojnosť, či prejavov týkajúcich sa trestnej činnosti.

A.6.2 Mobilné zariadenia a práca na diaľku

Cieľ: *Dosiahnuť bezpečnosť pri práci na diaľku a pri používaní mobilných zariadení.*

A.6.2.1 Politika mobilných zariadení

Zavedenie politiky, ktorá bude definovať povinnú registráciu mobilných zariadení a ich vlastníkov, požiadavky na fyzickú ochranu, obmedzenie inštalácie softwaru, požiadavky na verziu softwaru a riadenie prístupu.

V súčasnosti organizácia disponuje tromi mobilnými zariadeniami s operačným systémom Android. Pre zvýšenie bezpečnosti mobilných zariadení navrhujem použitie Eset Mobile Security. Ročné náklady na licenciu pre jedno zariadenie sú v čase písania práce na úrovni 10€. V prípade ich odcudzenia je vhodné nastavenie použitia kódového zámku obrazovky a tiež vybraných aplikácií a tiež automatické uzamknutie zariadenia po určitom časovom intervale.

A.6.2.2 Práca na diaľku

V súčasnosti nie je zamestnancom umožnená práca na diaľku ani používanie vlastných zariadení. V prípade budúceho zavádzania tohto riešenia je nutné zavedenie bezpečnostných opatrení aj v tejto oblasti, napríklad zavedenie kryptovaného prenosu minimálne cez protokol SSH a nepoužívať pre autorizáciu vstupy meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite, prípadne využiť zabezpečenú VPN.

A.7 Personálna bezpečnosť

A.7.1 Pred nástupom do zamestnania

Cieľ: *Zabezpečiť, že zamestnanci a zmluvní partneri rozumejú svojej zodpovednosti a sú vhodní na výkon rolí, ktoré im boli pridelené.*

A.7.1.1 Preverovanie

Určenie osoby, ktorá bude zodpovedná za overenie životopisu, totožnosti a výpisu Registra trestov GP SR žiadateľa o zamestnanie, prípadne posudku od jeho bývalého zamestnávateľa. Všetky zhromaždené údaje musia byť uchovávané v súlade so zákonom o ochrane osobných údajov.

A.7.1.2 Podmienky pracovného pomeru

Stanovenie zmluvných zodpovedností zamestnancov či zmluvných strán za bezpečnosť informácií. V prípade zamestnancov či zmluvných strán, ktoré počas náplne svojej práce

prichádzajú do styku so zdravotnou dokumentáciou a inými osobnými dátami zároveň podpísanie **zmluvy o mlčanlivosti**, ktorej obsahom budú aj informácie o právnej zodpovednosti a možných opatreniach a následkoch (napr. sankcie, ukončenie pracovného pomeru a pod.) v prípade jej porušenia. Podpísanie zmluvy o mlčanlivosti musí prebehnúť pred udelením prístupu k aktívam a jej platnosť trvá aj po rozviazaní pracovného pomeru. Zamestnanec či zmluvná strana musí byť o všetkých spomínaných skutočnostiach informovaná pred podpisom zmluvy prijímajúcim pracovníkom.

A.7.2 Počas zamestnania

Cieľ: *Zabezpečiť, aby zamestnanci alebo zmluvní partneri poznali a plnili svoju zodpovednosť v oblasti informačnej bezpečnosti.*

A.7.2.1 Manažérska zodpovednosť

Zahrnutie zodpovedností vedenia týkajúcich sa presadzovania a aplikovania informačnej bezpečnosti do bezpečnostnej politiky organizácie. Stanovenie a zavedenie procesu informovania zamestnancov o predpisoch a ich zodpovednostiach.

A.7.2.2 Rozvoj bezpečnostného povedomia

Vytvorenie plánu rozvoja bezpečnostného povedomia zamestnancov, ktorý zahŕňa:

- predstavenie bezpečnostných politík organizácie,
- predstavenie opatrení, zavedených na ochranu informácií,
- spôsoby zaobchádzania s dátami, pracovnými stanicami,
- trénovanie schopnosti rozoznať pokus o útok,
- spôsob reagovania v prípade podozrenia na bezpečnostný incident,
- poučenie z minulých bezpečnostných incidentov.

Plán rozvoja bezpečnostného povedomia je periodicky vyhodnocovaný a neustále zlepšovaný.

Formy vzdelávania zamestnancov:

- klasické školenia
    - cielené na jednotlivé skupiny zamestnancov podľa úrovne ich znalostí o informačnej bezpečnosti,
    - zúčastniť sa musia všetci zamestnanci, ktorí prichádzajú do styku s informáciami a informačnými technológiami,

    - tréning schopnosti rozoznať útok realizovaný formou simulácií a cvičení,
    - nutná aktuálnosť (napr. v prípade technologických zmien, nových hrozieb, zraniteľností a techník útočníkov),
- informačné fórum v intranete,
- informácie prostredníctvom mailov ohľadom súčasných bezpečnostných hrozieb,
- upozornenie na prihlasovacej obrazovke pri prihlasovaní sa do pracovnej stanice,
- informačný plagát upozorňujúci na bezpečné správanie sa umiestnený k pracovným staniciam a tiež tam, kde zamestnanci na niečo čakajú a čas môže byť využitý na čítanie (napr. výťah, kuchynka). Príklad takéhoto plagátu je uvedený v Prílohách.
- e-learningové kurzy odporúčané manažérom informačnej bezpečnosti,
- v prípade pracovníkov IT oddelenia a manažéra informačnej bezpečnosti účasť na seminároch a konferenciách zaoberajúcich sa informačnou bezpečnosťou.

Viesť prezenčné listiny školení (príklad prezenčnej listiny uvedený v Prílohách) a zaviesť tiež periodické dotazníky na vyhodnotenie bezpečnostného povedomia zamestnancov a dodávateľov. Aspoň raz ročne overiť ich porozumenie politikám informačnej bezpečnosti a postupom, ako aj ich role v týchto postupoch. Vykonávať pravidelné cvičenia na overenie, či si zamestnanci a dodávatelia plnia svoje povinnosti v oblasti informačnej bezpečnosti napr. overenie, či zamestnanci kliknú na odkaz v podozrivom e-maile, alebo či poskytnú citlivé informácie cez telefón bez dostatočnej autentifikácie volajúceho.

A.7.2.3 Disciplinárne konanie

Vytvorenie formalizovaného postupu v prípade konania vedúceho k narušeniu informačnej bezpečnosti za účelom spravodlivého zaobchádzania so zamestnancami. Disciplinárny proces by mal zohľadňovať rozsah dopadu konania zamestnanca, úmyselnosť jeho činov, prípadné predchádzajúce porušenie bezpečnostných politík a na základe spomínaných skutočností uložiť napomenutie alebo v prípade závažného narušenia určenie finančnej sankcie na základe vzniknutých škôd, ukončenie pracovného pomeru prípadne riešenie problému súdnou cestou.

A.7.3 Ukončenie a zmena zamestnania

Cieľ: *Ochrániť záujmy organizácie ako súčasť procesu zmeny alebo ukončenia zamestnania.*

A.7.3.1 Zodpovednosti pri ukončení alebo zmene pracovného vzťahu

V rámci ukončenia pracovného pomeru oboznámenie daného zamestnanca s trvaním právnych zodpovedností vyplývajúcich zo zmluvy o mlčanlivosti. Zamestnanec je povinný odovzdať všetky aktíva, ktoré mu boli počas pracovného pomeru pridelené na výkon jeho práce a sú mu odňaté všetky pridelené prístupy (deaktivovanie emailovej adresy, odobratie kľúčov a pod.). Zvýšenú pozornosť venovať ukončeniu pracovného pomeru z dôvodu nespokojnosti na strane zamestnanca, pretože nespokojný zamestnanec je jednou z najčastejších príčin bezpečnostných incidentov.

V prípade zmeny pracovného pomeru je nutný podpis novej pracovnej zmluvy, čím sú ukončené súčasné zodpovednosti a zároveň zahájený nový pracovný pomer a z neho vyplývajúce zodpovednosti.

Pridelenie zodpovednosti za výkon procedúr spojených s ukončením alebo zmenou pracovného vzťahu konkrétnym zamestnancom. Je nutná spolupráca personálneho oddelenia a oddelenia IT.

A.8 Riadenie aktív

A.8.1 Zodpovednosť za aktíva

Cieľ: *Identifikovať aktíva organizácie a definovať zodpovednosť za primeranú ochranu.*

A.8.1.1 Zoznam aktív

Vytvorenie centralizovaného inventáru aktív, v ktorom budú identifikované a evidované všetky:

- aktíva a ich klasifikácia,
- vlastníci aktív,
- osoby zodpovedné za identifikáciu a evidenciu aktív.

Je nutná aktuálnosť inventáru aktív, každá zmena musí byť zaevidovaná bez zbytočného odkladu a kontrola správnosti dokumentu vykonávaná raz ročne. Viesť takisto zoznam vyradených aktív, v ktorom budú uvedené vyradené aktíva minimálne po dobu dvoch rokov spolu s dátumom ich vyradenia.

Identifikátor aktív je vytvorený kombináciou:

- typu aktíva:

- DT – dáta,
- HW – hardware,
- SW – software,
- SL – služby,

- trojmiestneho poradového čísla.

Postup klasifikácie aktív je rovnaký ako v prípade hodnotenia aktív v kapitole 3.1.1 Identifikácia a hodnotenie aktív.

Tabuľka č. 13: Návrh dokumentu Inventár aktív
(Zdroj: Vlastné spracovanie)

<table>
<tr><th colspan="6">Inventár aktív</th></tr>
<tr><td colspan="5">Zodpovedná osoba:</td><td rowspan="2">interný dokument</td></tr>
<tr><td colspan="5">Dátum poslednej úpravy:</td></tr>
<tr><th rowspan="2">ID</th><th rowspan="2">Aktívum</th><th colspan="3">Dopad na C, I, A</th><th rowspan="2">Dátum zaradenia</th><th rowspan="2">Vlastník</th></tr>
<tr><th colspan="3">Hodnota aktíva</th></tr>
<tr><td rowspan="2">HW001</td><td rowspan="2">osobné dáta pacientov</td><td>5</td><td>5</td><td>5</td><td rowspan="2">1.1.2018</td><td rowspan="2">každý, kto s nimi pracuje</td></tr>
<tr><td colspan="3">5</td></tr>
<tr><td rowspan="2">SW001</td><td rowspan="2">nemocničný IS (FONS)</td><td>5</td><td>5</td><td>5</td><td rowspan="2">1.7.2018</td><td rowspan="2">správca NIS</td></tr>
<tr><td colspan="3">5</td></tr>
<tr><td rowspan="2">SL001</td><td rowspan="2">kamerový systém</td><td>3</td><td>2</td><td>3</td><td rowspan="2">1.1.2019</td><td rowspan="2">oddelenie IT</td></tr>
<tr><td colspan="3">3</td></tr>
<tr><td>...</td><td>...</td><td colspan="3"></td><td>...</td><td>...</td></tr>
</table>

A.8.1.2 Vlastníctvo aktív

Priradenie každého aktíva konkrétnemu vlastníkovi. Vlastníkom aktíva môže byť jednotlivec alebo entita, nesúca plnú zodpovednosť za dané aktívum. Zodpovednosť za zdravotnícku dokumentáciu nesú všetci, ktorí s ňou pracujú. V prípade ukončenia pracovného alebo zmluvného vzťahu dochádza k vráteniu spravovaného aktíva a odobratiu prístupových práv zamestnanca.

A.8.1.3 Prípustné použitie aktív

Vytvorenie a implementácia pravidiel pre prípustné používanie informácií a aktív a zabezpečenie ich ochrany, ktorých charakter a rozsah je závislý od klasifikácie

informačných aktív. Pravidlá sú povinní dodržiavať zamestnanci a tiež zainteresované strany, ktoré majú k aktívam určitý prístup. Z tohto dôvodu je nutné sprístupnenie spomínaných pravidiel vo forme politiky všetkým zainteresovaným stranám.

A.8.1.4 Vrátenie aktív

Stanovenie formálneho procesu vrátenia pridelených aktív pri ukončení pracovného pomeru so zamestnancom, respektíve zmluvy s dodávateľom, ktorý je zaznamenaný vo forme výstupného listu zamestnanca.

A.8.2 Klasifikácia informácií

Cieľ: *Zabezpečiť, aby informácie dostali vhodnú úroveň ochrany v závislosti od ich dôležitosti pre organizáciu.*

A.8.2.1 Klasifikácia informácií

Zavedenie klasifikácie všetkých informácií a dokumentov organizácie v papierovej aj elektronickej podobe na základe ich dopadu na organizáciu..

Tabuľka č. 14: Klasifikácia informácií
(Zdroj: Vlastné spracovanie podľa: 11)

Klasifikácia	Dopad
Tajné	Zničujúci dopad
Dôverné	Veľmi negatívny dopad
Interné	Negatívny dopad
Verejné	Žiadny dopad

Osobné dáta pacientov (zdravotná dokumentácia, laboratórne výsledky) sú vždy klasifikované ako dôverné. Internými informáciami sa rozumejú informácie súvisiace s činnosťou organizácie, napríklad smernice.

A.8.2.2 Označovanie informácií

Zavedenie označovania dokumentov v papierovej aj elektronickej podobe podľa ich klasifikácie na prednej strane dokumentu, v pravom hornom rohu alebo na obale dátového nosiča. Označenie dokumentu pri jeho vzniku alebo prebratí od externej strany je úlohou osoby zaň zodpovednej. S klasifikáciou aj spôsobom označovania informácií oboznámiť zamestnancov aj zainteresované strany.

A.8.2.3 Manipulácia s informáciami

Stanoviť zásady pre manipuláciu s informáciami, ktorých cieľom je také spracovanie údajov, ktoré rešpektuje práva dotknutých osôb a neporušuje práva na zachovanie ľudskej dôstojnosti alebo ochranu súkromia. V prípade uschovávania dôverných informácií je nutné ich fyzické uzamknutie alebo zabezpečenie počítača a informačného systému prístupovým heslom. Odporúčam zavedenie nasledujúcich zásad:

- zákonnosť – spracovanie osobných a citlivých údajov len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby,
- obmedzenie účelu – získavanie údajov len na konkrétny výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom nezlučiteľným s týmto účelom,
- minimalizácia osobných údajov – údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú,
- správnosti – údaje musia byť správne, presné a aktualizované tak, aby sa zabezpečilo, že sa údaje, ktoré sú nesprávne, bezodkladne vymažú alebo opravia,
- minimalizácia uchovávania – uchovávanie údajov, kým je to potrebné na účel, na ktorý sa spracúvajú,
- integrita a dôvernosť – spracovanie údajov spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť údajov vrátane ochrany pred neoprávneným a nezákonným spracovaním údajov, náhodnou stratou, výmazom alebo poškodením,

V prípade zasielania informácií zaviesť nasledujúce pravidlá:

- odosielanie listinnej dokumentácie prostredníctvom doručenej pošty alebo kuriéra,
- elektronické dokumenty zasielané výhradne prostredníctvom nemocničných e-mailových adries,
- cezhraničný prenos údajov do krajiny, ktorá nezaručuje primeranú úroveň ochrany údajov uskutočniť len s písomným súhlasom dotknutej osoby. Súhlas musí obsahovať názov krajiny, ako aj upozornenie, že táto krajina nezaručuje primeranú úroveň ochrany údajov.

A.8.3 Manipulácia s médiami

Cieľ: *Zabrániť neautorizovanému vyzradeniu, úprave, zmazaniu alebo zničeniu informácií uložených na médiách.*

A.8.3.1 Správa výmenných médií

Stanovenie a implementácia politiky pre správu výmenných médií zahŕňajúcich napríklad pravidlá pre ich evidenciu, uloženie v bezpečnom prostredí v súlade so špecifikáciami výrobcu a šifrovanie dôverných dát uložených na médiách. Je tiež potrebné dáta preniesť na nové médium v prípade ich degradácie v záujme predídenia ich úplnej straty.

A.8.3.2 Likvidácia médií

Stanovenie formálnych postupov likvidácie médií spolu s pridelením zodpovedností za ich výkon. Média obsahujúce dôverné alebo tajné informácie musia byť zlikvidované až po odstránení týchto dát. Zmazanie súborov a formátovanie diskov nestačí, je nutné použitie spoľahlivej metódy zmazania dát, napríklad pomocou špeciálnych softwarových nástrojov alebo fyzickou likvidáciou.

A.8.3.3 Fyzický prenos médií

Zavedenie pravidiel pre fyzický prenos médií, ktorý by mal byť realizovaný spoľahlivým prepravcom (napr. kuriérskou službou). Citlivé dáta je nutné ochrániť pred neoprávneným prístupom ich šifrovaním.

A.9 Riadenie prístupu

A.9.1 Požiadavky na riadenie prístupu

Cieľ: *Obmedziť prístup k informáciám a zariadeniam spracúvajúcim informácie.*

A.9.1.1 Politika riadenia prístupu

Stanovenie politiky riadenia prístupu k informáciám a zariadeniam na spracovanie informácií, ktorá zohľadňuje klasifikáciu informácií a je založená na princípoch „need-to-know“ a „všetko, čo nie je povolené, je zakázané“.

A.9.1.2 Prístup k sieti a sieťovým službám

Keďže momentálne má nemocnica zapojené v počítačovej siete len stolné počítače, riadenie prístupu do siete je jednoduché - používajú sa pevne pridelené IP adresy. Dátové

zásuvky by nemali byť voľne prístupné. V prípade dodatočného zriadenia WLAN siete pre pacientov odporúčam túto sieť striktne oddeliť pomocou VLAN.

A.9.2 Riadenie prístupu užívateľov

Cieľ: *Zabezpečiť autorizovaným používateľom prístup a zabrániť neautorizovaný prístup k systémom a službám.*

A.9.2.1 Registrácia a zrušenie užívateľa

Každému používateľovi siete a informačného systému pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému. V prípade nemocničného IS je táto požiadavka splnená, v súčasnosti sa však do rovnakého konta na počítači prihlasuje niekoľko používateľov. Navrhujem zavedenie Active Directory Domain Servera, kde bude mať každý užívateľ vytvorené svoje vlastné konto s jemu určenými privilégiami. Ako login odporúčam použitie jedinečného ID, ktoré bude pozostávať z prvých troch písmen priezviska a osobného čísla zamestnanca.

Určenie osoby zodpovednej za riadenie prístupu užívateľov, ktorými sú v prípade informačného systému správcovia NIS, čo sa týka siete IT technici. Ich zodpovednosť zahŕňa prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej politiky.

Užívatelia budú mať zriadené všetky potrebné účty v prvý deň nástupu do zamestnania. IT technik, respektíve správca NIS vytvorí účet na základe písomnej žiadosti. Žiadosť musí obsahovať pravdivé a správne vyplnené údaje, za ktoré zodpovedá osoba žiadateľa. Zriadiť a dodržiavať proces na zrušenie prístupu vypnutím účtov okamžite po ukončení pracovného pomeru so zamestnancom alebo dodávateľom. Po zrušení účtu je potrebné zašifrovať a presunúť s ním spojené súbory na bezpečný server na analýzu.

A.9.2.2 Zriadenie prístupu užívateľa

Je potrebné identifikovať požiadavky pre prístup jednotlivých používateľov (princíp need-to-know) k skupinám informácii a na ich základe definovať ACL (Access Control List). Zapnúť detailné logovanie na všetkých serveroch, aby bolo možné vystopovať pokus o neoprávnený prístup alebo situáciu, kedy niekto pristupoval k dátam, ku ktorým by nemal pristupovať.

A.9.2.3 Riadenie privilegovaných prístupových práv

Stanoviť nasledujúce pravidlá pri riadenie privilegovaných prístupových práv:

- Používať automatizované nástroje na inventarizáciu všetkých administratívnych účtov a preverovať, že každý takýto účet je schválený vedením.
- Pred nasadením akýchkoľvek nových zariadení v sieťovom prostredí je potrebné zmeniť všetky pôvodné heslá pre aplikácie, operačné systémy, routery, firewally, bezdrôtové prístupové body a iné systémy na heslá, ktoré sú ťažko uhádnuteľné.
- Používať automatizované skripty na uistenie sa, že sa administratívne účty využívajú len k administratívnym úkonom a nie na čítanie e-mailov, vytváranie dokumentov alebo surfovanie po internete. Internetové prehliadače a e-mailoví klienti musia byť nakonfigurované tak, aby ich nebolo možné spustiť pod administratívnym účtom. Tiež je možné nakonfigurovať administrátorské účty tak, aby na prístup do internetu používali webové proxy 127.0.0.1 a neobsahovali e-mailového klienta.
- Každá osoba, ktorá potrebuje administratívny prístup, musí mať samostatný účet. Administratívne účty sa nesmú nikdy zdieľať medzi používateľmi. Účty ako „administrator“ vo Windows sa môžu použiť len v krajných prípadoch.
- Implementovať dôsledné auditovanie používania administratívnych účtov a funkcií a monitorovať podozrivé správanie (napr. rekonfigurácie počas noci).
- Nakonfigurovať systémy tak, aby vytvorili log záznam a upozornenie, keď je pridaný alebo odobraný účet zo skupiny doménových administrátorov.
- Používať dvojstupňovú autentifikáciu pri všetkých administratívnych prístupoch, vrátane administratívneho prístupu do domény.
- Blokovať prístup do strojov pre účty s administratívnymi oprávneniami. Namiesto toho by sa administrátori mali prihlasovať pomocou neadministratívnych účtov a po prihlásení (bez administrátorských práv) získať administratívne privilégia pomocou nástrojov ako „runas“ vo Windows.
- Diferencovať administrátorské účty na základe definovaných rol v rámci organizácie. Napr. administrátor pracovnej stanice môže mať prístup len do pracovných staníc, notebookov atď.

- Pomocou politík a zvyšovaním povedomia používateľov vyžadovať, aby administrátori zaviedli jedinečné a rôzne heslá do ich administratívnych a neadministratívnych účtov.

A.9.2.5 Preskúmavanie prístupových práv

Preveriť všetky používateľské kontá a vymazať/vypnúť tie, ktoré nie sú spojené s procesom alebo vlastníkom. Pravidelne (štvrťročne alebo aspoň ročne) vyžadovať, aby manažéri porovnali aktívnych zamestnancov a dodávateľov s existujúcimi používateľskými účtami. Účty, ktoré nie sú k nim priradené, je potrebné vymazať. Takisto monitorovať používanie účtov na odhalenie „spiacich" účtov, ktoré neboli použité istú dobu (napr. 30 dní) a upozorniť na to používateľa a jeho nadriadeného. Po dlhšej dobe (napr. 60 dní) je potrebné účet zrušiť alebo vypnúť. Zaviesť systém, denne vytvárajúci správu, ktorá obsahuje zoznam zamknutých účtov, vypnutých účtov, účty so starými heslami a účty s heslami, ktorých platnosť nikdy nevyprší. Tento zoznam potom bezpečným spôsobom zasielať administrátorovi.

A.9.2.6 Odoberanie alebo úprava prístupových práv

Každý používateľ by mal mať len také prístupové práva, aké nevyhnutie potrebuje k výkonu svojej práce. V prípade zmeny pracovnej pozície, je nutné aby neodkladne došlo k úprave prístupových práv a to aj z hľadiska fyzického, teda odstránením, zrušením či výmenou kľúčov, identifikačných kariet, predplatného alebo vybavenia, ktoré slúži na spracovanie údajov.

A.9.3 Zodpovednosti užívateľov

Cieľ: *Urobiť používateľov zodpovedných za ochranu ich autentizačných informácií.*

A.9.3.1 Použitie tajných autentizačných informácií

Poučenie zamestnancov o ich zodpovednosti za ochranu svojich autentizačných informácií. Pri zaobchádzaní s týmito informáciami by mali dodržiavať nasledujúce pravidlá:

- nepoužívať heslá, spojiteľné s konkrétnou osobou (dátum narodenia, rodné priezvisko, atď.),
- neuchovávať zapísané autentizačné údaje v blízkosti pracovnej stanice, napr. pod klávesnicou,

- neukladať heslá v automatizovaných prístupoch,
- okamžitá zmena údajov v prípade podozrenia či náznaku ich možného zneužitia,
- nezdieľať vzájomne autentizačné údaje užívateľov,
- nepoužívať rovnaké heslo pre rôzne prístupy,
- nepoužívať rovnaké autentizačné údaje v osobnom a firemnom prostredí.

Pravidlá pre vytvorenie dostatočne bezpečného hesla:

- dĺžka 12-16 znakov,
- kombinácia malých a veľkých písmen spolu so špeciálnymi znakmi,
- absencia diakritiky,
- nepoužívať reálne slová.

A.9.4 Riadenie prístupu k systémom a informáciám

Cieľ: *Zabrániť neautorizovaným prístupom do systémov a aplikácií.*

A.9.4.1 Obmedzenie prístupu k informáciám

Politika riadenia prístupu by mala zahŕňať tiež obmedzenie prístupu k informáciám, založené na individuálnych požiadavkách aplikácií. Vykonávanie pravidelnej kontroly prístupov užívateľov a tiež ich prístupových práv v podobe práv na čítanie, zápis a mazanie.

A.9.4.2 Bezpečné postupy prihlásenia

Definovanie bezpečného postupu prihlásenia, v súlade s politikou prístupu, ktorý zahŕňa nasledujúce pravidlá:

- Zobrazovať varovanie, že systém či aplikácie môžu využívať len oprávnení užívatelia.
- Zadávané heslo je skryté a v priebehu jeho zadávania sa nezobrazujú žiadne pomocné hlásenia, ktoré by mohli neoprávnenému užívateľovi pomôcť.
- Po ôsmich neúspešných pokusoch o prihlásenia v rozmedzí 45 minút je potrebné účet zamknúť na 120 minút.
- Pravidelne monitorovať používanie účtov a automaticky odhlasovať používateľov po štandardnej dobe nečinnosti.
- Použitie viacfaktorovej autentizačnej metódy. Spoločnosť využíva na autentizáciu prístupu do časti informačného systému (eZdravie), ktorá je súčasťou verejného

informačného systému, dvojfaktorovú autentizáciu pomocou hesla a čipovej karty. Použitie dvojfaktorovej autentizácie navrhujem aj v prípade prístupu do siete a informačného systému ako celku.

- Pre každého používateľa vytvoriť profil typického používania účtu na základe bežného času a dĺžky prístupu. Generovať denné správy, ktoré poukazujú na používateľov prihlásených počas nezvyčajného času alebo s nezvyčajne dlhou dobou prihlásenia (o 150 percent).
- Používať vhodné a dostatočne bezpečné šifrovanie.

A.9.4.3 Systém správy hesiel

Zavedenie systému správy hesiel, ktorý bude spĺňať nasledujúce odporúčania:

- Pri všetkých neadministrátorských účtoch vyžadovať minimálne 12-znakové heslá obsahujúce písmená, čísla a špeciálne znaky. Heslá sa musia meniť aspoň každých 90 dní a nesmie byť povolené použitie heslá z posledných 15 použitých hesiel.
- Každé administratívne heslo má minimálne 16 pseudonáhodných znakov. Nakonfigurovať všetky účty na administratívnej úrovni tak, aby vyžadovali pravidelné zmeny hesiel v intervaloch nie dlhších ako 60-90 dní a opäť nesmie byť povolené použitie heslá z posledných 15 použitých hesiel.
- Všetky servisné účty majú dlhé a ťažko uhádnuteľné heslá, ktoré sú pravidelne menené (tak ako aj pri administratívnych a používateľských účtoch) v intervaloch nie dlhších ako 90 dní.
- Heslá do všetkých systémov musia byť uložené oddelene od dát aplikácie, v dobre hašovanom alebo šifrovanom formáte, slabšie formáty ako napr. Windows LANMAN haš treba odstrániť z prostredia.

Odporúčam použiť napríklad nástroj KeePass, ktorý je bezplatný a umožňuje generovanie a zapamätanie silných hesiel.

A.9.4.4 Použitie privilegovaných programových nástrojov

Použitie systémových programov a utilít umožňujúcich obídenie bezpečnostných mechanizmov musí byť riadené.

A.10 Kryptografia

A.10.1 Kryptografické opatrenia

Cieľ: *Zabezpečiť správne a efektívne používanie šifrovania na zabezpečenie dôvernosti, preukázania pôvodu alebo neporušenosti informácií.*

A.10.1.1 Politika použitia kryptografických opatrení

Zavedenie politiky používania kryptografických opatrení

Nemocnica v súčasnosti nepoužíva digitálny podpis ale v záujme uľahčenia administrácie navrhujem zavedenie jeho používania, konkrétne aplikáciu QES vyvinutú príslušníkom úradu pre orgán dohľadu. Je poskytovaná bezplatne a spĺňa požiadavky Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

Aplikáciu QES možno použiť pre časové pečiatkovanie a pre tvorbu podpisov a pečatí v súlade s vykonávacím rozhodnutím komisie (EÚ) 2015/1505 a vykonávacím rozhodnutím komisie (EÚ) 2016/1506 (dokumenty PDF, aplikácie EXE alebo akýkoľvek iný druh dokumentov, najmä v ZIP kontajneri, ktorý môže byť aj vnorený):

- kvalifikovaným elektronickým podpisom,
- kvalifikovanou elektronickou pečaťou,
- kvalifikovanou elektronickou časovou pečiatkou,

ako aj na prezeranie s možnosťou exportu a náhľadu do autorizovaných dokumentov z kontajnerov ASiC a PDF.

A.10.1.2 Správa kľúčov

Odporúčaná minimálna veľkosť RSA kľúča je 2048 bitov a maximálna veľkosť pre zachovanie rozumnej použiteľnosti je 4096 bitov. Odporúčaná doba platnosti kľúča je maximálne 2 roky. Pre zdieľanie kľúčov odporúčam použitie komunikačných aplikácii, ktoré využívajú end-to-end šifrovanie. Je potrebné používať silné heslo, ktoré nebude ukladané do mailových klientov a podobne.

A.11 Fyzická bezpečnosť a bezpečnosť prostredia

A.11.1 Zabezpečené oblasti

Cieľ: *Zabránenie neautorizovanému fyzickému prístupu, zničeniu alebo zasahovaniu do informácií organizácie alebo zariadení spracúvajúcich informácie.*

A.11.1.1 Fyzický bezpečnostný perimeter

Definovanie bezpečnostného perimetra a jeho úrovní. Navrhujem rozdeliť bezpečnostný perimeter do 4 úrovní:

1. úroveň – areál nemocnice, priestory prístupné verejnosti,
2. úroveň – priestory, kde smú vstupovať pacienti pod dozorom personálu,
3. úroveň – priestory určené len pre zamestnancov,
4. úroveň – serverovňa, archív, rozvodné miestnosti.

1. úroveň

Nemocnica má 5 vstupných vchodov prístupných verejnosti zabezpečených automatickými dverami s bezpečnostným sklom. Vchod pre urgentný príjem je otvorený nonstop, zvyšné vchody sú mimo prevádzkových hodín uzamknuté. Ich zabezpečenie je zodpovednosťou vrátnika. Zvyšné vstupy do budovy určené výlučne pre určitý personál nemocnice sú obyčajné exteriérové dvere, ktoré sú po celý čas zamknuté.

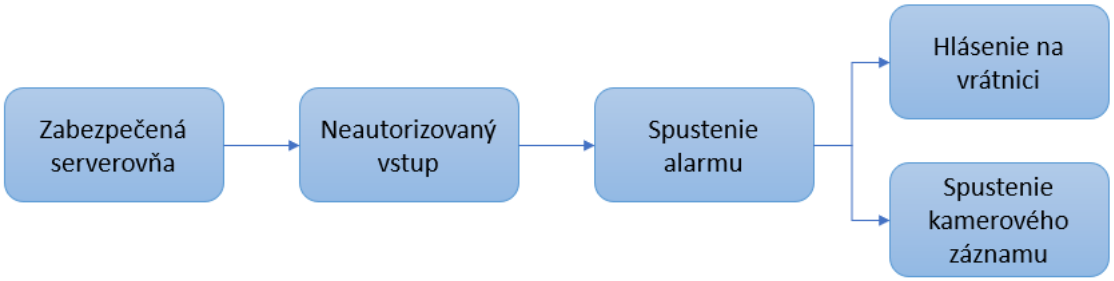
V súčasnosti je kamerovým systémom monitorovaný vchod urgentného príjmu, čakáreň traumatologickej a internej príjmovej ambulancie a vstup a východ plateného parkoviska nemocnice. Navrhujem kamerovým systémom zabezpečiť všetky vstupy do budovy nemocnice a tiež ďalší vstup do areálu a teda vrátnicu. Z hľadiska zabezpečenia pasívnych prvkov siete v priestoroch prvej úrovne perimetra, musí byť kabeláž vedená v podhľade alebo káblovom žľabe a dátové zásuvky umiestnené v podhľade.

2. a 3. úroveň

Priestory perimetra druhej a tretej úrovne sú zabezpečené vstupnými dverami s bezpečnostným zámkom. Kľúče od týchto dverí, majú len zamestnanci, ktorých náplň práce to vyžaduje. Pre tieto úrovne perimetra navrhujem zavedenie elektronického zabezpečovacieho systému, ktorý by permanentne detegoval neoprávnený vstup v čase, kedy nie sú priestory využívané. Prípadné narušenie bude hlásené na vrátnici. Cenová kalkulácia navrhovaného riešenia je uvedená v kapitole Ekonomické zhodnotenie.

4. úroveň

Okrem bezpečnostných protipožiarnych dverí s päťbodovým zamykaním navrhujem obe serverovne vybaviť kamerovým systémom a tiež elektronickým zabezpečovacím systémom s pohybovým snímačom a snímačom otvorenia dverí. V prípade neautorizovaného vstupu do zabezpečenej serverovne by sa spustil alarm, ktorý by vyvolal hlásenie na vrátnici a zároveň spustenie kamerového záznamu.



Obrázok č. 13: Schéma fungovania zabezpečenia serverovne
(Zdroj: Vlastné spracovanie)

A.11.1.2 Riadenie fyzických prístupov

Momentálne je kontrola fyzického vstupu realizovaná knihou príchodov a odchodov zamestnancov jednotlivých oddelení. Navrhujem zavedenie elektronického dochádzkového systému, ktorý by bol centralizovaný pre celú nemocnicu. Súčasťou tohto systému by boli elektrické zámky na dverách jednotlivých oddelení s RFID čítačkou. Zamestnanci by na prístup využívali kartu stravovacieho systému, ktorú má pridelenú každý zamestnanec.

A.11.1.3 Zabezpečenie kancelárií, miestností a vybavenia

Zabezpečenie kancelárií, ambulancií a serverovní v čase ich nevyužívania elektrickým zabezpečovacím systémom s duálnym pohybovým snímačom. Zamestnanec nesmie v spomínaných priestoroch umožniť prítomnosť cudzích osôb bez dozoru. Umožniť vstup do miestnosti neoprávneným osobám (upratujúci personál, servisní zamestnanci, návštevy a pod.) až po zabezpečení ochrany údajov uzatvorením dokumentov v elektronickej podobe alebo zatvorením spisového materiálu v listinnej podobe. Využiť všetky dostupné prostriedky na zabezpečenie údajov pred prístupom neoprávnenej osoby (napríklad uchovávanie dokumentov v uzamknutých častiach nábytku). Ten, kto

posledný opúšťa miestnosť je povinný ju zamknúť a po skončení pracovnej doby musí zatvoriť všetky okná a zapnúť alarm. Je nutné pridelenie zodpovednosti za pravidelnú kontrolu správnej funkčnosti zabezpečovacieho systému.

A.11.1.4 Ochrana pred vonkajšími a prírodnými hrozbami

Nemocnica má vzhľadom na povodňové ohrozenie dobrú polohu, nachádza sa na území, v ktorom je pravdepodobnosť opakovania povodne raz za sto rokov. Aktuálne umiestnenie hlavnej serverovne je z hľadiska povodňového rizika vyhovujúce, nachádza sa na treťom, najvyššom poschodí. Avšak súčasný stav strechy predstavuje pre zariadenia umiestnené v serverovni riziko poškodenia vodou. Navrhujem preto využiť serverovňu na druhom poschodí ako primárnu. V organizácii tiež existuje vyššia miera rizika vzniku požiaru v dôsledku množstva elektrických zariadení a horľavých látok. Navrhujem preto použitie detektorov dymu do priestorov, v ktorých sa nachádza väčšie množstvo horľavých látok a elektrických zariadení. Je nutné tieto zariadenia zahrnúť do pravidelnej revízie zariadení.

A.11.1.5 Práce v zabezpečených oblastiach

Vytvorenie, zavedenie a kontrola dodržiavania postupov pre prácu v zabezpečenej oblasti, týkajúcich sa zamestnancov organizácie ale aj externých strán pracujúcich v danej oblasti. V postupoch by malo byť zavedené pravidlo vyvarovania sa práce bez dohľadu.

A.11.2 Bezpečnosť zariadení

Cieľ: *Zabrániť stratám, zničeniu, krádeži alebo vyzradeniu aktív alebo prerušeniu činností organizácie.*

A.11.2.1 Umiestnenie zariadenia a jeho ochrana

Umiestnenie zariadení vyžadujúcich zvýšenú ochranu v zabezpečenej serverovni. Serverovňa je zabezpečená proti neoprávnenému vniknutiu a krádeži, proti poškodeniu vodou či vzniku požiaru. Požadované teplotné podmienky zaisťujú dve klimatizácie, z ktorých je jedna záložná. Zabezpečiť, že v blízkom okolí serverovne sa nevyskytujú zariadenia, ohrozujúce prvky v nej umiestnené, akými sú napríklad kanalizácia, vodovod, horľavé alebo iné materiály.

Umiestnenie pracovných staníc a iných zariadení do priestorov bez prístupnosti verejnosti, pokiaľ to nie je možné zabezpečiť ich pomocou lankového bezpečnostného zámku.

A.11.2.2 Podporné služby

Zabezpečenie serverovne v prípade výpadku elektrickej energie je momentálne riešené vhodne a dostačujúco. Chýbajúce postupy pravidelnej kontroly záložných zdrojov je však nutné stanoviť a dodržiavať. Odporúčam tieto zariadenia kontrolovať osobne IT technikmi v pravidelnom intervale dvoch týždňov a o výsledku kontroly viesť patričnú dokumentáciu.

Navrhujem tiež zriadenie redundantného internetového pripojenia. Súčasné riešenie pomocou VDSL technológie použiť ako záložné pripojenie a ako primárnu technológiu použiť licencovaný rádiový spoj peer-to-peer. Vzhľadom na aktuálnu ponuku poskytovateľov internetových služieb odporúčam spoločnosť SWAN, a. s., ktorý ponúka zároveň možnosť prenájmu firewall zariadenia umožňujúceho automatické prepnutie na redundantné internetové pripojenie v prípade výpadku primárneho pripojenia. Náklady na toto riešenie sú zahrnuté v kapitole Ekonomické zhodnotenie.

A.11.2.3 Bezpečnosť káblových rozvodov

Zavedenie dostatočnej ochrany káblových rozvodov pred odpočúvaním, rušením a ich poškodením. Vzhľadom k tomuto opatreniu je v organizácií použitá tienená kabeláž a v priestoroch prístupných verejnosti je vždy vedená podhľadom prípadne v lište vo výške 2,2 metra. Je nutné oddelenie komunikačných káblov od napájacích za účelom eliminácie rušenia. Zodpovednosťou IT technikov je vedenie aktuálnej schémy vedenia káblových rozvodov a pravidelná kontrola stavu kabeláže. Taktiež navrhujem použitie bezpečnostných prvkov systému NISS (Network Infrastructure Security Solution) 0. a 1. stupňa a to konkrétne:

- popisné štítky na zásuvky, panely a PatchCordy,
- prvky na blokovanie metalických portov RJ45 a USB,
- prvky na ochranu proti vytiahnutiu (uzamknutie) PatchCordov.

A.11.2.4 Údržba zariadení

V záujme predchádzania zlyhania zariadení je potrebné stanoviť, zaviesť a kontrolovať postupy pravidelnej revízie zariadení založenej na hodnotení aktív, so stanovenými frekvenciami servisu na základe špecifikácie dodávateľa. Opravu zariadení môže vykonávať len autorizovaný servis alebo autorizovaný pracovník údržby. V prípade servisu zariadení obsahujúcich citlivé dáta, je zariadenie zasielané na servis po spoľahlivom zabezpečení dát prípadne ich odstránení zo zariadenia. O vykonanej údržbe, oprave či kontrole je nutné viesť dokumentáciu.

A.11.2.5 Odstránenie aktív

Ustanoviť odnášanie majetku z priestorov organizácie alebo jeho svojvoľné premiestňovanie za porušenie pracovnej disciplíny. Vynášanie alebo prenášanie aktív z priestorov organizácie umožniť len osobám, ktorým táto činnosť vyplýva z pracovnej funkcie alebo z predpisov organizácie.

A.11.2.6 Bezpečnosť zariadení a aktív mimo priestorov organizácie

Stanovenie a implementácia bezpečnostných pravidiel, upravujúcich prenos informačných aktív mimo priestory organizácie. V prípade poruchy zariadenia, ktoré by mohlo obsahovať dáta, musí IT technik pred odovzdaním tohto zariadenia do opravy odstrániť všetky možné médiá, na ktorých by sa dáta mohli nachádzať (pevné disky, CD, DVD médiá a podobne). Ak je poškodený pevný disk, IT technik je povinný dať zástupcovi servisnej firmy podpísať čestné prehlásenie o mlčanlivosti, ktoré bude súčasťou zmluvy, prípadne objednávky.

A.11.2.7 Bezpečná likvidácia alebo opakované použitie zariadenia

Vypracovanie, zavedenie a kontrola dodržiavania pravidiel pre bezpečnú likvidáciu alebo opakované použitie zariadení, určených na spracovanie informácií. Likvidáciu dát v prípade opakovaného použitia realizovať metódou spoľahlivého zmazania dát, napríklad použitím softwarového nástroja vykonávajúceho viacnásobný prepis pamäťových médií. V prípade likvidácie zariadenia je možné napríklad mechanické znehodnotenie. Zodpovednosť za ich správne dodržanie prideliť pracovníkom IT oddelenia.

A.11.2.8 Neobsluhované užívateľské zariadenia

Užívateľovi určiť povinnosť použiť šetrič obrazovky chránený prístupovým heslom alebo odhlásiť sa z operačného systému pri odchode od svojej pracovnej stanice. Jednotlivé prostriedky chrániť tiež fyzickými opatreniami (napr. zámkom).

A.11.2.9 Zásada prázdneho stolu a prázdnej obrazovky monitora

Zavedenie zásady prázdneho stolu a prázdnej obrazovky do *Bezpečnostnej politiky NsP PB*, ktorých účelom je zníženie rizika straty alebo vyzradenia informácie a rizika neoprávneného prístupu. Podstatou zásady prázdneho stolu je nenechávať dôverné, súkromné alebo interné informácie bez dozoru v opustenej kancelárii. Vhodné je odstránenie blokov a papierikov s informáciami, ktoré by bolo možné zneužiť. Zásada prázdnej obrazovky spočíva v pravidle odhlásenia sa v prípade zanechania pracovnej stanice alebo mobilného zariadenia bez obsluhy a zabezpečenia zariadenia proti prihláseniu bez autentizácie užívateľa. Doporučené je nastavenie automatického zamykania obrazovky pri nečinnosti.

A.12 Bezpečnosť prevádzky

A.12.1 Prevádzkové postupy a zodpovednosti

Cieľ: *Zabezpečiť správnu a bezpečnú prevádzku zariadení spracúvajúcich informácie.*

A.12.1.1 Dokumentácia prevádzkových postupov

Vypracovanie dokumentov upravujúcich pravidlá pri práci na pracovnej stanici, používanie informačného systému, služieb internetu a elektronickej pošty. Prevádzkové postupy je nutné schváliť vedením a oboznámiť s nimi všetkých zamestnancov, ktorých sa dokumenty dotýkajú. Zverejniť dokumenty v intranete, aby boli v prípade potreby prístupné zamestnancom.

A.12.1.2 Riadenie zmien

Všetky zmeny v organizácií, podnikových procesoch, technickom vybavení na spracovanie informácií a tiež systémoch, ktoré ovplyvňujú informačnú bezpečnosť musia byť riadené a dokumentované. Vždy je nutné posúdiť dopad plánovaných zmien na bezpečnosť informácií v rámci stanoveného formálneho postupu na schvaľovanie zmien.

Po vykonaní zmien je nutné overiť, či sú aj naďalej splnené všetky požiadavky na bezpečnosť informácií.

A.12.2 Ochrana proti malwaru

Cieľ: *Zabezpečiť, aby informácie a zariadenia spracúvajúce informácie boli chránené pred škodlivých softwarom.*

A.12.2.1 Opatrenia proti malwaru

V záujme ochrany proti škodlivému softwaru zaviesť nasledujúce opatrenia:

- Nasadiť automatizované nástroje na neustále monitorovanie pracovných staníc, serverov, mobilných zariadení na aktívnu ochranu pred škodlivým softvérom pomocou antivírusu, antispywaru, osobného firewallu a IPS (host based).
- Všetky udalosti detekcie škodlivého softvéru majú byť logované a odosielané do systému na administráciu škodlivého softvéru.
- Nasadiť automatické aktualizácie softvéru na ochranu pred škodlivým softvérom a vírusovej databázy, prípadne ich nechať denne manuálne aktualizovať IT technikmi.
- Nakonfigurovať notebooky, pracovné stanice a servery tak, aby neumožňovali automatické spúšťanie obsahu z USB kľúčov, tokenov, CD/DVD, zariadení s Firewire alebo iných médií.
- Nakonfigurovať systémy tak, aby umožnili automatickú kontrolu škodlivého softvéru na vymeniteľných médiách okamžite po ich vložení.
- Všetky prílohy e-mailov by mali byť skenované a v prípade, že obsahujú škodlivý kód, alebo typy súborov, ktoré sú pre organizáciu nepotrebné, by mali byť blokované ešte pred príchodom do e-mailovej schránky používateľa.
- Automatizované nástroje na monitorovanie by mali využívať detekciu anomálií správania na doplnenie a zlepšenie tradičnej detekcie na základe znakov (signature based detection).
- Nástroje proti škodlivému kódu by mali obsahovať centrálnu konzolu, prostredníctvom ktorej administrátori dokážu identifikovať infikované zariadenia a zariadenia, na ktorých neprebehol sken alebo neprebehla aktualizácia signatúr.
- Organizácie by mali nasadiť nástroje na kontrolu prístupu do siete na overenie bezpečnej konfigurácie pred povolením prístupu do siete.

- Malo by byť nasadené nepretržité monitorovanie odchádzajúcej prevádzky. Akékoľvek väčšie toky dát, alebo neautorizovaná šifrovaná prevádzka by mala byť označená. Pokiaľ bude vyhodnotená ako škodlivá, je potrebné daný počítač presunúť do izolovanej VLAN.
- Implementovať procesy na riešenie incidentov, ktoré umožnia organizácii získať vzorky škodlivého softvéru zo systémov organizácie a v prípade potreby ich poskytnúť výrobcovi antivírusového produktu nasadeného v organizácií.

A.12.3 Zálohovanie

Cieľ: *Ochrániť pred stratou údajov.*

A.12.3.1 Zálohovanie informácií

Vytvorenie, zavedenie a kontrola dodržiavania postupov zálohovania informácií, ktoré sú v súlade s nasledujúcimi odporúčaniami:

- Zálohovanie sa vykonáva v čase mimo pracovnej doby, prípadne v čase najnižšieho používania a to dvojúrovňovo. Prvá záloha sa ukladá na vnútorný disk servera, ale nie na disk, kde je umiestnená databáza IS. Druhá záloha sa vytvorí po ukončení zálohovania, kopírovaním zálohy na archívny server. Tým sa zároveň kontroluje aj jej použiteľnosť.
- Zálohy sa archivujú na samostatných serveroch s vysokou kapacitou diskového priestoru, obsahujúcich RAID5. Umiestnené sú v zabezpečenej serverovni s riadeným prístupom, klimatizáciou a v inej miestnosti ako primárny server.
- Zabezpečiť, aby boli všetky systémy zálohované aspoň raz týždenne a systémy s citlivými dátami častejšie. Aby bolo možné rýchlo zo zálohy obnoviť operačný systém, aplikačný softvér a dáta, je potrebné, aby ich obnova bola zahrnutá a popísaná v celkovom postupe zálohovania.
- Kľúčoví zamestnanci musia byť vyškolení na proces zálohovania a aj proces obnovy. Vyškolení musia byť aj zastupujúci zamestnanci pre prípad nedostupnosti kľúčových zamestnancov.
- Zabezpečiť, že zálohy sú dostatočne chránené fyzickou bezpečnosťou, resp. sú šifrované na ich lokálnom umiestnení ako aj pri presune po sieti.
- Prideliť zodpovednosť za zálohovanie konkrétnej osobe/oddeleniu.

- Ďalej navrhujem každé dva mesiace realizovať pravidelnú zálohu databázových údajov, ktorá bude uložené v zabezpečenom súbore na pamäťové médium, ktoré bude uložené v uzavretom a uzamknutom protipožiarnom priestore (napr. trezor).

A.12.4 Zaznamenávanie formou logov a monitorovania

Cieľ: *Zaznamenávať udalosti a vytvárať dôkazy.*

A.12.4.1 Zaznamenávanie udalostí formou logov

Zaviesť zaznamenávanie udalostí formou logov a aplikovať nasledovné bezpečnostné opatrenia:

- Overiť nastavenia auditných log záznamov pre každé zariadenie a softvér na ňom nainštalovaný. Uistiť sa, že logy obsahujú dátum, čas (timestamp), zdrojovú a cieľovú adresu a ostatné užitočné časti paketu. Systémy majú uchovávať logy v štandardizovanom formáte (ak nie, je potrebné ich normalizovať).
- Uistiť sa, že všetky systémy, ktoré ukladajú logy majú dostatočný úložný priestor pre pravidelne generované logy. Logy musia byť pravidelne archivované a digitálne podpísané.
- Nakonfigurovať operačné systémy tak, aby logovali udalosti spojené s prístupom (používateľa k súborom a zložkám) bez oprávnenia. Neúspešné pokusy o prihlásenie musia byť tiež logované.
- Raz za dva týždne vykonať kontrolu a urobiť zápisy anomálií logov, preveriť ich a zdokumentovať pracovníkmi IT oddelenia.
- Hraničné sieťové zariadenia ako firewally a proxy musia byť nastavené tak, aby logovali celú prichádzajúcu (povolenú aj blokovanú) prevádzku.
- Pre všetky servery je potrebné zabezpečiť, aby boli logy ukladané iba na write-only zariadenia alebo dedikované logovacie servery oddelené od zariadení generujúcich logy.

A.12.4.4 Synchronizácia času

Nastavenie synchronizácie systémových hodín voči jednotnému času na všetkých serveroch, v záujme zaistenia presnosti auditných záznamov a včasnej realizácie naplánovaných úloh.

A.12.5 Riadenie operačného softwaru

Cieľ: *Zabezpečiť integritu operačných systémov.*

A.12.5.1 Inštalácia softwaru na prevádzkové systémy

Stanovenie základných bezpečnostných pravidiel pre zavádzanie systémov do prevádzkového prostredia minimalizujúcich riziko zavedenia neautorizovaných zmien a ohrozenie požadovaných bezpečnostných parametrov.

A.12.6 Správa a riadenie technických zraniteľností

Cieľ: *Zabrániť zneužitiu technickej zraniteľnosti.*

A.12.6.1 Správa a riadenie technických zraniteľností

Organizácia by mala aspoň raz polročne spúšťať nástroje na skenovanie zraniteľností všetkých systémov v sieti. Tam, kde je to možné, je potrebné skenovať denne. Každá zistená zraniteľnosť by mala byť včas odstránená a kritické zraniteľnosti by mali byť odstránené do 72 hodín. Zaviesť porovnávanie minulých výsledkov skenov zraniteľností, v záujme overenia, že zraniteľnosti boli riešené buď prostredníctvom záplat, zavedením opatrenia alebo akceptáciou a zdokumentovaním rizika. Manažér informačnej bezpečnosti by mal zdieľať správy o zraniteľnostiach s vedením, aby malo prehľad o kritických problémoch a motiváciu na ich odstránenie. IT oddelenie by malo vytvárať rebríček neošetrených, kritických zraniteľností pre každé oddelenie. Logy z udalostí by mali byť korelované s informáciami zo skenov zraniteľností, aby bolo možné overiť, že sa loguje aktivita samotných skenovacích nástrojov a aby bolo možné overiť, či bola pri prípadnom útoku využitá známa zraniteľnosť.

Organizácia by mala zaviesť automatizované nástroje na plátanie zraniteľností. Kritické záplaty musia byť vyhodnotené v testovacom prostredí ešte pred tým, ako budú nasadené do produkčného systému. Ak tieto záplaty narušia kritické aplikácie na testovacích strojoch, je potrebné nájsť iné opatrenia na ošetrenie zraniteľností, ktoré znemožnia ich zneužitie a nenarušia funkcionalitu kritických procesov a aplikácií.

A.12.6.2 Obmedzenie inštalácie softwaru

V spoločnosti je zavedené obmedzenie inštalácie softwaru na základe prednastaveného obmedzenia inštalácie v nastaveniach operačného systému. Každú novú inštaláciu musia realizovať výlučne IT technici po prihlásení administrátorského konta.

A.12.7 Audit informačných systémov

Cieľ: *Minimalizovať vplyv aktivít auditu na operačné systémy.*

A.12.7.1 Opatrenia auditu informačných systémov

Pridelenie zodpovednosti za pravidelné vytváranie a sledovanie auditných záznamov (logov) jednotlivým správcom informačných a komunikačných technológií – IT oddeleniu a správcom NIS, resp. iným zamestnancom, ktorým to vyplýva z pracovnej náplne. Audit systémov musí byť plánovaný a odsúhlasený oprávnenými zamestnancami, aby sa minimalizovalo riziko prerušenia procesov organizácie. Stanovenie pravidiel pre plánovanie a vykonávanie interných auditov v podobe smernice.

A.13 Bezpečnosť komunikácií

A.13.1 Správa bezpečnosti siete

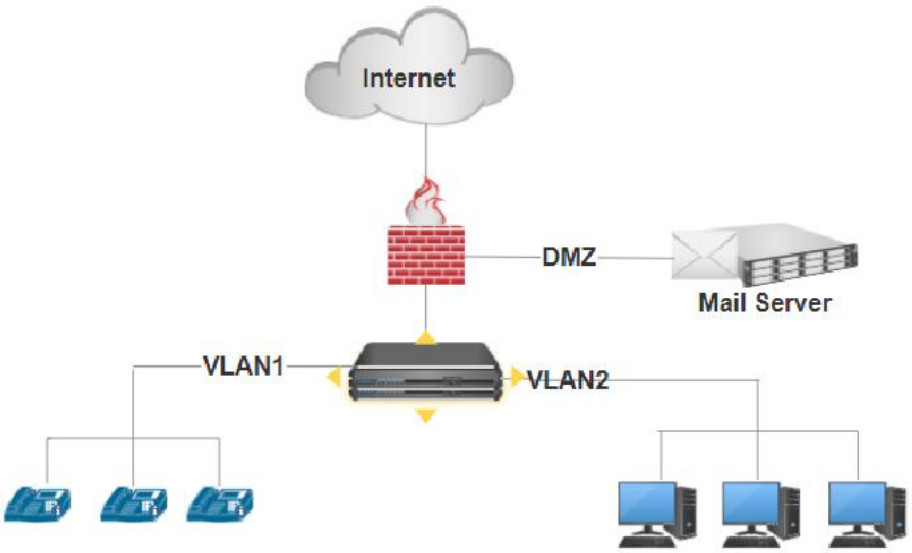
Cieľ: *Zabezpečiť ochranu informácií v sieti a v podporných zariadeniach, ktoré ich v sieti spracúvajú.*

A.13.1.1 Opatrenia v sieti

Zavedenie organizačných, technologických a kontrolných opatrení zabezpečujúcich ochranu a bezpečnú správu a prevádzku počítačovej siete. Identifikovanie a ohodnotenie rizík spojených so správou a prevádzkou počítačovej siete v analýze rizík. Zadefinovanie pravidiel filtrovania komunikácie medzi jednotlivými segmentami siete a medzi jednotlivými VLAN.

A.13.1.3 Oddeľovanie sietí

Odporúčam vytvorenie demilitarizovanej zóny, v ktorej bude pripojený MAIL Server. Ďalej odporúčam vytvorenie dvoch segmentov siete. Prvý segment je určený pre systém IP telefónie a v druhom segmente budú pripojené pracovné stanice. Medzi jednotlivými sieťovými segmentami je nutné zadefinovať pravidlá filtrovania komunikácie.



Obrázok č. 14: Schéma odporúčaného oddelenia sietí
(Zdroj: Vlastné spracovanie)

A.13.2 Prenos informácií

Cieľ: *Ošetriť bezpečnosť prenášaných informácií v rámci organizácie a s treťou stranou.*

A.13.2.1 Politiky a postupy pri prenose informácií

Stanoviť a zaviesť politiky a postupy pri prenose informácií. Užívatelia siete sú povinní riadiť sa pri používaní Internetu a elektronickej pošty všeobecne záväznými právnymi predpismi, autorským právom, či obchodnými značkami. Používanie elektronickej pošty na účely, ktoré nesúvisia s výkonom pracovnej činnosti je zakázané. Používateľ Internetu a elektronickej pošty musí byť oboznámený s tým, že prevádzkovateľ má právo v súlade s platnou legislatívou preverovať použitie týchto prístupov.

A.13.2.3 Elektronické predávanie správ

Šifrovanie elektronických súborov, ktoré sú prílohou elektronickej pošty (najmä formáty Pdf., Rtf.., Xcs.) prostredníctvom šifrovacích a hašovacích algoritmov integrovaných do voľne dostupných programových aplikácií (napr. PDFMate Free PDF Merger, Acrobat X Pro); pričom heslo je potrebné odoslať príjemcovi prostredníctvom SMS alebo ho oznámiť telefonicky, príp. osobne, ale vždy iným komunikačným kanálom, ako je elektronická pošta. Zabezpečiť MAIL Server platným SSL šifrovacím certifikátom.

A.13.2.4 Zmluvy o dôvernosti alebo utajení

Zamestnanec alebo tretia strana sú povinní pred udelením prístupu k citlivým informáciám podpísať zmluvu o mlčanlivosti a následne zachovávať mlčanlivosť o osobných a citlivých údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení pracovného alebo zmluvného vzťahu. Zachovanie mlčanlivosti neplatí, ak je to nevyhnutné, na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákonu.

A.14 Akvizícia, vývoj a údržba systému

A.14.1 Bezpečnostné požiadavky informačných systémov

Cieľ: *Zabezpečenie integrácie informačnej bezpečnosti do informačných systémov v celom ich životnom cykle*

A.14.1.1 Analýza a špecifikácia požiadaviek bezpečnosti informácií

Zaviesť do procesu zaobstarávania nových systémov aj analýzu bezpečnostných požiadaviek, ktoré definujú určení špecialisti pre danú oblasť. Toto opatrenie by malo predísť potrebe implementácie dodatočných opatrení do systémov a s ňou spojenými dodatočnými nákladmi.

A.14.2 Bezpečnosť pri vývoji a pri podporných procesoch

Cieľ: *Zabezpečiť implementáciu informačnej bezpečnosti do vývojového cyklu informačného systému.*

A.14.2.2 Postupy riadenia systémových zmien

Zavádzanie zmeny v informačnom systéme je v súčasnosti realizované prvotne výlučne na testovacej prevádzke programu. Odporúčam však aby testovacia verzia programu obsahovala len náhodne vygenerované dáta. Po dôkladnom otestovaní systémovej zmeny je možné ju následne implementovať do ostrej prevádzky informačného systému a to s čo najmenším zásahom do plynulej prevádzky organizácie.

A.14.2.3 Technické preskúmanie aplikácií po zmene operačného systému

IT technici sú povinný vykonávať testy kompatibility kritických aplikácií v prípade inštalácie novej verzie operačného systému za účelom zamedzenia nepriaznivého vplyvu

zmien operačných systémov na funkčnosť alebo bezpečnosť dôležitých informačných systémov.

A.14.2.4 Obmedzenie zmien v softwarových balíčkoch

V záujme minimalizovať riziko ohrozenia funkčnosti bezpečnostných opatrení vstavaných dodávateľom priamo do aplikačných systémov je modifikácia systému realizovaná len v prípade, ak špecifické požiadavky kladené na systém nie je možné realizovať využitím existujúceho prevádzkovaného softwaru, ani štandardného softwaru.

A.15 Vzťahy s dodávateľmi

A.15.1 Bezpečnosť informácií vo vzťahoch s dodávateľmi

Cieľ: *Zabezpečiť ochranu aktív organizácie, ku ktorých pristupujú dodávatelia.*

A.15.1.1 Politika bezpečnosti informácií pre oblasť vzťahov s dodávateľmi

Pri uzatváraní dodávateľských zmlúv je vedenie povinné zabezpečiť, aby každá takáto zmluva obsahovala článok ošetrujúci bezpečnosť informácií a uvádzajúci povinnosť dodávateľa zachovať mlčanlivosť pri styku s osobnými údajmi zamestnancov alebo pacientov NsP PB.

A.15.1.2 Ošetrenie bezpečnosti v zmluvách s dodávateľmi

Článok ošetrujúci bezpečnosť informácií v zmluve s treťou stranou obsahuje najmenej:

- ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi,
- ustanovenie o povinnosti chrániť všetky poskytnuté informácie,
- ustanovenie o povinnosti dodržiavať a prijímať bezpečnostné opatrenia treťou stranou,
- konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma tretia strana a vyjadrenie súhlasu s nimi,
- zoznam pracovných rolí tretej strany, ktoré majú mať prístup k informáciám a údajom, s povinnosťou oznámiť každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti,
- ustanovenie o rozsahu, spôsobu a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby v tretej strane,

- vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie namiesto dodávateľa,
- ustanovenia o povinnosti informovať o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti,
- ustanovenie o sankčných mechanizmoch pri porušení zmluvy,
- záväzok tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má tretia strana počas trvania zmluvného vzťahu prístup.

A.15.2 Riadenie dodávateľských služieb

Cieľ: *Udržiavať dohodnutú úroveň informačnej bezpečnosti a dodávaných služieb podľa zmlúv o dodávkach.*

A.15.2.1 Monitorovanie a preskúmavanie služieb dodávateľov

Vykonávanie kontroly dodržiavania zmlúv zo strany dodávateľov, ktorá je zodpovednosťou manažéra informačnej bezpečnosti. Manažér informačnej bezpečnosti musí mať prehľad o dodávateľoch a ich prístupoch k citlivým informáciám. V prípade porušenia zmluvných podmienok je treba postupovať podľa sankčných mechanizmov uvedených v zmluve.

A.15.2.2 Riadenie zmien služieb dodávateľov

Stanovenie spôsobu riadenia dodávateľských služieb. V prípade potreby vykonania zmeny dodávaných služieb je nutné jej schválenie vedením, zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii. Zmeny vykonané úpravou alebo aktualizáciou bezpečnostnej politiky či postupov a opatrení organizácie musia byť premietnuté aj do zmlúv s dodávateľmi. Takisto zmeny zo strany dodávateľa ako napríklad použitie nových technológií, nové produkty, verzie/vydania alebo zmena subdodávateľa musia byť monitorované a posudzované z hľadiska dopadu na bezpečnosť informácií.

A.16 Riadenie incidentov bezpečnosti informácií

A.16.1 Riadenie incidentov bezpečnosti informácií a zlepšovanie

Cieľ: *Zabezpečiť konzistentný a efektívny prístup na riadenie incidentov informačnej bezpečnosti vrátane komunikácie o bezpečnostných udalostiach.*

A.16.1.1 Zodpovednosti a postupy

Vytvoriť postupy na riešenie incidentov zahŕňajúce definíciu rol zamestnancov pri riešení incidentov. Je nutné priradiť pracovné zaradenie a povinnosti pre riešenie počítačových a sieťových incidentov. Určiť manažérskych zamestnancov, ktorí budú podporovať proces riešenia incidentov pri kľúčových rozhodnutiach.

A.16.1.2 Podávanie správ o udalostiach bezpečnosti informácií

Zaviesť časové rámce pre systémových administrátorov a ostatných zamestnancov na hlásenie nezvyčajných udalostí, formalizovať mechanizmus hlásenia a druh informácií, ktoré musia byť zahrnuté v notifikácií o incidente.

Zamestnanec, ktorý má podozrenie na výskyt bezpečnostného incidentu, neodkladne ohlási túto skutočnosť IT oddeleniu pomocou formulára. Incidentom sa v tomto prípade rozumie aj zlá funkcia softwaru, hardwaru, zlyhanie ľudského faktoru či prelomenie opatrení fyzickej bezpečnosti. Príklad formulára určeného na nahlásenie bezpečnostného incidentu administrátorom je uvedený v prílohe. Ohlasovaciu povinnosť vládnemu CSIRT/CERT tímu má manažér informačnej bezpečnosti. Ten je povinný neodkladne nahlásiť každý závažný kybernetický bezpečnostný incident prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, a tiež identifikovať ich kategóriu na základe presiahnutia kritérií podľa §24 zákona č. 69/2018 Z.z.. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

A.16.1.3 Podávanie správ o slabých miestach bezpečnosti informácií

Do pravidelných školení zahrnúť aj informácie ohľadom hlásenia počítačových anomálií a incidentov, zverejnených národným CERT/CSIRT tímom, v záujme zvýšenia bezpečnostného povedomia.

A.16.1.4 Posudzovanie a rozhodovanie o udalostiach bezpečnosti informácií

Zodpovednosť za prvotné posúdenie a riešenie nahlásenej udalosti na základe informácií poskytnutých vo formulári prideliť IT oddeleniu. IT oddelenie je následne povinné oznámiť udalosť manažérovi informačnej bezpečnosti, ktorý preberie zodpovednosť za rozhodnutia ohľadne nahlásenej udalosti a v spolupráci s IT oddelením a úradom ju ďalej rieši.

Priority pri riešení bezpečnostného incidentu:

- bezodkladné obnovenie bežnej prevádzky IS aspoň v núdzovom režime, zabezpečenie ochrany údajov, zachovanie dôkazového materiálu nevyhnutného na ďalšiu analýzu príčin vzniku bezpečnostného incidentu,
- zistenie príčin, ktoré viedli k vzniku bezpečnostného incidentu,
- určenie zodpovednosti za vznik bezpečnostného incidentu a vyvodenie dôsledkov,
- zovšeobecnenie zistených skutočností a návrh opatrení na zabránenie opakovaného výskytu bezpečnostného incidentu.

A.16.1.5 Odozva na incidenty bezpečnosti informácií

Definovanie procedúr upravujúcich spôsob reakcie na identifikované bezpečnostné udalosti a bezpečnostné incidenty v záujme minimalizovania dopadu bezpečnostných incidentov na procesy a aktíva organizácie. Reakcia by mala spočívať v zhromaždení dôkazov, vykonania analýzy a klasifikácie incidentu. nahlásení interným a externým stranám, ktoré majú byť informované a po úspešnom vysporiadaní sa s incidentom jeho zdokumentovanie pre budúcu analýzu. Dokumentuje sa predovšetkým príčina vzniku incidentu (pokiaľ je známa), dôsledky, všetky opatrenia prijaté pri riešení incidentu a ich účinnosť a tiež zistené nedostatky v existujúcom pláne pre prípad výskytu bezpečnostného incidentu.

A.16.1.6 Ponaučenie z incidentov bezpečnosti informácií

Evidovať formuláre nahlásenia podozrenia na výskyt bezpečnostného incidentu v elektronickej forme, na základe ktorých je následne vykonávaná analýza výskytu incidentov podľa typu či klasifikácie. Výsledky analýzy zdieľať v rámci pravidelného sedenia pre zamestnancov poverených riešením incidentov ohľadom možných scenárov

priebehu incidentov a zaistenia pochopenia súčasných hrozieb a rizík, ako aj ich zodpovednostiam pri riešení incidentov. V prípade, že analýza poukáže na nedostatky bezpečnostnej politiky, je nutné jej preskúmanie a návrh ďalších bezpečnostných opatrení, aby sa incident neopakoval.

A.16.1.7 Zber dôkazov

Stanovenie a zavedenie funkčného procesu vyšetrovania bezpečnostných incidentov s dôrazom na prevenciu výskytu opakujúcich sa bezpečnostných incidentov.

A.17 Aspekty informačnej bezpečnosti v riadení kontinuity

A.17.1 Kontinuita bezpečnosti informácií

Cieľ: *Zabudovanie kontinuity informačnej bezpečnosti do systému riadenia obchodnej kontinuity v organizácii.*

A.17.1.1 Plánovanie kontinuity bezpečnosti informácií

Vypracovanie stratégie a krízových plánov na udržanie kontinuity činností organizácie zahŕňajúcich bezpečnosť informácií s nemennými bezpečnostnými požiadavkami za každej situácie. Plán kontinuity činnosti by mal byť navrhnutý tak, aby bol zrozumiteľný aj človeku, ktorý na ňom nespolupracoval. Definuje komunikačný plán spolu s kontaktnými údajmi, určuje roly a zodpovednosti na plnení havarijných plánov a plánov obnovy, cieľovú dobu obnovy jednotlivých procesov, siete a informačných systémov a aplikácií. Mal by tiež zahŕňať popis procesu zabezpečenia dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu a určenie doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb. Na základe BSI Standardu 100-4 odporúčam obsah plánu, uvedený v kapitole Prílohy.

Súčasťou plánovania kontinuity je tiež vyčlenenie adekvátnych finančných, materiálno-technických a personálnych zdrojov na zabezpečenie riadenia kontinuity činností.

A.17.1.2 Implementácia kontinuity bezpečnosti informácií

Implementáciu kontinuity bezpečnosti informácií pozostáva z oboznámenia zamestnancov so stanoveným plánom kontinuity a ich rolou a zodpovednosťou spojenou

s plnením havarijných plánov a plánov obnovy a vystavením stanoveného plánu takým spôsobom, aby bol v prípade potreby dostupný všetkým zamestnancom. Navrhujem tiež zavedenie pohotovostnej služby IT oddelenia a to nasledujúcim spôsobom:

- stála služba: nepretržitý pobyt na pracovisku počas pracovnej doby 7:00 – 15:00 hod.,
- pohotovostná služba počas pracovných dní v čase 15:00 – 20:00 hod.: zabezpečenie kontroly prevádzky informačných systémov, bezpečnosť uložených dát, riešenie akútnej poruchy, vykonávanie stanovených testov, záloh, antivírových kontrol, profylaktiky siete a serverov,
- pohotovostná služba na telefóne v dňoch pracovného voľna a pokoja v čase 7:00 – 20:00 hod.: riešenie akútnych problémov užívateľov telefonickou konzultáciou alebo osobným príchodom na miesto poruchy s následnými opatreniami na odstránenie chýb, zabránenie poškodeniu alebo úniku osobných údajov.

A.17.1.3 Verifikácia, preskúmavanie a vyhodnotenie kontinuity bezpečnosti informácií

Zavedenie pravidelného preskúmavania a vyhodnocovania jednotlivých procesov riadenia kontinuity činností a ich testovanie prostredníctvom cvičení na zaistenie ich vhodnosti, efektívnosti a aktuálnosti. Výsledky z preskúmavania a testovania je potrebné vyhodnocovať a aplikovať opatrenia na zvýšenie odolnosti sietí a informačných systémov.

A.17.2 Redundancia

Cieľ: *Zabezpečiť dostupnosť zariadení na spracovanie informácií.*

A.17.2.1 Dostupnosť vybavenia na spracovanie informácií

Dostupnosť vybavenia na spracovanie informácií je momentálne zabezpečená dostatočne. Avšak fyzické oddelenie umiestnenia redundantných zariadení od primárnych zariadení, ktoré zálohujú, realizované nie je. Preto odporúčam umiestnenie redundantných serverov do sekundárnej serverovne, ktorá bude mať funkciu záložnej serverovne.

A.18 Súlad s požiadavkami

A.18.1 Súlad so zákonnými a zmluvnými požiadavkami

Cieľ: *Zabrániť vzniku právnych, štatutárnych, regulačných a zmluvných porušení povinností vo vzťahu k informačnej bezpečnosti.*

A.18.1.1 Identifikácia príslušnej legislatívy a zmluvných požiadaviek

Prideliť zodpovednosť za identifikáciu platnej legislatívy a zabezpečenie súladu s ňou. V prípade nemocnice je táto zodpovednosť pridelená právnemu oddeleniu.

A.18.1.2 Práva k duševnému vlastníctvu

Informovať zamestnancov o povinnosti používať len schválený a licencovaný software a zavedenie tohto pravidla do bezpečnostnej politiky organizácie. Zodpovednosť za dodržiavanie licenčných podmienok v rámci organizácie nesie konkrétna osoba, a to prevádzkový námestník. Jeho úlohou je uchovávanie dokladov vlastníctva licencií a nákup softwaru len u overených zdrojov.

A.18.1.3 Ochrana záznamov

Zabezpečenie súladu s pravidlami smerníc organizácie, upravujúcich ochranu záznamov podľa §22 zákona č.576/2004 o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov je zodpovednosťou kontrolóra kvality. Za ochranu zdravotníckej dokumentácie na jednotlivých oddeleniach zodpovedajú dokumentačné pracovníčky, v prípade ambulancií zdravotná sestra. Prípadné zistenie porušenia povinností bude považované za porušenie pracovnej disciplíny.

A.18.1.4 Súkromie a ochrana osobných údajov

Zaistenie súladu bezpečnostných politík je zodpovednosťou právneho oddelenia v spolupráci s manažérom informačnej bezpečnosti. Prípadné zistenie porušenia povinností alebo zneužitie oprávnení pri spracúvaní osobných údajov bude považované za porušenie pracovnej disciplíny alebo za hrubé porušenie pracovnej disciplíny. Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobnými údajmi čeliť aj trestnému stíhaniu za trestné činy podľa § 247 a § 374 zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov alebo môže voči nej byť vedené disciplinárne konanie.

A.18.2 Preskúmanie bezpečnosti informácií

Cieľ: *Zabezpečenie zavedenie informačnej bezpečnosti a jej vykonávanie v súlade s politikami a postupmi organizácie.*

A.18.2.1 Nezávislé preskúmanie bezpečnosti informácií

Naplánovanie a realizácia nezávislých auditov v pravidelných intervaloch, ktoré sú vykonávané nezávislým audítorom v súlade s požiadavkami príslušných smerníc. Výsledkom preskúmania bezpečnosti informácií je neustále zlepšovanie primeranosti a účinnosti zavedených politík a opatrení.

A.18.2.2 Súlad s bezpečnostnými politikami a normami

Zavedenie procesu interného auditu podporujúceho zabezpečenie súladu so zavedenými politikami a predpismi organizácie. Zodpovednosť v tomto prípade nesie manažér informačnej bezpečnosti. V prípade, že zistí akýkoľvek nesúlad, vykoná nápravné opatrenia na odstránenie príčiny nesúladu a po implementovaní preskúma účinnosť ich zavedenia. Proces interného auditu je nutné dokumentovať a záznamy uchovávať.

A.18.2.3 Preskúmavanie technického súladu

Vykonávanie kontroly technického súladu na viacerých úrovniach (súčasť zavádzania nových systémov a prostriedkov do prevádzkového prostredia, penetračné testovanie a podobne). Výkon kontrolných činností je zabezpečený IT oddelením, prípadne špecialistami v jednotlivých oblastiach.

3.3 Ekonomické zhodnotenie

Tabuľka č. 13 obsahuje súhrnné zhodnotenie nákladov potrebných na zavedenie bezpečnostných opatrení. Vo fáze implementácie by bola nutná investícia zo strany organizácie vo výške približne 30 000 €. Výška tejto sumy je len orientačná, pretože všetky investície vyššie ako 5 000 € podliehajú zákonu č. 343/2015 Z. z. o verejnom obstarávaní. Samotná implementácia vybavenia a systémov spadá do réžie interných zamestnancov, takže vyčíslenie nákladov je v človekohodinách potrebných na implementáciu. Tá by si celkovo vyžiadala približne 426 človekohodín, resp. 54 človekodní. Ročné náklady na prevádzku systémov by predstavovali investíciu vo výške zhruba 32 000 € a 4 človekodní.

Tabuľka č. 15: Náklady potrebné na zavedenie bezpečnostných opatrení
(Zdroj: Vlastné spracovanie)

Opatrenie	Potrebné vybavenie	Jednotková cena [EUR]	Počet [ks]	Náklady na implementáciu		Ročné náklady na prevádzku	
				EUR	Č/H	EUR	Č/H
Ochrana mobilných zariadení	ESET mobile security	10€/rok	2		1	20	
Kamerový systém	IP kamera Wisenet LNV-6010R	141	4	5545	64		2
	Ip kamera Wisenet LNO-6070R	183	5				
	NVR Wisenet XRN-1610A	1550	1				
	HDD 3TB WD30PURZ Purple	104	1				
	BELDEN F/FTP Cat.6A 100m	56	1				
	Ostatný drobný materiál	100	1				
Zabezpečovací systém + Protipožiarny elektronický systém	Ústredňa DSC PC1864	124	1	6182,8	112	40	2
	Klávesnica PTK 5507	324	1				
	Zónový expandér PC 5108	22,2	4				
	Pir detektor duálny LC-104P/MV	41	36				
	Gsm komunikátor Secolink GSV5	140	3				
	Magnetický kontakt	8	5				
	Dymový detektor Bentel 601P	28	36				
	Ustredňa DSC1832 + klavesnica	220	2				
	Bateria do ustredne 12V/12AH	47	3				
	Kábel komunikačný 300m	71	1				
	Drobný inštalačný materiál	50	1				
	Montáž+zaškolenie	2000	1				
Dochádzkový systém	SYSTEM-IS AMS pre 1800 zamest.	2500	1	7170	80		8
	dochádzkový terminál ATT990LC	934	5				
Active Directory server	Dell PowerEdge R540 S-4108	3541	1	6211	120		8
	DELL HDD 3.5" 2TB NL SAS	230	8				
	DELL Server 2019 Standard DOEM	830	1				
Presun prvkov do "sekundárnej" serverovne	Aruba 2530 48G Switch	817	2	1678	24		2
	OEM X121 1G SFP LC LX	11	4				
Internetové pripojenie	Business Internet	416€/mes	1		16	4992	10
Zabezpečenie prac.staníc	Natec Lobster Key	2,5	50	125	8		
Protipožiarny trezor	Rottner POWER SAFE 600IT	244	1	244	1		
Manažér informačnej bezpečnosti	Mzdové ohodnotenie	1500/mes	1			18000	
Pohotovostná služba	Mzdové ohodnotenie	700€/mes	1			8400	
Prvky NISS	Blokovanie metalických portov 10ks	108 €	4	108	4		
	Zámky Patch cordov 10ks	25 €	5	125	4		
CELKOM				**27389**	**434**	**31452**	**32**

ZHODNOTENIE A PRÍNOSY PRÁCE

Nadobudnutím platnosti zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov vznikla analyzovanému zdravotníckemu zariadeniu povinnosť zavedenia určitých bezpečnostných opatrení. Vzhľadom na to, že spoločnosť doposiaľ informačnú bezpečnosť riešila len okrajovo, bolo nutné venovať pozornosť všetkým oblastiam bezpečnostných opatrení povinných pre danú kategóriu poskytovateľa základnej služby. Zavedením navrhnutých opatrení by spoločnosť dosiahla súlad s legislatívnymi požiadavkami, čo bolo jedným z cieľov práce.

Zavedenie opatrení navrhnutých v tejto práci zaistí zvýšenie celkovej úrovne bezpečnosti informácií, s vysokou mierou návratnosti počiatočnej investície čím bol naplnený stanovený hlavný cieľ práce. Príklad škody, ktorá by mohla vzniknúť v prípade rozhodnutia neaplikovať navrhované bezpečnostné opatrenia demonštruje bezpečnostný incident z decembra minulého roka v nemocnici Rudolfa a Stefanie Benešov. Kybernetický útok prostredníctvom ransomwaru Ryuk mal za následok znefunkčnenie počítačovej siete nemocnice a komunikáciu s inými nemocnicami. Nemocnica bola nútená obmedziť prevádzku, čo spolu s nákladmi na preinštalovanie softwaru predstavuje odhadovanú výšku škody 38 miliónov českých korún. Ďalšiu stratu predstavujú platby od zdravotných poisťovní, ktorých údajná výška bola 3 milióny českých korún denne za obdobie 3 týždňov.

Práca môže byť tiež použitá ako pomocný materiál pri zavádzaní systému riadenia informačnej bezpečnosti do analyzovanej spoločnosti. Napriek tomu, že v súčasnosti spoločnosť neuvažuje o získaní certifikácie podľa ISO/IEC 27001, zavedenie navrhovaných bezpečnostných opatrení uľahčí jej získanie v prípade budúceho záujmu.

ZÁVER

Hlavným cieľom tejto diplomovej práce bol návrh zavedenia bezpečnostných opatrení v súlade s ISMS, ktoré by zabezpečili zvýšenie úrovne bezpečnosti nemocničného zariadenia. Navrhované bezpečnostné opatrenia spĺňajú stanovený hlavný cieľ a taktiež ostatné ciele, keďže sú v súlade s odporúčaniami noriem ISO/IEC rady 27000 a platnou legislatívou.

Predstavenie teoretických východísk objasňujúcich problematiku informačnej bezpečnosti, systém riadenia informačnej bezpečnosti vychádzajúci z noriem rady ISO/IEC 27000 a tiež platnej legislatívy týkajúcej sa nemocničného zariadenia boli nutným krokom v procese navrhovania bezpečnostných opatrení, ktorému bola venovaná prvá časť tejto práce.

Ďalšia časť spracúva predstavenie zvolenej spoločnosti, analýzu súčasného stavu sieťovej infraštruktúry nemocnice a tiež aktuálnej úrovne bezpečnosti v spoločnosti. V analytickej časti práce boli tiež zadefinované požiadavky pre navrhované bezpečnostné opatrenia.

Samotný návrh opatrení, ktorému je venovaná posledná časť práce, má niekoľko častí. V prvej časti boli identifikované a ohodnotené aktíva spoločnosti a tiež hrozby na ne vplývajúce. Následne bola vypracovaná analýza rizík, ktorej výstupom bolo identifikovanie problematických prvkov bezpečnosti v spoločnosti. Na základe analýzy rizík a požiadaviek pre navrhované bezpečnostné opatrenia popisuje nasledujúca časť konkrétne bezpečnostné opatrenia. Záver kapitoly venovanej návrhu vlastného riešenia obsahuje ekonomické zhodnotenie zavedenia odporúčaných opatrení a prínosu práce pre zvolenú spoločnosť.

ZOZNAM POUŽITÝCH ZDROJOV

1. ISO/IEC 2382. Information technology – Vocabulary. 2015
2. ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno:CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-87.
3. OLEJÁR, Daniel. Úvod do informačnej bezpečnosti: Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. In: Informatizácia [online]. 2020, 2013 [cit. 2020-04-20]. Dostupné z: www.informatizacia.sk
4. JORDÁN, Vilém a Viktor ONDRÁK. Infrastruktura komunikačních systémů II: kritické aplikace. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5240-4.
5. BRANDIS, Knud, Ricardo COLOMO-PALACIOS, Srdan DZOMBETA, Knut HAUFE a Vladimir STANTCHEV. A process framework for information security management. International Journal of Information Systems and Project Management [online]. 2016, 2016, **4**(4), 27-47 [cit. 2020-04-12]. DOI: 10.12821. ISSN 2182-7788.
6. Riadenie bezpečnosti informácií ISMS. ICZ: Integrované softwarové a sieťové riešenia [online]. [cit. 2020-04-12]. Dostupné z: www.iczgroup.com/wp-content/uploads/2017/08/ICZ_PL_SEC_ISMS_SK_1707_TLA%C4%8C_01.pd
7. About the IEC. IEC: International Electrotechnical Commission [online]. 2020 [cit. 2020-04-14]. Dostupné z: www.iec.ch/about
8. 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.
9. About us. ISO: International Organization for Standardization [online]. 2020 [cit. 2020-04-14]. Dostupné z: www.iso.org
10. O nás. *Česká agentura pro standardizaci* [online]. Praha, 2017 [cit. 2020-05-01]. Dostupné z: agentura-cas.cz
11. Úvod. Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky [online]. Bratislava, 2019 [cit. 2020-05-01]. Dostupné z: sutn.sk
12. CHLIPALA, Miroslav. Zákon o kybernetickej bezpečnosti: komentár. Bratislava: EUROKÓDEX, 2019. ISBN 978-80-8155-086-7.

13. Vyhláška o bezpečnostných opatreniach podľa zákona o kybernetickej bezpečnosti. Národný bezpečnostný úrad [online]. 21.1.2019 [cit. 2020-03-31]. Dostupné z: www.nbu.gov.sk/2019/01/21/vyhlaska-o-bezpecnostnych-opatreniach-podla-zakona-o-kybernetickej-bezpecnosti
14. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
15. Zákon č. 45/2011 Z. z. o kritickej infraštruktúre
16. Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy
17. Nový slovenský zákon o ochrane osobných údajov - výnimky z GDPR. Konečná & Zacha: Advokátní kancelář [online]. [cit. 2020-03-31]. Dostupné z: www.konecna-zacha.com/novy-slovensky-zakon-o-ochrane-osobnych-udajov-vynimky-z-gdpr/
18. O nemocnici. Nemocnica s poliklinikou Považská Bystrica [online]. [cit. 2020-03-31]. Dostupné z: www.nemocnicapb.sk/o-nemocnici
19. FONS Enterprise. STAPRO SLOVENSKO [online]. Košice, 2020 [cit. 2020-05-01]. Dostupné z: http://www.stapro.sk/produkty-fons/fons-enterprise/
20. KONEČNÝ. POMŮCKA K AUDITU BEZPEČNOSTNÍCH OPATŘENÍ PODLE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI. *Národní centrum kybernetické bezpečnosti* [online]. 2016 [cit. 2020-05-13]. Dostupné z: https://www.govcert.cz/download/kii-vis/container-nodeid-580/vkbchecklistfinalv21rev.pdf
21. ČSN ISO/IEC 27000. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Přehled a slovník. Praha: Český normalizační institut, 2017.
22. ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.
23. ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.
24. ČSN EN ISO 27799. Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002. Praha: Český normalizačný institut, 2019.

ZOZNAM POUŽITÝCH SKRATIEK

CD	compact disk
ČSN	Česká technická norma
EÚ	Európska únia
GDPR	General Data Protection Regulation
GP	Generálna prokuratúra
ICT	informačné a komunikačné technológie
IEC	International Electrotechnical Commission
IMS	Integrated Management System
IS	informačný systém
IS VS	informačný systém verejnej správy
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	informačné technológie
KI	kritická infraštruktúra
KII	kritická informačná infraštruktúra
KS	komunikačný systém
MISE	MediaSys Image Search Engine
NAS	Network Attached Storage
NsP	nemocnica s poliklinikou
NBÚ	Národný bezpečnostný úrad
RDP	Remote Desktop Protocol
SLA	Service Level Agreement
USB	Universal serial bus – univerzálna sériová zbernica
VKB	vyhláška kybernetického zákona
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

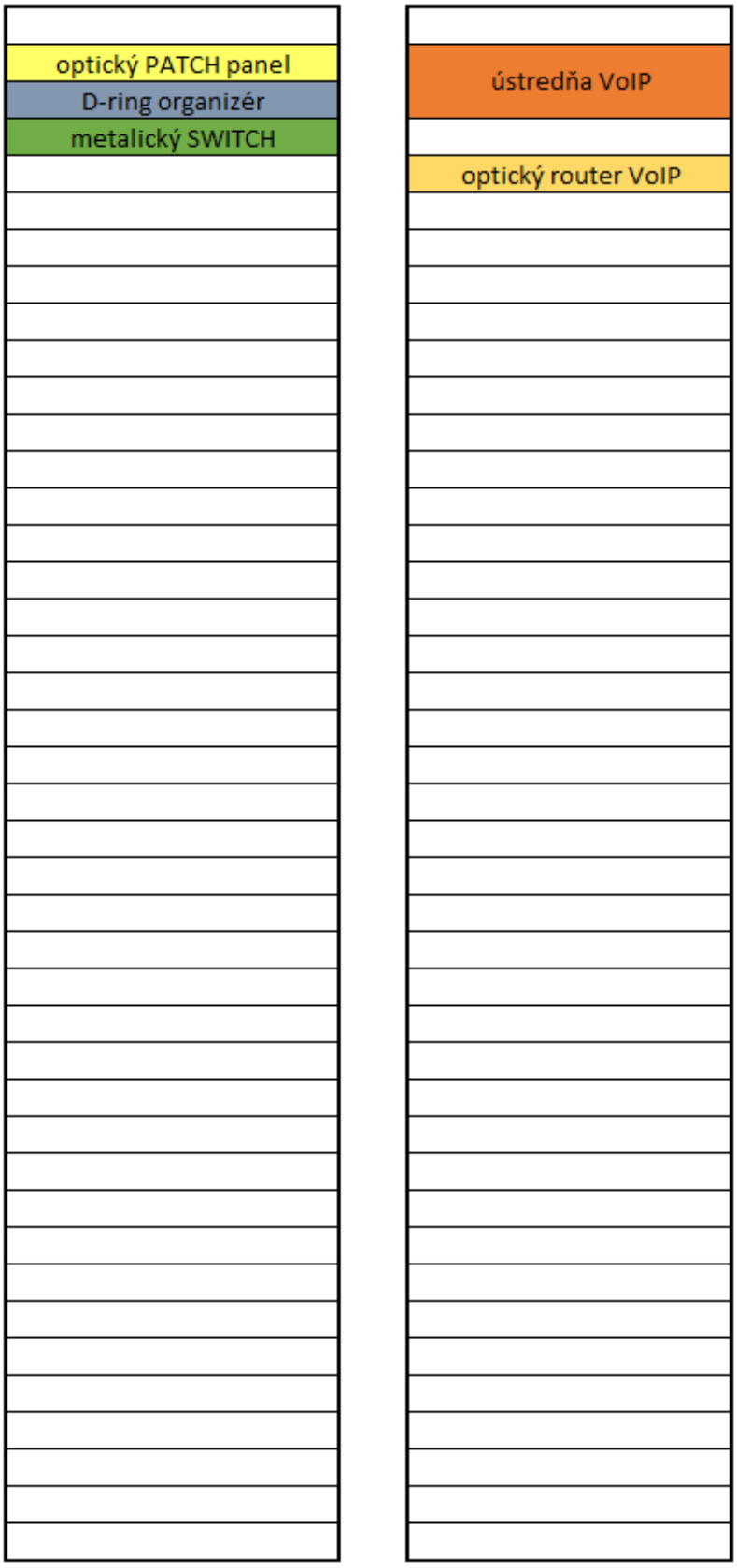
ZOZNAM POUŽITÝCH OBRÁZKOV

ZOZNAM POUŽITÝCH TABULIEK

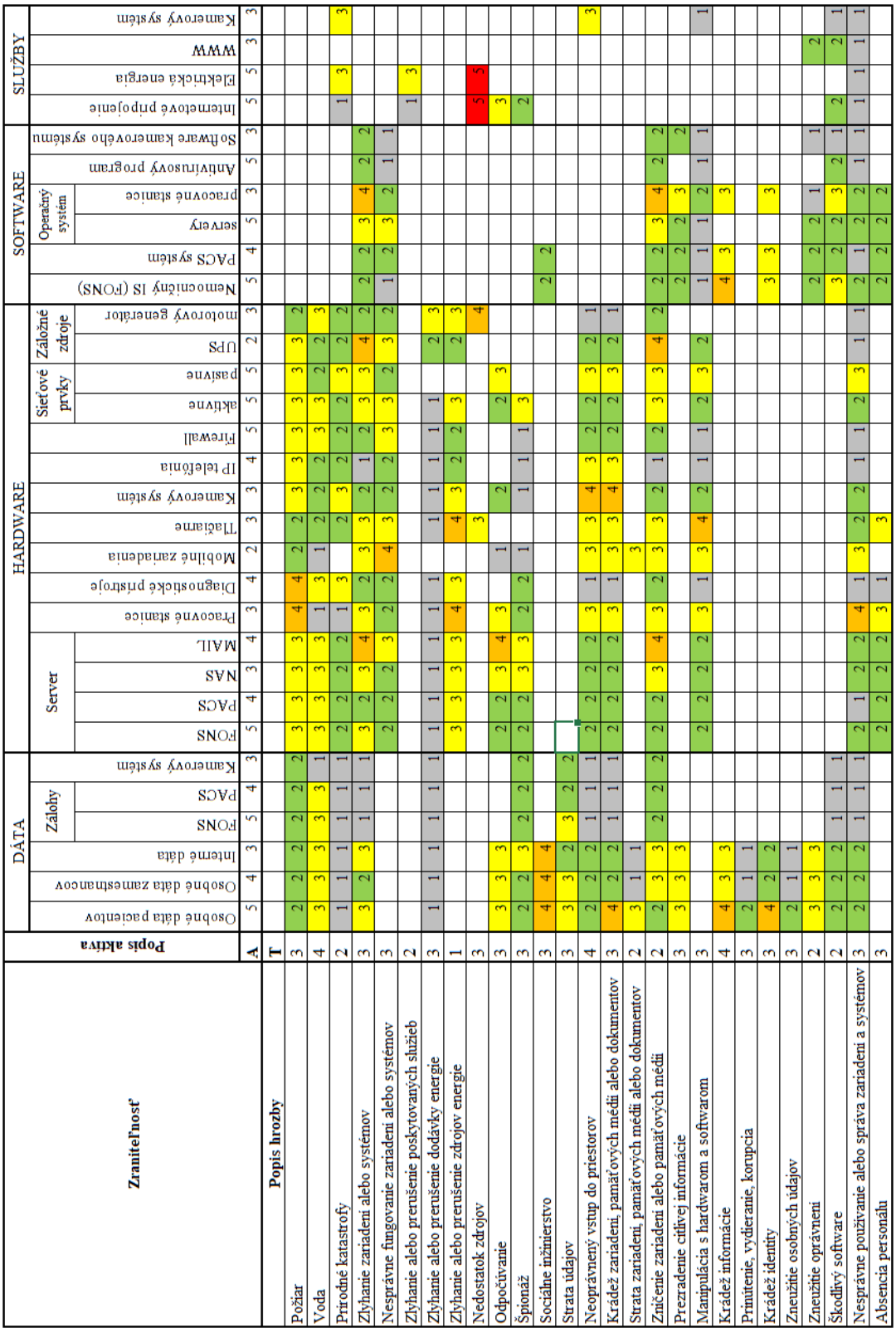
ZOZNAM PRÍLOH

Príloha č. 1: Usporiadanie prvkov v rozvádzačoch – primárna serverovňa

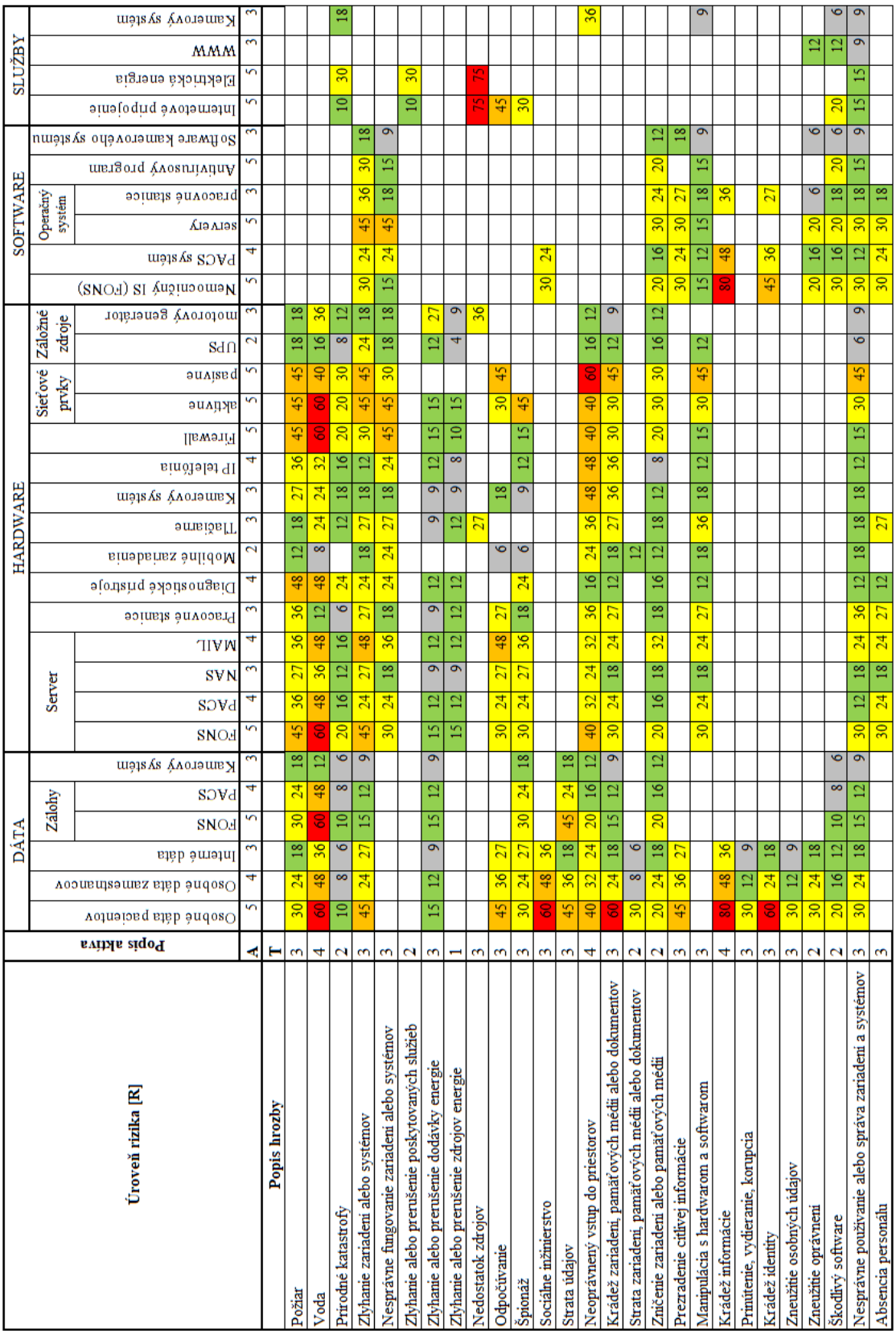
Príloha č. 2: Usporiadanie prvkov v rozvádzačoch – sekundárna serverovňa



Príloha č. 3: Matica zraniteľnosti



Príloha č. 4: Matica úrovní rizík



Príloha č. 5: Príklad plagátu na zvýšenie bezpečnostného povedomia

Príloha č. 6: Príklad prezenčnej listiny školenia informačnej bezpečnosti

PREZENČNÁ LISTINA ŠKOLENIA INFORMAČNEJ BEZPEČNOSTI		
		interný dokument
Dátum školenia:		NEMOCNICA S POLIKLINIKOU Považská Bystrica
Školiteľ:		
Obsah školenia:		
Meno a priezvisko zamestnanca	**Osobné číslo**	**Podpis**

Príloha č. 7: Formulár pre nahlásenie bezpečnostného incidentu

Formulár hlásenia bezpečnostného incidentu			
V prípade podozrenia výskytu bezpečnostného incidentu vyplniť zvýraznené informácie a odoslať na adresu: **oit@nemocnicapb.sk**			interný dokument
ID hlásenia:	(pridelí IT oddelenie)		
Dátum:		NEMOCNICA S POLIKLINIKOU Považská Bystrica	
Čas:			
Meno oznamovateľa:			
Popis bezpečnostného incidentu:			
Dátum prijatia hlásenia:			
Čas prijatia hlásenia:			
Meno prijímajúceho zamestnanca:			
Podpis prijímajúceho zamestnanca:		**Podpis oznamovateľa:**	
		(v prípade tlačenej verzie hlásenia)	

Príloha č. 8: Odporúčaná štruktúra plánu kontinuity

1. Úvod
    - všeobecné informácie: názov organizácie, názov plánu, ciele, rozsah
    - aktivácia a deaktivácia plánu
    - riadenie dokumentu: verzia, autor, zodpovedný pracovník
    - zoznam skratiek
    - relevantné a súvisiace dokumenty
2. Štáb pre kontinuitu činností organizácie
    - zodpovedná osoba
    - tím kontinuity činností, jeho povinnosti a právomoci
3. Obnova prevádzkových systémov
    - stratégia obnovy
    - ciele obnovy a maximálna doba pohotovostnej prevádzky
    - požiadavky na zdroje jednotlivých procesov
    - náhrady pre pohotovostnú a náhradnú prevádzku
    - návrat do bežnej prevádzky
    - následné úlohy
4. Scenáre
    - pre zlyhanie jednej lokality
        - požiadavky na náhradnú lokalitu
        - reaktívne opatrenia pre obnovu
        - zmeny v prevádzkových postupoch počas pohotovostnej prevádzky
        - opatrenia na obnovu a návrat do bežnej prevádzky
    - pre zlyhanie technológie
        - následné scenáre
        - požiadavky na pohotovostnú prevádzku
        - preskúmanie jednotlivých aplikácií/IS
        - plán nákupu náhradných technológií
    - pre stratu zamestnancov
        - následné scenáre

        - požiadavky na pohotovostnú prevádzku
        - reaktívne opatrenia pre obnovu
        - zmeny v prevádzkových postupoch počas pohotovostnej prevádzky
        - opatrenia na obnovu a návrat do bežnej prevádzky
    - pre zlyhanie poskytovateľa služieb
        - následné scenáre
        - reaktívne opatrenia pre obnovu
        - zmeny v prevádzkových postupoch počas pohotovostnej prevádzky
        - opatrenia na obnovu a návrat do bežnej prevádzky
5. Dodatočné informácie
    - lokality
    - pokyny pre príchod na lokality
    - ...
6. Prílohy
    - formuláre
    - šablóny
    - kontrolné záznamy
7. Referenčné dokumenty